Edited by
Fred H. Cate and James X. Dempsey

BULK COLLECTION

Systematic Government Access to Private-Sector Data

OXFORD

Bulk Collection

Bulk Collection

Systematic Government Access to Private-Sector Data

Edited by Fred H. Cate

and

James X. Dempsey

OXFORD
UNIVERSITY PRESS

OXFORD
UNIVERSITY PRESS

Oxford University Press is a department of the University of Oxford. It furthers the University's objective of excellence in research, scholarship, and education by publishing worldwide. Oxford is a registered trademark of Oxford University Press in the UK and certain other countries.

Published in the United States of America by Oxford University Press
198 Madison Avenue, New York, NY 10016, United States of America.

Library of Congress Cataloging-in-Publication Data
Names: Cate, Fred H., editor. | Dempsey, James X., editor.
Title: Bulk collection : systematic government access to private-sector data / Edited by Fred H. Cate and James X. Dempsey.
Description: New York : Oxford University Press, 2017. | Includes bibliographical references and index.
Identifiers: LCCN 2017009578 | ISBN 9780190685515 ((hardback) : alk. paper)
Subjects: LCSH: Government information—Law and legislation. | Electronic records—Access control. | Privacy, Right of. | Data protection—Law and legislation. | Electronic surveillance—Law and legislation. | Internet—Government policy. | Data transmission systems—Law and legislation.
Classification: LCC K3264.C65 B85 2017 | DDC 342/.0662—dc23
LC record available at https://lccn.loc.gov/2017009578

9 8 7 6 5 4 3 2 1

Printed by Edwards Brothers Malloy, United States of America

Note to Readers

This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is based upon sources believed to be accurate and reliable and is intended to be current as of the time it was written. It is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If legal advice or other expert assistance is required, the services of a competent professional person should be sought. Also, to confirm that the information has not been affected or changed by recent developments, traditional legal research techniques should be used, including checking primary sources where appropriate.

(Based on the Declaration of Principles jointly adopted by a Committee of the American Bar Association and a Committee of Publishers and Associations.)

For

Beth E. Cate and

Joan C. Williams

In Memoriam

Joseph H. Alhadeff

CONTENTS

ACKNOWLEDGMENTS

This volume reflects the work of a nearly six-year project created and funded by The Privacy Projects (TPP). We are grateful to members of The Privacy Projects' board, past and present—Audrey Plonk, Chair; Peter Cullen, Vice-chair; Stanley Crosley, Secretary; Joseph Alhadeff (d. 2017); Elizabeth Denham; Toby Milgrom Levin; Deirdre Mulligan; Jules Polonetsky; and Richard Purcell—for their vision and unflagging support.[1]

We are grateful to all of the contributors to this volume who not only prepared and revised essays, but in many cases also participated in discussions that were informed by, and also helped to inform, their contributions.

Earlier versions of a number of these chapters were published in OUP's *International Data Privacy Law*. For that opportunity, we are grateful to Christopher Kuner, Editor-in-Chief, and his colleagues.

A key part of the project on which this volume is based were six multinational meetings held in Brussels, London, Montreal, and Washington. We are grateful for the generous, selfless contributions of all of the participants in those meetings. Their names are listed in the Appendix. Although their participation has greatly strengthened this volume, they bear no responsibility for our recommendations or any errors.

The practical arrangements for those meetings were organized by The Center for Applied Cybersecurity Research at Indiana University and the Center for Democracy & Technology. We are grateful for the practical support afforded by these organizations, and particularly wish to thank James Boyd, Leslee Cooper, Dara Eckart, and Sarah Portwood. Space for the first meeting, in Washington, DC, was generously donated by Hunton & Williams LLP and its Centre for Information Policy Leadership.

The responsibility for coordinating and, in many cases, editing the work of more than two dozen authors was borne by Sarah Portwood. We are indebted to her for her sustained, skilled, and cheerful assistance.

1. One of the authors of this volume, Fred H. Cate, is also a member of The Privacy Projects' board.

Finally, although many of these colleagues played critical roles we have already acknowledged above, we owe special thanks to Martin Abrams, Bojana Bellamy, Julie Brill, Michael Donohue, Jacob Kohnstamm, Christopher Kuner, Ronald D. Lee, Steve Martin, Gregory T. Nojeim, Ira S. Rubinstein, and Jennifer Stoddart.

LIST OF CONTRIBUTORS

Sunil Abraham
Sunil Abraham is the Executive Director of a Bengaluru-based research organization, the Centre for Internet and Society. He founded Mahiti in 1998, a company committed to creating high impact technology and communications solutions. Today, Mahiti employs more than 50 engineers. Mr. Sunil continues to serve on the board.

He was elected an Ashoka fellow in 1999 to "explore the democratic potential of the Internet" and was also granted a Sarai FLOSS fellowship in 2003. Between June 2004 and June 2007, he also managed the International Open Source Network, a project of United Nations Development Programme's Asia-Pacific Development Information Programme serving 42 countries in the Asia-Pacific region. Between September 2007 and June 2008, he managed ENRAP, an electronic network of International Fund for Agricultural Development projects in the Asia-Pacific region, facilitated and co-funded by International Development Research Centre, Canada.

Martin Abrams
Martin Abrams is Executive Director and Chief Strategist at The Information Accountability Foundation. Previously, Mr. Abrams was the co-founder and President of the Centre for Information Policy Leadership at Hunton & Williams LLP, which he led for 13 years. Prior to that, he was Vice President of Information Policy at Experian and Director of Information Policy at TRW Information Systems, where he designed one of the earliest privacy impact assessment tools. He also chaired their Consumer Advisory Council. Mr. Abrams began his consumer policy work at the Federal Reserve Bank of Cleveland, where he was Assistant Vice President and Community Affairs Officer. At the Federal Reserve Bank, he drove collaboration by helping banks and the communities they serve find their intersection of self-interest.

Rebecca Azzopardi
Ms. Azzopardi is completing an LLM thesis at Bond University on the collection and sharing of information for national security purposes with a focus on border protection. She has been practicing law in Australia for 12 years with a varied background in tax litigation, family law, administrative and government

law, and now specializes in information law including privacy and secrecy. The opinions expressed in her chapter are her own and do not reflect the view of any particular entity.

Jane Bailey
Jane Bailey, BAS (Trent), MIR (Queens), LLB (Queens), LLM (Toronto), is a Full Professor at the University of Ottawa Faculty of Law in Canada where she teaches Cyberfeminism and Technoprudence. She co-leads a 7-year partnership called The eQuality Project, which is funded by the Canadian Social Sciences and Humanities Research Council. eQuality is focused on cyberviolence and the discriminatory impact of the algorithmic sort associated with big data practices, particularly in relation to young people from equality-seeking communities. She is the co-editor of *eGirls eCitizens* (uOttawa Press, 2015) and was named a member of the New College of the Royal Society of Canada in 2016.

Eduardo Bertoni
Professor Eduardo Bertoni (PhD, Buenos Aires University) is the Director of the National Data Protection Authority in Argentina. He was the founder and the first director of the Center for Studies on Freedom of Expression and Access to Information (CELE) at Palermo University School of Law, Argentina. He was the Executive Director of the Due Process of Law Foundation (DPLF) until May 2006. Previously, he was the Special Rapporteur for Freedom of Expression of the Inter-American Commission of Human Rights at the Organization of American States (2002–2005). Professor Bertoni is an Argentinean lawyer and holds a Masters in International Policy and Practice from the Elliot School of International Affairs, George Washington University. He currently teaches at Buenos Aires University School of Law and New York University School of Law (Global Clinical Professor).

Beth E. Cate
Clinical Associate Professor Beth Cate's expertise includes intellectual property law, data privacy and security, research regulation, and constitutional law. A practicing lawyer for 20 years, she joined the faculty of Indiana University's School of Public and Environmental Affairs in 2011. She teaches graduate and undergraduate courses examining the intersection of law and public affairs, including a seminar in strategic litigation to advance public policy objectives. Recent publications include entries in *Springer's Global Encyclopedia of Public Administration, Public Policy, and Governance*, on constitutional rights of public employees and the constitutional intersection of civil liberties and public administration; a coauthored set of guidelines published in the *FASEB Journal* for ensuring due process in animal research investigations; and a chapter (coauthored with Andrea Need) examining race and criminal justice reform in Tavis Smiley's *Covenant with Black America—Ten Years Later.*

Fred H. Cate
Fred H. Cate is Vice President for Research, Distinguished Professor, and C. Ben Dutton Professor of Law at Indiana University. The author of more

than 150 articles and books and a frequent advisor to government and industry on privacy and security issues, he serves as a senior policy advisor to the Centre for Information Policy Leadership at Hunton & Williams LLP and is one of the founding editors of the OUP journal, *International Data Privacy Law*.

Scott Charney
Scott Charney is Corporate Vice President for Microsoft's Trustworthy Computing Group. This group is responsible for the security of Microsoft's products and services, as well as other corporate programs enforcing Microsoft's mandatory engineering policies. Earlier in his career, Mr. Charney served as Chief of the Computer Crime and Intellectual Property Section (CCIPS) at the US Department of Justice where he was responsible for implementing the Justice Department's computer crime and intellectual property initiatives. Under his direction, CCIPS investigated and prosecuted national and international hacker cases, economic espionage cases, and violations of the federal criminal copyright and trademark laws. He served three years as Chair of the G8 Subgroup on High-Tech Crime, was Vice Chair of the OECD Group of Experts on Security and Privacy, was cochair of the CSIS Commission on Cybersecurity for the 44th Presidency, and currently serves on the President's National Security and Telecommunications Advisory Committee.

Ashley S. Deeks
Ashley Deeks joined the University of Virginia Law School in 2012 as an associate professor of law. Her primary research and teaching interests are in the areas of international law, national security, intelligence, and the laws of war. Earlier she served as the assistant legal adviser for political-military affairs in the US Department of State's Office of the Legal Adviser. In 2005, she served as the embassy legal adviser at the US Embassy in Baghdad. Professor Deeks was a 2007–2008 Council on Foreign Relations International Affairs Fellow. She received her JD with honors from the University of Chicago Law School, where she served on the Law Review, and clerked for Judge Edward R. Becker of the US Court of Appeals for the Third Circuit. She is a member of the State Department's Advisory Committee on International Law and is a senior contributor to the *Lawfare* blog.

James X. Dempsey
James X. Dempsey is executive director of the Berkeley Center for Law & Technology at the University of California, Berkeley, School of Law. Previously, he was at the Center for Democracy & Technology, where he held a number of leadership positions, including Executive Director and head of CDT West. From 2012 to January 2017, he served as a member of the Privacy and Civil Liberties Oversight Board, an independent federal agency charged with advising senior policymakers and overseeing US counterterrorism programs. He is coauthor (with David Cole) of *Terrorism & the Constitution: Sacrificing Civil Liberties in the Name of National Security*.

Justin Hemmings
Justin Hemmings is an associate in Alston & Bird's Technology practice and Cybersecurity Preparedness & Response Team. He focuses his practice on cybersecurity, data security, and information privacy. He has provided advice on a range of cybersecurity topics, including cryptography, international mutual legal assistance, telecommunications privacy, and digital advertising.

Mr. Hemmings holds a BA from Rutgers University and a JD from American University. He was a research associate at the Georgia Institute of Technology Scheller College of Business, where he worked with Professor Peter Swire.

Sang Jo Jong
Sang Jo Jong, Professor of Law at Seoul National University, graduated from Seoul National University and did his PhD studies at the London School of Economics. He taught Korean Law at Harvard Law School and at the University of Washington School of Law, and also taught comparative intellectual property law at Georgetown University Law Center and at Duke Law School. He has served as a civilian member of the Presidential Council on Intellectual Property, President of the Korea Game Law & Policy Society, the Director of the SNU Center for Law & Technology, the Dean of the SNU School of Law, and a Panel Member of the WIPO Arbitration and Mediation Center. His publications include "Fair Use: A Tale of Two Cities" in *Intellectual Property in Common Law and Civil Law* (Northampton: Edward Elgar, 2013) and many others.

Collin Kurre
Collin Kurre is the Policy and Communications Officer for Internet & Jurisdiction, a global multi-stakeholder policy network. Previously, she served as the Public Policy Intern at CELE, the Center for Freedom of Expression and Access to Information in Buenos Aires, Argentina. Ms. Kurre holds a Master of Public Policy from Georgetown University, where she specialized in multi-stakeholder Internet governance. She also holds a Master of International Development from the Universidad Nacional de San Martín in Argentina and a BA (cum laude) in English Literature. She was a US National Merit scholar and speaks English, Spanish, and French.

Ronald D. Lee
Ronald D. Lee, a partner of Arnold & Porter LLP in Washington, DC, is a national security, cybersecurity, privacy, and government contracts lawyer. He served as General Counsel of the US National Security Agency from 1994 to 1998 and as Associate Deputy Attorney General, US Department of Justice, from 1998 to 2000.

Mr. Lee graduated from Princeton University with highest honors. He received an MPhil in International Relations from the University of Oxford, where he attended Balliol College as a Rhodes Scholar, and a JD from Yale Law School. He served as a law clerk to Justice John Paul Stevens, United States Supreme Court, and as a law clerk to Judge Abner J. Mikva, United States Court

of Appeals for the District of Columbia Circuit. He is an elected member of the American Law Institute and regularly writes and speaks on cybersecurity, privacy, counterterrorism, national security, and government contracts.

Bruno Magrani
Bruno Magrani is the Head of Public Policy for Facebook in Brazil. Before joining Facebook, Mr. Magrani worked as a professor and researcher of law at the Center for Technology and Society at FGV Law School focusing on intellectual property, innovation, and data protection. He holds law degrees from Harvard Law School and the Federal University of Rio de Janeiro.

Winston J. Maxwell
Winston Maxwell is a partner in the international law firm Hogan Lovells. In 2014 he was appointed to the French National Assembly's Commission on Digital Rights, and was asked to contribute to the French Conseil d'Etat's 2014 report on fundamental rights in the digital age. Mr. Maxwell has completed projects for the European Commission, the French telecom regulatory authority (ARCEP), and data protection authority (CNIL) on forward-looking regulatory issues. After authoring a 2011 book on net neutrality with a member of France's telecommunications regulatory authority, he has become one of the country's leading experts on net neutrality. Mr. Maxwell holds a JD from Cornell Law School and a PhD in Economics from Telecom ParisTech. He is a member of the Paris and New York bars.

Gregory T. Nojeim
Gregory Nojeim is Director of the Freedom, Security and Technology Project at the Center for Democracy and Technology, a Washington, DC NGO dedicated to Internet freedom. Mr. Nojeim specializes in protecting privacy in the digital age as against intrusion by the government. He is a recognized expert regarding the PATRIOT Act, FISA, and the application of the Fourth Amendment to the US Constitution to electronic surveillance.

Mr. Nojeim directs CDT's privacy initiatives that respond to the 2013 disclosures about NSA surveillance, and was engaged in CDT's successful efforts to promote the 2015 USA Freedom Act. He is also involved in a multi-year project to update the 1986 Electronic Communications Privacy Act.

He sits on the Board of Directors of the Global Network Initiative. Prior to joining CDT, he was the Associate Director of the ACLU's Washington Legislative Office. He received his law degree from the University of Virginia in 1985.

Stephanie K. Pell
Stephanie Pell is an Assistant Professor and Cyber Ethics Fellow at West Point's Army Cyber Institute and teaches Cyber Ethics in the Department of English and Philosophy. She writes about privacy, surveillance, cybersecurity, and national security law and policy, and is particularly interested in the tensions inherent in enabling traditional law enforcement efforts and making our communications networks more secure. Prior to joining West Point's faculty, Professor Pell served as Counsel to the House Judiciary Committee and was a federal prosecutor for

over fourteen years. She was a lead prosecutor in *United States v. Jose Padilla* (American citizen detained as an enemy combatant prior to criminal indictment and trial), and in *United States v. Conor Claxton* (IRA operatives who purchased weapons in South Florida and smuggled them into Belfast, Northern Ireland, during peace process negotiations). She received her undergraduate, master's and law degrees from the University of North Carolina at Chapel Hill.

Giorgio Resta
Giorgio Resta, PhD University of Pisa, is Professor of Comparative Law, University of Roma Tre, Italy. A Visiting Professor at several universities (among them McGill, EHESS, and Nagoya), he is a member of the International Academy of Comparative Law and cofounder of the Italian Academy for the Internet Code. He has authored more than 90 publications in the fields of comparative law, information law and new technologies, data protection, intellectual property, and torts. Among his books are *Dignità, persone, mercati* (Giappichelli 2014); *Trial by Media as a Legal Problem: A Comparative Analysis* (E.S. 2009); *Le persone fisiche e i diritti della personalità* (UTET, 2006); *Autonomia privata e diritti della personalità* (Jovene, 2005; prize Club dei Giuristi). He is the editor of *La protezione transnazionale dei dati personali* (RomaTrepress 2016); *Riparare risarcire ricordare* (E.S. 2012; prize Italian Research Council); *Karl Polanyi, For a New West* (Polity Press, 2014).

Ira S. Rubinstein
Ira Rubinstein is a Senior Fellow at the Information Law Institute (ILI) of the New York University School of Law. His research interests include Internet privacy, electronic surveillance law, big data, and voters' privacy. Mr. Rubinstein lectures and publishes widely on issues of privacy and security and has testified before Congress on these topics. Prior to joining the ILI, he spent 17 years in Microsoft's Legal and Corporate Affairs department, most recently as Associate General Counsel in charge of the Regulatory Affairs and Public Policy group. Mr. Rubinstein is currently a Senior Fellow at the Future of Privacy Forum and serves on the Board of Advisers of the American Law Institute for the Restatement Third, Information Privacy Principles. He also served as Rapporteur for the EU-US Privacy Bridges Project, which was presented at the 2015 International Conference of Privacy and Data Protection Commissioners. He graduated from Yale Law School in 1985.

Paul M. Schwartz
Paul Schwartz is a leading international expert on information privacy law. He is Jefferson E. Peyser Professor at the University of California, Berkeley, School of Law and a director of the Berkeley Center for Law and Technology. Professor Schwarz is the author of many books, including the leading casebook, "Information Privacy Law," and the distilled guide, "Privacy Law Fundamentals," each with Daniel Solove. Professor Schwartz's over 50 articles have appeared in journals such as the *Harvard Law Review, Yale Law Journal, Stanford Law Review, University of Chicago Law Review,* and *California Law Review*. He publishes on

a wide array of privacy and technology topics including data analytics, cloud computing, financial privacy, European data privacy law, and comparative privacy law. His home page is www.paulschwartz.net, and his Twitter account is @paulmschwartz.

Sara Shayan
Sara Shayan is interested in the intersections of law, technology, and policy, particularly with regard to privacy and digital security. She holds a Bachelor of Arts (Hons) from the University of British Columbia and is a JD candidate at the University of Ottawa.

Sarah St.Vincent
Sarah St.Vincent is a researcher and advocate on national security, surveillance, and domestic law enforcement for the United States program at Human Rights Watch. She previously served as a fellow on human rights and surveillance at the Center for Democracy & Technology and as a Skadden Fellow at the Advice on Individual Rights in Europe (AIRE) Centre. She holds a JD from the University of Michigan Law School, an MA in East Asian regional studies from Harvard, and a BA from Swarthmore College.

Dan Jerker B. Svantesson
Professor Svantesson is a Co-Director of the Centre for Commercial Law at the Faculty of Law Bond University and a Researcher at the Swedish Law & Informatics Research Institute, Stockholm University. He specializes in international aspects of the IT society, a field within which he has published a range of books and articles and given presentations in Australia, Asia, North America, and Europe.

Professor Svantesson was an Australian Research Council Future Fellow (2012–2016) and is the Managing Editor for International Data Privacy Law, published by Oxford University Press. He is a Member of the Editorial Boards for the International Journal of Law and Information Technology, the Commonwealth Law Bulletin, the International Review of Law Computers and Technology, the Masaryk University Journal of Law and Technology and the Computer Law and Security Review. In 2016, he was awarded both the Faculty of Law Research Excellence Award and the Vice Chancellor's Award for Research Excellence.

Peter Swire
Peter Swire is the Huang Professor of Law and Ethics at the Georgia Tech Scheller College of Business, and Senior Counsel with Alston & Bird, LLP.

In 2015, the International Association of Privacy Professionals, among its over 20,000 members, awarded him its Privacy Leadership Award. In 2013, he served as one of five members of President Obama's Review Group on Intelligence and Communications Technology.

Under President Clinton, Mr. Swire was the Chief Counselor for Privacy, in the US Office of Management and Budget, as the first person to have US

government-wide responsibility for privacy policy. Under President Obama, he served as Special Assistant to the President for Economic Policy.

Mr. Swire is author of six books and numerous scholarly papers. He has testified often before Congress and been quoted regularly in the press. He graduated from Princeton University and the Yale Law School.

Omer Tene
Omer Tene is Vice President of Research and Education at the International Association of Privacy Professionals. He is an Affiliate Scholar at the Stanford Center for Internet and Society and a Senior Fellow at the Future of Privacy Forum. He is Associate Professor at the College of Management School of Law, Rishon Lezion, Israel (on leave).

Motohiro Tsuchiya
Motohiro Tsuchiya is a professor of Graduate School of Media and Governance at Keio University in Japan and Deputy Director at Keio Global Research Institute (KGRI). Prior to joining the Keio faculty, he was associate professor at the Center for Global Communications (GLOCOM), International University of Japan. He is interested in the impact of the information revolution on international relations, regulations regarding telecommunications and the Internet, global governance and information technologies, and cyber security. He authored *Cyber Terror* (Tokyo: Bungeishunju, 2012, in Japanese), *Cyber Security and International Relations* (Tokyo: Chikura Shobo, 2015, in Japanese), and coauthored more than 20 books including *Cybersecurity: Public Sector Threats and Responses* (Boca Raton, FL: CRC Press, 2012, in English) and *Information Governance in Japan: Towards a New Comparative Paradigm* (SVNJ eBook series, Kindle Edition, 2016). He earned his BA in political science, MA in international relations, and PhD in media and governance from Keio University.

Nico van Eijk
Nico van Eijk is Professor of Media and Telecommunications Law and Director of the Institute for Information Law (IViR, Faculty of Law, University of Amsterdam. http://www.ivir.nl/staffpage/eijk/). He also works as an independent legal adviser.

Among other things, he is the Chairman of the Dutch Federation for Media and Communications Law (Vereniging voor Media- en Communicatierecht, VMC), chairman of a committee of The Social and Economic Council of the Netherlands (SER), member of the Knowledge network of the Dutch Review Committee on the Intelligence and Security Services (CTIVD), and member of the Royal Holland Society of Sciences and Humanities (KHMW).

Zhizheng Wang
Zhizheng Wang graduated from the Peking University Law School with a Juris Master degree. He previously was a graduate fellow of the Indiana University Center for Applied Cybersecurity Research and held teaching positions in Beijing Jiaotong University and Beihang University. He has been engaged in the information technology industry for more than 20 years and is the founding President and Chief Executive Officer of Qeca Private Foundation.

GLOSSARY OF ACRONYMS AND ABBREVIATIONS

ABIN	Brazilian Intelligence Agency
ACHR	American Convention on Human Rights
ACRI	Association for Civil Rights in Israel
ADC	Argentine Asociación por los Derechos Civiles
AFI	Argentine Federal Intelligence Agency
AFP	Australian Federal Police
American Declaration	American Declaration of the Rights and Duties of Man
ANAC	Brazilian National Civil Aviation Agency
ANATEL	Agência Nacional de Telecomunicações, aka Brazilian Communications Agency
API	Advance Passenger Information
APIPPA	Korean Act on Personal Information Protection of Public Agencies
ASIO	Australian Security Intelligence Organisation
AUSTRAC	Australian Transaction Reports and Analysis Centre
Basic Law	Israeli Basic Law: Human Dignity and Freedom
BDSG	*Bundesdatenschutzgesetz*
Bill C-13	Protecting Canadians from Online Crime Act
Bill C-22	Canadian National Security and Intelligence Committee of Parliamentarians Act
Bill C-44	Protection of Canada from Terrorists Act
Bill C-51	Canadian Anti-Terrorism Act, 2015
BRS	Brazilian Revenue Service
BSFC	Brazilian Supreme Federal Court
BND	*Bundesnachrichtendienst*
CALEA	US Communications Assistance for Law Enforcement Act
CAU	FBI Communications Assistance Unit
CBSA	Canada Border Services Agency

CCP	Chinese Communist Party
CERT	Cyber Event Readiness Team
CJEU	Court of Justice of the European Union
CMS	Central Monitoring System
CNCTR	Commission for Oversight of Intelligence Gathering Techniques
COAF	Counsel for the Control of Financial Activities
Communications Data Act	Israeli Criminal Procedure Act (Enforcement Powers—Communications Traffic Data), 2007
CNIL	*Commission Nationale de l'Informatique et des Libertés*
CRTC	Canadian Radio-television and Telecommunications Commission
CSE/CSEC	Canadian Communications Security Establishment
CSIS	Canadian Security Intelligence Service
DARPA	US Defense Advanced Research Projects Agency
DCAF	Democratic Control of Armed Forces
DIBIS	Department for the Integration of activities developed by the Brazilian Intelligence System
DIJIN	Directorate of Criminal Investigation and Interpol
DINI	Peruvian National Intelligence Directorate
DND	Canadian Department of National Defence
DOD	US Department of Defense
DOJ	US Department of Justice
DRIPA	Data Retention and Investigatory Powers Act 2014
ECHR	Convention for the Protection of Human Rights and Fundamental Freedoms, aka the European Convention on Human Rights
ECJ	European Court of Justice
ECPA	Electronic Communications Privacy Act
ECS	electronic communications service
ECtHR	European Court of Human Rights
EDPS	European Data Protection Supervisor
EFF	Electronic Frontier Foundation
ETSI	European Telecommunications Standards Institute
EU Charter	Charter of Fundamental Rights of the European Union
FAA	US FISA Amendments Act of 2008
FBI	Federal Bureau of Investigation
FINTRAC	Canadian Financial Transactions and Reports Analysis Centre
FISA	US Foreign Intelligence Surveillance Act

FISC	US Foreign Intelligence Surveillance Court
FOIA	Israeli Freedom of Information Act, 1998; also US Freedom of Information Act
FTC	US Federal Trade Commission
GDPR	General Data Protection Regulation of the European Union
GSS	Israeli Internal Security
GNI	Global Network Initiative
HRC	Human Rights Committee (the UN body that oversees the implementation of the ICCPR)
IACHR	Inter-American Commission on Human Rights
IACtHR	Inter-American Court of Human Rights
IAJC	Inter-American Juridical Committee
IC	Intelligence Community
ICCPR	International Covenant on Civil and Political Rights
IG	Inspector General
INCB	Israel National Cyber Bureau
IoT	Internet of Things
IP	Internet Protocol
IPP	Information Privacy Principle
ISA	Israeli Security Agency (aka "Shin Bet" or "Shabak")
ISP	Internet Service Provider
ISAA	Israeli General Security Service Act, 2002
ISU	Integrated Security Unit
MLAT	Mutual Legal Assistance Treaty
MND	Canadian Minister of National Defence
Mossad	Israeli Foreign Intelligence
MPS	Canadian Minister of Public Safety; also Chinese Ministry of Public Security
NATGRID	National Intelligence Grid
NDA	Canadian National Defence Act
NSA	National Security Agency
NSL	National Security Letter
OHCHR	Office of the United Nations High Commissioner for Human Rights
PAA	US Protect America Act of 2007
PCC	Privacy Commissioner of Canada
PCLOB	US Privacy and Civil Liberties Oversight Board
PIPA	Korean Personal Information Protection Act
PIPEDA	Personal Information and Protection of Electronic Documents Act
PNR	passenger name record
PPA	Israeli Privacy Protection Act, 1981

PSC	Public Safety Canada
RCMP	Royal Canadian Mounted Police
RCS	Remote Computing Service
RFPA	US Right to Financial Privacy Act
SCA	US Stored Communications Act
SCC	Supreme Court of Canada
SIRC	Canadian Security Intelligence Review Committee
SWIFT	Society for Worldwide Interbank Financial Telecommunications
Telecommunications Act	Israeli Telecommunications Act
TIA	Total Information Awareness (later renamed "Terrorism Information Awareness")
TPP	The Privacy Projects
TSP	Terrorist Surveillance Program; also telecommunications service provider
VoIP	Voice over Internet Protocol
Wiretap Act	Israeli Wiretap Act, 1979

INTRODUCTION AND BACKGROUND

FRED H. CATE AND JAMES X. DEMPSEY

The tensions between privacy and security seem sharper than ever. Concerns about terrorism are driving many governments to adopt more expansive surveillance powers, while human rights courts, at least in Europe, continue to cite privacy rights to strike down overbroad measures. The digital services woven into our personal and professional lives generate more and more information revealing our movements, actions, and intentions, while encryption that shields communications from interception and blocks access to data stored on mobile devices is becoming widespread. Big data techniques make it easier for governments to ingest large amounts of data and mine it to discern patterns and make decisions, but governments simultaneously complain they are "going dark" in the face of technological change, unable to obtain evidence crucial to criminal and national security investigations. Regulators seek to promote enhanced cybersecurity, yet fairly simple phishing techniques expose huge volumes of email and documents to hackers, undermining not only privacy but the democratic process.

This volume represents the culmination of a nearly six-year project examining this tension. It began as an effort to obtain a snapshot of what seemed to be growing government demands for bulk access to data held by the private sector. After leaks and authorized disclosures lifted the shroud of secrecy around the bulk collection activities of some governments, it turned into something much more ambitious: an effort to explore what should be the rules for government access to data and what should be the responses of private sector companies to those demands.

Throughout, the project unfolded in the context of the vast changes wrought by the ongoing revolution in information and communications technology. As a part of daily life, individuals around the world use services that collect and store data in digital form. The expansive aggregation of personal data in the hands of private-sector companies is true equally of businesses firmly rooted in the physical world—retailers, health care providers, financial institutions, utilities, airlines, hotels—and of those based online. The emergence of the Internet of Things—always on, always collecting—is further amplifying this trend.

Within this ocean of data is information of value to governments pursuing legitimate interests and, of course, to those seeking to suppress and control. Governments understandably want access to this data. At the top of their list is communications data—the content of communications and also records of who is calling whom, mobile phone location data, and Internet connection records. Also of interest are bank records, travel records, and potentially any kind of data that could reveal a person's activities. Essentially every government in the world claims the power to compel disclosure of this data by the companies that hold it. The rules surrounding such disclosures—how much can be obtained, under what standard, and upon the approval of what authority—remain an urgent concern of both citizens and the companies holding their data.

Our project was premised on the view that there is a fundamental distinction between situations where government agents demand from third parties data regarding a particular target and, on the other hand, situations where the government is collecting large quantities of data without discrimination. For the former, which traditionally characterized law enforcement investigations, practices and rules have for some time been relatively clear (even as the variety of information available has expanded): when seeking data about an individual in a criminal investigation, government agents must have some threshold of particularized suspicion linking that person to a specific crime, they must obtain independent authorization for the surveillance or data acquisition, and the intrusion on privacy must be limited in time and scope to the acquisition of evidence relevant to the crime being investigated.

However, it is now clear, governments have also been collecting information without particularized suspicion, often for intelligence or national security purposes but also, almost unnoticed, for regulatory purposes. These nonparticularized, bulk demands pose unique questions that our project explored. Four issues in particular are salient. The first concerns transparency: What powers are governments exercising? When we began this work, bulk collection programs conducted in the name of national security had not been publicly avowed. The second question is about legality: Does a publicly-available statute authorize and define the government's power in clear terms? The third issue is normative: What standards should limit government access, and what structure of control and oversight can assure against abuse? Finally, even if publicly avowed and even if statutorily authorized, can a system of safeguards and oversight ever be robust enough to legitimize mass surveillance, or are bulk programs incompatible with human rights principles of necessity and proportionality?

OUR PROCESS

In 2011, under the auspices of The Privacy Projects, we began exploring what we called at the time "systematic government access to data held by the private sector." By "systematic access," we meant both direct access by the government to private-sector databases, without the mediation or interaction of an employee or agent of the entity holding the data; and government access, whether or not

mediated by a company, to large volumes of private-sector data. It seemed to us at the time that there had been an increase worldwide in government demands for data held by the private sector, driven by a variety of factors, and that this had included an expansion in government requests for direct access or bulk disclosures.

Two years before the Snowden leaks, we commissioned papers from leading experts in nine countries (Australia, Canada, China, Germany, India, Israel, Japan, the UK, and the United States), asking them to explore what, if anything, was publicly known about bulk collection in their countries and to describe the laws regarding broad government access to private-sector data. In April 2012, we convened a meeting in Washington of academics, privacy advocates, and private-sector leaders to review those papers and chart a course for further research.[2] Among other things, we decided to expand the geographic scope of the study and commissioned four additional papers (covering Brazil, France, Italy, and the Republic of Korea),[3] which were the subject of another multi-stakeholder roundtable, held in London in May 2013.

These initial papers confirmed our thesis, identifying various examples of "systematic access" in a wide range of countries. The research also found a general lack of transparency about the nature and scope of data collection practices carried out in the name of national security or foreign intelligence. Many were not publicly acknowledged by the governments, and the companies subject to the demands were prohibited from disclosing them. Moreover, laws on the books did not expressly authorize bulk collection. Even the experts we enlisted admitted that they were uncertain of what the law permitted or how it was being interpreted. Oversight mechanisms, our authors found, were limited and, if they existed, were themselves often shrouded in secrecy.

In June 2013, weeks after our London roundtable, the Snowden leaks began. Unauthorized and authorized disclosures of intelligence programs in the United States, the UK, and some other European countries partly lifted the shroud of secrecy, at least with respect to some countries. The disclosures gave detailed substance to our core concerns about expansive and lightly regulated government demands for access to data held (or transmitted) by the private sector. "Bulk surveillance" came to be featured prominently in national and international debates over governmental power, corporate responsibility, and individual privacy. Policymakers around the world professed shock and concern about the intrusiveness of government (usually other governments') programs of bulk collection.

In the immediate wake of the Snowden leaks, however, much of the commentary was misleading, especially in suggesting that bulk collection was

2. The first nine country reports were published in November 2012 in Volume 2, Issue No. 4 of *International Data Privacy Law*, https://academic.oup.com/idpl/issue/2/4.

3. These papers were published in February 2014 in Volume 4, Issue No. 1 of *International Data Privacy Law*, https://academic.oup.com/idpl/issue/4/1.

predominantly a US and UK practice. Our earlier research had shown that the practice was much more widespread. To highlight our findings and to seek to drive a more accurate discussion of the legal and policy issues, The Privacy Projects organized a public workshop in Brussels in November 2013 for private-sector and civil society representatives to meet with data protection authorities and other government officials. The Privacy Projects also commissioned a major article summarizing the project's findings to date.[4] We also turned our attention to the questions of oversight and accountability, hosting additional workshops in 2014 in Montreal and London focused on means of achieving accountability when the government accesses private-sector records.

Finally, in an effort to pull together these various threads, we commissioned a series of essays from prominent industry leaders, activists, and academics from around the world. These papers addressed in practical terms the elements of oversight that should be applied to any government program seeking broad access to personal data held by the private sector. Other papers address the question of how industry should respond to such requests or demands and how the divergent interests of government, companies, and individuals can be understood. Last, we commissioned papers that assessed bulk or indiscriminate collection against the evolving framework of international law and human rights law.

OUR FINDINGS

This volume contains the fruits of our project. Twelve country reports have been complied here. Most of them have been updated to account for new revelations, laws, and court decisions. They are accompanied by the comparative analysis of Ira Rubinstein, Greg Nojeim, and Ron Lee, also updated. They provide extensive evidence that governments around the world have been collecting data on a very large scale. These collection programs are often conducted in the name of national security, but some are also available for ordinary law enforcement, and there are many broad collection programs conducted for regulatory purposes, such as tax compliance.

The country reports show that, despite some reforms, the worldwide trend continues in the direction of ever larger collections. Indeed, the only country that has conclusively terminated a bulk collection program in recent years is the United States. Counter to its Snowden-induced reputation as a voracious collector of data, in 2015, the United States ended the bulk collection of metadata on domestic and international calls. Congress enacted the USA FREEDOM Act, which amended all potentially applicable statutes to make it clear that they could not be used as the basis for bulk domestic collection in national security matters. Meanwhile, the UK, France, Germany and other countries have ratified or expanded collection programs.

4. Ira Rubinstein, Greg Nojeim, and Ronald Lee, "Systematic Government Access to Personal Data: A Comparative Analysis," 4 *International Data Privacy Law* 96 (2014), http://idpl.oxfordjournals.org/content/4/2.toc.

Many of the country reports discuss not only programs of bulk or mass surveillance—surveillance that involves, for example, all telephone calls or all Internet service—but also programs that are targeted (focused on specific individuals or accounts) but that nevertheless collect very large amounts of data on large numbers of individuals. Given modern technology, even targeted collection programs can be very broad. The intake of such programs, if stored for extended periods of time, can constitute quite a comprehensive database on quite a large swath of the public. How such data is searched, for example, may be as important as the rules for how it was collected in the first place. Even though our baseline distinction between targeted and indiscriminate collection remains valid, the country reports remind us that it is probably best to view government collection activities as arrayed across a spectrum from the tightly targeted and rarely applied to the targeted but broadly applied to the comprehensive. Especially where companies are required to maintain databases of records (data retention mandates) and to install filtering or retrieval capabilities on their networks for use by the government at will (as France and the UK now seem to require), the distinction between targeted and bulk collection may disappear. Systematic access (our initial focus) may no longer require bulk collection.

The country reports and the papers in the second half of the volume also reveal that there have been some positive developments since we began this project. Although powers of bulk surveillance had, until recently in all the countries surveyed, been exercised in the dark, lately there has been a move toward greater transparency. In response to the Snowden leaks, the United States and the UK officially acknowledged a number of practices. In other countries, bulk collection programs continue to be shrouded in secrecy, but there has been "progress" in the sense that a number of countries have amended their laws to more explicitly describe the powers exercised by their governments. This at least theoretically subjects the programs to the democratic process.

Another positive development is that these new laws, while generally ratifying or even extending bulk collection powers, have included new oversight or accountability measures. The UK's new Investigatory Powers Act includes a "double-lock" for the most intrusive powers, so that warrants issued by a Secretary of State will also require the approval of a senior judge. The Act creates a new Investigatory Powers Commissioner to oversee how the new powers are used, establishes limits on government access to journalistic and legally privileged material, and creates new criminal offenses for misusing the powers. France, in its 2015 law, created a new, independent Commission for Oversight of Intelligence Gathering Techniques. Under the law, intelligence gathering measures can be implemented only when a specific authorization is given by the prime minister or his or her designee, and the prime minister's authorization can be granted only after the Commission has rendered an opinion, albeit one that is not binding, on the compatibility of the measure with the principles set forth in the law.[5]

5. Winston Maxwell, "French Surveillance Law Permits Data Mining, Drawing Criticism from Privacy Advocates" (August 6, 2015), http://www.hldataprotection.com/2015/08/

Several chapters in this volume explore the development of oversight mechanisms. With Marty Abrams, we have a chapter showing how the principle of accountability, now woven into data protection law in the commercial context, has direct application to government surveillance. Eduardo Bertoni and Collin Kurre describe still-evolving oversight mechanisms in Latin America. Nico van Eijk, drawing on the jurisprudence of the European Court of Human Rights, fleshes out the multiple elements needed for a truly effective oversight program.

As van Eijk explains, effective oversight must encompass prior authorization, after-the- fact review, and redress of complaints. No one body or structure can be relied on to provide adequate control of government surveillance. Courts, no matter how independent, can secretly approve programs that seem unreasonable in the light of day. Parliamentary bodies may grant broad powers. Effective oversight can be achieved only with a web of checks and balances, implemented by multiple bodies of varying competencies, reinforcing each other. Overall, the principles of oversight and accountability seem to be gaining wide credence in democratic countries, if only because governments recognize that they must maintain some level of trust if they are to retain their expansive powers.

But the most remarkable development of the past six years, second only to the startling revelations of bulk collection, has been the insistence of human rights courts and other institutions on the principles of privacy and the willingness of those bodies to strike down or criticize surveillance measures even when justified in the name of fighting terrorism. Especially assertive have been the two human rights courts in Europe: the European Court of Human Rights (ECtHR) and the Court of Justice of the European Union (CJEU). In the *Schrems* case, the CJEU invalidated the EU-US Safe Harbor for failing to address standards for US government access to data that global companies transfer from Europe to the United States for storage and other processing. In *Digital Rights Ireland*, it overturned the EU directive that had required service providers to retain metadata on customer communications. The ECtHR invalidated surveillance laws in Russia (the *Zakharov* case) and Hungary (the *Szabó and Vissy* case) on the ground that the laws were insufficiently discriminate in their targeting standards. At the national level, the French Constitutional Council in October 2016 declared a provision of the 2015 French law unconstitutional. Also in October 2016, the UK's investigatory powers tribunal ruled that British intelligence agencies had been unlawfully collecting massive volumes of confidential personal data without proper oversight for 17 years.[6] Nonjudicial independent oversight bodies also proved their value. In the

articles/international-eu-privacy/french-surveillance-law-permits-data-mining-drawing-criticism-from-privacy-advocates/.

6. "UK Security Agencies Unlawfully Collected Data for 17 Years, Court Rules," *The Guardian* (October 17, 2016), https://www.theguardian.com/world/2016/oct/17/uk-security-agencies-unlawfully-collected-data-for-decade.

United States, the Privacy and Civil Liberties Oversight Board played an important role in ending the program that collected telephone calling records in bulk.[7]

As the chapters by Ashley Deeks and Sarah St.Vincent, as well as the comparative analysis of Rubinstein, Nojeim, and Lee, show, there is remarkable consistency in defining the components of an effective system of checks and balances. The elements of the framework of oversight and accountability are drawn from long-accepted principles of the rule of law, human rights, and democratic governance. Most important for our project, the conclusion that bulk or indiscriminate collection is fundamentally incompatible with human rights principles may be gaining hold.

Two actions taken after most of the chapters in this book were written—the UK's November 2016 adoption of a new investigatory powers act and the December 2016 decision of the CJEU striking down national data retention laws of Sweden and the UK—illustrate both the assertion of bulk powers by governments and the application of human rights principles to reject those claims.

The UK's Investigatory Powers Act lays out a breathtaking array of surveillance powers. It authorizes the issuance of notices to communications service providers requiring them to retain data on the activities of all users. Government authorities will be able to access this data using a process called the "request filter." Described by the Act's proponents as a safeguard intended to ensure that the government obtains only relevant data, the request filter also serves as a federated search engine, allowing searches across multiple corporate databases without the need to ingest them into government coffers. On top of that, the Act unabashedly embraces the concept of bulk collection, explicitly authorizing the issuance of "bulk interception warrants" for the interception of communications between persons in the UK and persons overseas; "bulk acquisition warrants," which require telecommunications operators to disclose communications data (metadata); "bulk equipment interference warrants," which allow hacking to obtain "overseas-related" communications or information; and "bulk personal dataset warrants," authorizing intelligence services to retain and examine datasets where most of the information pertains to persons *not*, and who are unlikely to become, of interest to the intelligence service in the exercise of its functions.

Five weeks after the UK adopted its Investigatory Powers Act, the CJEU handed down its decision in the *Tele2* and *Watson* cases, ruling invalid under EU law the Swedish data retention mandate and a similar mandate under the UK law that had preceded the Investigatory Powers Act. The Court found that even the objective of fighting serious crime cannot in itself justify national legislation providing for the general and indiscriminate retention of all traffic and location data. National legislation that covers, in a generalized manner, all subscribers and all means of electronic communication as well as all traffic data "exceeds the limits

7. One of the authors of this volume, James X. Dempsey, served as a member of the Privacy and Civil Liberties Oversight Board. The views in this chapter and other chapters he coauthored in this volume are his own and do not represent the US government, the Board, or any Board Member.

of what is strictly necessary and cannot be considered to be justified, within a democratic society."[8] The Court held that the EU directive on communications data and the Charter of Fundamental Rights of the EU "must be interpreted as precluding national legislation which, for the purpose of fighting crime, provides for the general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication."[9] The Directive and the Charter, the Court stated, "do not prevent a Member State from adopting legislation permitting, as a preventive measure, the *targeted* retention of traffic and location data, for the purpose of fighting serious crime, provided that the retention of data is *limited*, with respect to the categories of data to be retained, the means of communication affected, the persons concerned and the retention period adopted, to what is strictly necessary."[10] The Court seemed to be saying, in essence, that generalized retention (and it would seem even more so, the generalized collection) of traffic data is never permitted, since by definition it is not limited as to "the persons concerned."

Separately, the CJEU considered the question of access to the retained data. General access to retained data cannot be regarded as limited to what is strictly necessary, it said. Instead, the national legislation concerned must be based on objective criteria in order to define the circumstances and conditions under which the national authorities are to be granted access to the data. In that regard, the Court said, "access can, as a general rule, be granted, in relation to the objective of fighting crime, only to the data of individuals suspected of planning, committing or having committed a serious crime or of being implicated in one way or another in such a crime."[11] Moreover, the Court ruled, "in order to ensure, in practice, that those conditions are fully respected, it is essential that access of the competent national authorities to retained data should, as a general rule, except in cases of validly established urgency, be subject to a prior review carried out either by a court or by an independent administrative body."[12]

So, at the end of nearly six years, we are left with movement simultaneously in the direction of both more government powers and an expanded assertion of human rights principles to curtail government powers. In the digital age it is increasingly clear that governments have legitimate reasons to collect data from the private-sector entities that provide communications and other services. At the same time, the power to compel disclosure must be subject to robust checks and balances, defined by a growing international consensus around the

8. Judgment of the Court (Grand Chamber), *Tele2 Sverige AB v Post-och telestyrelsen* and *Secretary of State for the Home Department v Tom Watson and Others* (December 21, 2016), para. 107, http://curia.europa.eu/juris/liste.jsf?num=C-203/15.

9. Ibid. para. 112.

10. Ibid. para. 108 (emphasis added).

11. Ibid. para. 119.

12. Ibid. para. 120.

principles of legality, proportionality, and accountability. Even when those critical protections are present, however, it is an increasingly important and difficult question whether bulk or indiscriminate collection by the government of personal data from the private sector can ever be compatible with those principles. And it is that critical question that this volume is designed to help the reader explore.

PART ONE

Country Reports

Overview

1

Systematic Government Access to Private-Sector Data

A Comparative Analysis

IRA S. RUBINSTEIN, GREGORY T. NOJEIM, AND RONALD D. LEE*

I. ABSTRACT

There has been an increase worldwide in government demands for data held by the private sector. In most, if not all countries studied, the publicly accessible law provides an inadequate foundation for systematic access, both from a human rights perspective and at a practical level. Transparency about systematic access remains weak. Access for national security purposes is more sparingly regulated than is access for criminal investigation purposes.

Relying on the country reports prepared for this project, this chapter develops both a descriptive framework for comparing national laws on surveillance and government access to data held by the private sector, and a normative framework based on factors derived from constitutional and human rights law.

A robust, global debate is needed on the standards for government surveillance, premised on greater transparency about current practices. International human rights law provides a useful framework for that debate.

II. INTRODUCTION

In recent years, there has been an increase worldwide in government demands for data held by the private sector, driven by a variety of factors. This increase

* The authors wish to thank Jake Laperruque and Christine Galvagna for their assistance in preparing this chapter for publication. Mr. Lee took no part in the preparation of any portions of this chapter referring to US government activities and programs.

includes an expansion in government requests for what we call "systematic access": direct access by the government to private-sector databases or networks, or government access, whether direct or mediated by the company that maintains the database or network, to large volumes of data. The June 2013 disclosures by Edward Snowden about systematic access programs conducted by the United States, the United Kingdom, and other countries dramatically illustrated the issue and brought it to the forefront of international debates.

Although it seems that systematic access is growing, there are also cases—in Germany and Canada—where government proposals for expanded access have been rejected due to public and corporate concerns about privacy, cost, and the impact on innovation.

Systematic access raises hard questions for companies that face demands for government access to data they hold. They must decide whether the demand or request is lawful, though the law may be vague. Companies must also decide what information about their responses to these demands they may disclose to their customers and to the public—the "transparency" issue that has received increased attention since June 2013 as discussed below.

This chapter identifies a number of common themes in the national laws on government surveillance and access to data held by the private sector of the 13 countries surveyed at the behest of The Privacy Projects. It presents a descriptive framework for analyzing and comparing these national laws. We also develop a normative framework based on a series of factors that can be derived from the concept of "rule of law," from constitutional principles, and from existing (although still evolving) international human rights jurisprudence.

Among our key findings are the following: First, we found that in most, if not all countries studied, existing legal structures provide an inadequate foundation for the conduct of systematic access, both from a human rights perspective and at a practical level. Transparency about systematic surveillance programs is weak, so we lack an accurate or comprehensive understanding of systematic access. Nevertheless, we found that the relevant laws are at best vague and ambiguous, and government interpretations of them are often hidden or even classified; that practices are often opaque (because it is sometimes in the interests of both governments and companies to proceed quietly, and the companies are often prohibited from public comment); and that oversight and reporting mechanisms are either absent or limited in scope when they exist, and generally do not reach voluntary data sharing. Transparency remained weak even after information about some systematic surveillance activity appeared in the press as a result of leaks of classified information by former NSA contractor Edward Snowden in June 2013 and even after changes in US law permitted companies to provide a limited amount of information about US law enforcement and national security processes.

Second, in every country we studied, even those nations with otherwise comprehensive data protection laws, access for regulatory, law enforcement, and national security purposes is often excluded from such laws; alternatively, they are treated as accepted purposes for which access is authorized under separate laws that may or may not provide adequate safeguards against possible abuses.

Moreover, almost everywhere, when it comes to data protection, access for national security purposes is more sparingly regulated than is access for law enforcement purposes.

Third, it seems overall there had been, until recently, relatively little discussion of the complex legal and political issues associated with asserting jurisdiction over data stored in other countries or relating to citizens of other countries. Also, until the Snowden revelations, discussion of the complex questions regarding extraterritorial application of human rights raised by trans-border surveillance had been lacking.

Fourth, although standards for real-time interception of communications for law enforcement purposes are high in most of the countries we surveyed (but not in India and China), standards for access to stored communications held by third parties are less consistent. When it comes to transactional data regarding communications, standards are even weaker.

Fifth, with respect to the standards for government access to communications in national security investigations, the overall picture is very complex. Almost half the countries studied do not have provisions requiring court orders for surveillance undertaken in the name of national security or for foreign intelligence gathering.

Finally, most countries handle travel and financial data under laws requiring routine, bulk reporting for specified classes of data.

This chapter proceeds as follows: Section III describes "systematic access" to data, highlighting evolving practices by governments across the globe. Section IV briefly describes the Snowden revelations. Section V considers the common themes emerging from an analysis of the law and practice of systematic access in the 13 countries the project surveyed.[1] Section VI sets forth a descriptive framework that can be used to analyze national laws that set standards for governmental access to privately-held data, whereas Section VII lays out a normative framework, based on human rights principles, and offers some comparative observations. Finally, Section VIII offers preliminary recommendations and next steps in responding to the challenges of systematic government access to private-sector data.

Here is our basic conclusion: in most if not all countries, existing legal structures provide an inadequate foundation for the conduct of systematic access, both from a human rights perspective and at a practical level. At the practical level, the law provides little guidance, leaving companies to fill the gaps with their own judgments. From the human rights perspective, the systematic access that many governments obtain is not foreseeable from the text of the law, calling into question whether the laws in those countries meet evolving human rights standards.

1. Over its lifetime, the project surveyed 13 countries. Twelve of those surveys are published in this volume, most of them updated to reflect recent developments. Because the UK law was completely rewritten late in 2016, there was insufficient time to update the UK chapter, and therefore there is no UK report in this volume.

III. WHAT IS SYSTEMATIC ACCESS?

Governments around the world have always demanded that commercial entities disclose data about their customers in connection with criminal investigations, enforcement of regulatory systems, and national security matters. Companies have always felt an obligation—and oftentimes are under legal compulsion—to cooperate, but they have also felt a business need and sense of responsibility to protect their customers' personal data and, in most cases, have diligently sought to balance those interests.[2] In recent years, there has been an increase worldwide in government demands for data held by the private sector, driven by a variety of factors. This has included an expansion in government requests for what we call "systematic access." We use this term to encompass both *direct access* by the government to private-sector databases, without the mediation or interaction of an employee or agent of the entity holding the data, and government access, whether or not mediated by a company, to *large volumes* of private-sector data.

Here are some examples of what we mean by systematic access to stored data, covering a very wide range of data and justifications:

- In the United States, a special court ordered certain telecommunications service providers to disclose to the National Security Agency (NSA), on a daily basis, metadata (number making the call, number called, time, duration) for all telephone calls handled by the carriers to, from, and within the country. The bulk disclosure orders were renewed every 90 days from 2006 to 2015, when Congress adopted legislation ending it.
- Although most countries have long-standing systematic reporting requirements of a regulatory or administrative nature, especially in the area of financial services and employment, mandatory reporting of income data and other data related to the administration of taxes has expanded in recent years.[3] In other countries, there is systematic reporting of hotel registrations or airline travel itineraries.
- In Germany, as Paul Schwartz outlines in his chapter in this volume, telecommunication providers are required to collect certain data about their customers, such as name, address, and telephone number, before the service is established. This information, termed "inventory information," is sent to a databank of the Federal Network Agency, and other governmental agencies can make automated requests for this information from the databank.
- The Chinese government maintains almost unlimited and unfettered access to private sector data, through a variety of regulatory requirements. As Zhizheng Wang observes in his chapter on China

2. "Personal data" generally refers to any data that relates or is linkable to an identifiable individual, and may include aggregations of data.

3. See, for example, Giorgio Resta's chapter on Italy in this volume.

in this volume, "the government's systematic access to data held by anyone will become possible and realistic with the evolution of the e-government strategy, in accordance with its vital interest of maintaining the state's control on information and 'preserving the stability' of the society."

- The Brazilian Communications Agency (ANATEL) can request metadata from service providers and also maintains the technical ability to directly access metadata.[4]
- In India, as Sunil Abraham explains in his chapter in this volume, the government is building a Central Monitoring System (CMS) that is intended to allow the government to engage in real-time interception of email, chats, voice calls, texting, without intervention of the service providers.[5]
- A 2015 French statute expanded the government's authority to obtain user data. Among other things, the government may demand that a provider automatically analyze all metadata it processes with algorithms to identify suspicious activity.[6]
- In the United Kingdom, the Investigatory Powers Act of 2016 mandates data retention by telecommunications service providers and expressly authorized the issuance of "bulk personal dataset warrants."[7]

We also found examples where, although the government requested records one at a time regarding particular individuals, devices, facilities, or accounts, the volume of requests was quite large. For example, in the UK, government agencies

4. Dennys Antonialli and Jacqueline de Souza Abreu, "State Surveillance of Communications in Brazil and the Protection of Fundamental Rights," *Electronic Frontier Foundation* (March 2016), at p. 37, https://necessaryandproportionate.org/files/brazil-en-march2016.pdf ("In performing its supervisory duties (article 8, Law no. 9472/97), ANATEL may access billing documents, which contain account information and call records, by requesting them from service providers. At present, there is infrastructure in place allowing direct and unlimited online access, pursuant to article 38, Resolução no. 596/12."); ibid., at 10.

5. Sneha Johari, "Govt's Central Monitoring System Already Live in Delhi & Mumbai," *Medianama* (May 11, 2016), http://www.medianama.com/2016/05/223-india-central-monitoring-system-live-in-delhi-mumbai/. See also Shalini Singh, "India's Surveillance Project May Be as Lethal as PRISM," *The Hindu* (June 21, 2013); Bharti Jain, "Govt Tightens Control for Phone Tapping," *The Times of India* (June 18, 2013); Anjani Trivedi, "In India, Prism-Like Surveillance Slips Under the Radar," *Time* (June 30, 2013), http://world.time.com/2013/06/30/in-india-prism-like-surveillance-slips-under-the-radar/.

6. Olivier Le Bot, "France under Mass-Surveillance? The French Constitutional Council and the Limits on the Intelligence Service's Powers," *ConstitutionNet* (Sept. 29, 2015), http://www.constitutionnet.org/news/france-under-mass-surveillance-french-constitutional-council-and-limits-intelligence-services.

7. Investigatory Powers Act, Parts 4 and 7, http://www.legislation.gov.uk/ukpga/2016/25/contents/enacted.

made 500,000 requests for telephony metadata in one year.[8] Paul Schwartz notes that, in Germany, where local police departments can request cell tower data about any person located in a given area during a specific time period, a Berlin newspaper reported in 2012 that the Berlin police since 2008 had made 410 "radio cell inquiries" that collected information pertaining to 4.2 million cell phone connections. In the United States, government agencies issued over 1.3 million demands to mobile carriers in 2011, covering information ranging from basic subscriber identifying data to call detail records to cell site location information to call content.[9] Directly comparable information for years since 2011 is not available, because the figure of 1.3 million demands was released by US Senator Edward Markey based on data several carriers reported to him. However, the transparency reports of just three of the largest US wireless carriers for recent years indicate that the volume remains substantial. Verizon reported 289,378 law enforcement demands for customer data, and AT&T reported 287,980 US criminal and civil demands for customer data in 2015. T-Mobile reported 339,270 federal, state, and local law enforcement requests in 2014.[10] The volume of requests can lead governments and private-sector entities to develop automated interfaces or other arrangements that facilitate high volume access.[11]

8. Ian Brown, "Government Access to Private-Sector Data in the United Kingdom" (2012) 2/4 *International Data Privacy Law* 230–38. For statistics on the volume of requests for retained transactional data in other European countries, see European Commission, *Report from the Commission to the Council and the European Parliament Evaluation Report on the Data Retention Directive (Directive 2006/24/EC)* (2011), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0225:FIN:en:PDF.

9. Eric Lichtblau, "More Demands on Cell Carriers in Surveillance," *New York Times* (July 8, 2012) (the figure of 1.3 million understated the volume as one major carrier did not disclose the number of requests it had received).

10. See *AT&T Transparency Report* (2016), http://about.att.com/content/dam/csr/Transparency%20Reports/ATT_Transparency%20Report_Jan%202016.pdf; *Verizon United States Report* (last visited April 27, 2017), http://www.verizon.com/about/portal/transparency-report/us-report/; *T-Mobile Transparency Report for 2013 and 2014*, https://newsroom.t-mobile.com/content/1020/files/NewTransparencyReport.pdf.

11. For example, it has been reported that one mobile operator in the United States established an online interface to allow law enforcement agencies to "ping" cell phones for location data. Kim Zetter, "Feds 'Pinged'Sprint GPS Data 8 Million Times over a Year," *Wired* (December 1, 2009). As Stephanie Pell notes in her chapter in this volume, the Department of Justice Inspector General reported several years ago that major telephone companies had placed their employees, with access to phone company databases, inside FBI offices in order to respond more quickly to FBI requests for metadata records. In 2013, the *New York Times* reported that AT&T was placing its employees "in drug-fighting units around the country. Those employees sit alongside Drug Enforcement Administration agents and local detectives and supply them with the phone data from as far back as 1987." See Scott Shane and Colin Moynihan, "Drug Agents Use Vast Phone Trove, Eclipsing N.S.A.'s," *New York Times* (September 1, 2013), http://www.nytimes.com/2013/09/02/us/drug-agents-use-vast-phone-trove-eclipsing-nsas.html?_r=0.

Although it seems that systematic access is growing, we also found cases where proposals for expanded access had been rejected. In Germany, in 2011, the federal government abandoned the proposed ELENA project, which was intended to streamline the collection of a wide variety of employee data into a central databank run by a government agency, containing name, date of birth, insurance number, home address, time missing work, and "possible misbehavior." In Canada in 2013 the government abandoned Bill C-30, which would have imposed various intercept capability and reporting requirements on communications service providers.

When this project began, it focused primarily on access to stored data held by businesses, distinct from real-time interception of communications. However, Snowden revealed information about systematic access to communications in transit such as the US government's MYSTIC program, which is capable of intercepting and storing for 30 days all phone calls made nationwide in certain countries.[12] A study for the European Parliament concluded that the practice of "upstreaming" (governmental surveillance accomplished by tapping into an entire communication stream, as opposed to receiving only particularized disclosures from communications service providers) appears to be a relatively widespread feature of surveillance by several EU Member States.[13] Just as most governments have long asserted the power to demand access to stored data held by businesses about their customers, so they have also asserted the power to intercept in real-time communications passing over networks of telecommunications service providers. Sometimes such interception is conducted with the cooperation of the service provider, sometimes without. The rules and practices surrounding real-time collection can be very complex, but in certain circumstances the electronic surveillance activities of governments have long entailed large scale or systematic collection of communications for later analysis, especially for national security purposes and especially when conducted outside—or targeted at persons outside—the intercepting nation's territory. As we discuss further below, the Snowden revelations suggest that the digital revolution has been accompanied by a growth in large-scale real-time interception. In addition, it appears that there is a growing overlap between access to stored data and real-time interception: it has been reported that the United States intercepts huge volumes of stored data in real time as it is shifted globally from server to server.[14]

12. Barton Gellman and Ashkan Soltani, "NSA Surveillance Program Reaches Into the Past to Retrieve, Replay Phone Calls," *Washington Post* (March 18, 2014), https://www.washingtonpost.com/world/national-security/nsa-surveillance-programme-reaches-into-the-past-to-retrieve-replay-phone-calls/2014/03/18/226d2646-ade9-11e3-a49e-76adc9210f19_story.html.

13. European Parliament Study, *National Programmes for Mass Surveillance of Personal Data in EU Member States and Their Compatibility with EU Law* (October 2013), http://www.statewatch.org/news/2013/oct/ep-study-national-law-on-surveillance.pdf.

14. Barton Gellman and Ashkan Soltani, "NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Documents Say," *Washington Post* (October 30, 2013),

Systematic access as we define it also relates to concerns over data retention and design mandates. Data retention refers to legal requirements that certain service providers collect and retain specific categories of information about the users and usages of their systems for a specified period of time (often ranging from six months to two years), so that the data is available to the government upon demand. Most recently, debates over data retention have focused on government proposals that telecommunications service providers (both traditional telephone and wireless operators and ISPs) maintain subscriber identifying information or connection data (such as customer billing information and dialed number information) for a set period of time.[15] Design mandates include requirements that service providers design their systems to be "wiretap ready," that is, to be capable of facilitating real-time or near real-time interception upon request.[16]

Our research into actual practices, although hampered by a lack of transparency, confirmed that governments are in fact increasingly turning to the private sector for information that they see as critical in countering criminal activity, terrorism, and other threats. The Snowden revelations dramatically reinforce this conclusion, augmenting it with new information regarding extraordinary programs of systematic collection in real time. The reasons for these trends are simple enough: to begin with, private sector firms hold an increasingly large amount of data about individuals collected in the course of ordinary commercial transactions or created by users and stored on cloud platforms, supplemented in some countries by data retention mandates. The volume of digital data routinely generated, collected, and stored about individuals' purchases, communications, relationships, movements, finances, and tastes is staggering. At least three developments have fed the growing government appetite for this information: First are concerns about new and dangerous threats to national security, demonstrated by terrorist attacks in New York, Washington, Madrid, London, Mumbai, Boston, Paris, San Bernardino, Brussels, Istanbul, Nice, and elsewhere, and compounded by the rise in militant Islamic fundamentalism. Second are more mundane interests in tax collection and other regulatory or administrative goals. The third major factor is the steadily growing ability of businesses and

https://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html.

15. Center for Democracy and Technology, *Data Retention Mandates: A Threat to Privacy, Free Expression and Business Development* (October 2011), https://www.cdt.org/files/pdfs/CDT_Data_Retention_Long_Paper.pdf.

16. In the United States, see Communications Assistance for Law Enforcement Act (CALEA), Pub L No 103-404, 108 Stat 4279, 4280–81, codified at 47 U.S.C. § 1002 (2000); in the UK, see Investigatory Powers Act 2016, § 253; see also Andrei Solatov, "Lawful Interception: The Russian Approach," *Privacy International* (March 5, 2013), https://www.privacyinternational.org/blog/lawful-interception-the-russian-approach (describing "SORM," Russia's nationwide system of automated and remote legal interception).

governments to analyze large data sets in search of useful insights, a development often summed up with the phrase "big data."[17]

Other commentators have observed that governments in the post-9/11 era are increasingly dependent on the private sector to assist them in collecting and analyzing data for national security purposes, and have applied various theories in analyzing these modes of cooperation.[18] Our focus on systematic access was, until recently, almost unique. So too was our effort to explore the issue not only from the perspective of the governments' needs or the countervailing civil liberties and human rights values but also from that of companies that are responding to governmental demands in numerous countries and are, therefore, caught in the middle between competing interests.[19] They must often make judgments about how to respond to demands for systematic access when the law governing access is vague and susceptible to many interpretations. Legal requirements, business concerns, licensing schemes, the views of their customers, and the need to be perceived as cooperative in matters involving public safety or national security all play a role.

IV. REVELATIONS OF SYSTEMATIC SURVEILLANCE ACTIVITIES

On June 5, 2013, *The Guardian* began publishing information regarding surveillance activities of the US National Security Agency, based upon the leaking of classified documents by former contract employee Edward Snowden. Further disclosures by *The Guardian* and other major news outlets followed, along with official US government releases of previously classified documents in response to FOIA litigation and public demands for transparency.

One of the surveillance programs described in these disclosures involved systematic access of exactly the kind this project has been concerned with: the ongoing, bulk collection by the NSA of metadata on a large percentage of telephone calls to, from, and within the United States. The program operated under Section 215 of the USA PATRIOT Act, which authorized the government to seek a court order for the production of records relevant to a foreign intelligence investigation.[20] Such orders required major telecommunications companies to

17. See Fred H. Cate, James X. Dempsey, and Ira S. Rubinstein, "Systematic Government Access to Private-Sector Data" (2012) 2 *International Data Privacy Law* 195.

18. See, for example, Michael D. Birnhack and Niva Elkin-Koren, "The Invisible Handshake: The Reemergence of the State in the Digital Environment," 8 *Virginia Journal of Law & Technology* 6 (2003); Jack M. Balkin, "The Constitution in the National Surveillance State," 93 *Minnesota Law Review* 1 (2008); Jon D. Michaels, "All the President's Spies: Private-Public Intelligence Partnerships in the War on Terror," 96 *California Law Review* 901 (2008); Jon D Michaels, "Deputizing Homeland Security," 88 *Texas Law Review* 1435 (2010).

19. See Albert Gidari, Jr., "Companies Caught in the Middle: Legal Responses to Government Requests for Customer Information," 41 *Univ. of San Francisco L. Rev.* 535 (2007).

20. 50 U.S.C. § 1861 (2010).

disclose to the NSA call detail records on all calls by all of their customers and included originating and terminating telephone number and time and duration of call but not the substantive content of any communications.[21] In 2015, the US Congress outlawed the program in the USA FREEDOM Act.[22] It did this by requiring that all collection of call detail records under Section 215 of the USA PATRIOT Act be based on a "specific selection term" such as a phone number. It established a procedure for intelligence authorities to provide those terms to major telecommunications companies, which then search their customer information for "hits" on those terms.

It was also revealed that the NSA conducted for many years a program of systematic collection of Internet metadata. That program was discontinued in 2011 due to an assessment by the NSA that it was ineffective as a counterterrorism tool.[23] The USA FREEDOM Act outlawed such programs by extending a specific selection term requirement to all of the authorities in which metadata can be collected for intelligence purposes in the United States, rendering illegal the bulk collection of communications metadata in domestic intelligence surveillance.

Snowden also disclosed documents describing activities of the US government, conducted under Section 702 of FISA, as adopted by the FISA Amendments Act of 2008 (FAA), involving the collection of the contents of communications.[24] Section 702 authorizes the collection from service providers inside the United States of foreign intelligence about persons reasonably believed to be outside the United States. Initial reports about a program referred to as PRISM cited a government PowerPoint presentation saying that the government was collecting "direct from the servers" of leading communications service providers.[25] The government and the companies involved have denied that there is any direct access to service provider

21. Foreign Intelligence Surveillance Court, *Primary Order* (July 19, 2013), http://www.uscourts.gov/uscourts/courts/fisc/br13-09-primary-order.pdf. See also Office of the Director of National Intelligence, *DNI Statement on Recent Unauthorized Disclosures of Classified Information* (June 6, 2013), http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/868-dni-statement-on-recent-unauthorized-disclosures-of-classified-information [hereinafter "DNI June 2013 Statement"].

22. USA FREEDOM Act of 2015, Pub. L. No. 114-23, June 2, 2015, Title I.

23. See Siobhan Gorman and Jennifer Valentino-Devries, "Details Emerge on NSA's Now-Ended Internet Program," *Wall Street Journal* (June 27, 2013), http://online.wsj.com/article/SB10001424127887323689204578572063855498882.html.

24. Barton Gellman and Laura Poitras, "US, British Intelligence Mining Data from Nine US Internet Companies in Broad Secret Program," *Washington Post* (June 6, 2013), http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-programme/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html. See "NSA Slides Explain the PRISM Data-Collection Program," *Washington Post* (June 6, 2013), http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/.

25. See "NSA Slides" above note 24.

computers.[26] However, another program conducted under Section 702 has some elements of systematic access, in real time. According to a report by the US Privacy and Civil Liberties Oversight Board, the NSA's UPSTREAM program acquires communications as they transit circuits that facilitate communications over the "Internet backbone."[27] Communications that contain a selector such as an email address and that are not domestic communications are ingested into government databases.[28]

Snowden also leaked documents disclosing systematic surveillance programs in the UK, including one called "Mastering the Internet" and another called "Global Telecoms Exploitation." According to *The Guardian*, Britain's "GCHQ [the UK's signals intelligence agency] has secretly gained access to the network of cables which carry the world's phone calls and internet traffic and has started to process vast streams of sensitive personal information."[29] In an operation code named TEMPORA, GCHQ stores large volumes of data drawn from fiber optic cables for up to 30 days so that it can be sifted and analyzed.[30] According to *The Guardian*, GCHQ is able to "survey about 1,500 of the 1,600 or so high-capacity cables in and out of the UK at any one time" and was capable of extracting and collecting information (both content and metadata) from 200 of those cables at a time.[31] According to *The Guardian*, citing official documents, as of 2011 GCHQ recorded 39 billion separate pieces of information during a single day. According to another document cited by *The Guardian*, GCHQ "produces larger amounts of metadata collection than the NSA." The tapping operations within Britain were done under agreements with the commercial companies that own the fiber optic cables.

The controversy surrounding the Snowden leaks prompted journalists and activists to write about similar programs in a number of countries. Press reports have revealed the following:

- Germany's foreign intelligence agency, the BND, was monitoring communications at a Frankfurt communications hub that handles

26. Declan McCullagh, "No Evidence of NSA's 'Direct Access' to Tech Companies," *CNet* (June 7, 2013), http://news.cnet.com/8301-13578_3-57588337-38/no-evidence-of-nsas-direct-access-to-tech-companies/.

27. Privacy and Civil Liberties Oversight Board [hereinafter "PCLOB"], *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* (July 2, 2014), p. 37, https://www.pclob.gov/library/702-Report.pdf.

28. Ibid., at pp. 36–37.

29. Ewen MacAskill, "GCHQ Taps Fibre-Optic Cables for Secret Access to World's Communications," *The Guardian* (June 21, 2013), http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa.

30. Ewen MacAskill, "Mastering the Internet: How CGHQ Set Out to Spy on the World Wide Web," *The Guardian* (June 21, 2013), http://www.theguardian.com/uk/2013/jun/21/gchq-mastering-the-internet.

31. Ewen MacAskill, "How Does GCHQ's Internet Surveillance Work," *The Guardian* (June 21, 2013), http://www.theguardian.com/uk/2013/jun/21/how-does-gchq-internet-surveillance-work.

international traffic to, from, and through Germany, presumably using the strategic monitoring authority described by Paul Schwartz in his chapter, and the BND is seeking to significantly extend its capabilities.[32]

- France runs a vast electronic spying operation using NSA-style methods, reportedly with even fewer legal controls.[33] A 2015 statute expanded the government's surveillance powers. Among other things, it authorizes the government to require service providers to apply algorithms to all metadata they process in order to identify suspicious activity, and also to make that data available to the government.[34]

V. COMMON THEMES FROM THE COUNTRY REPORTS

The 13 countries surveyed for this project were chosen based on a variety of factors that included availability of English language materials, scholars, and practitioners to analyze national law, and the size of the country in terms of economy and population. But caution should be exercised in extrapolating from this survey: among other limitations, the survey included not a single country in Africa or the Middle East (apart from Israel). Moreover, by being heavily weighted to democracies and to European democracies in general, with India and China as outliers, it may suggest more commonality of legal norms than would be found in a broader survey. With those significant caveats, the country reports analyzing

32. Staff, "The German Prism: Berlin Wants to Spy Too," *Spiegel Online* (June 17, 2013), http://www.spiegel.de/international/germany/berlin-profits-from-us-spying-programme-and-is-planning-its-own-a-906129-2.html; "German Intelligence Admits to Frankfurt E-Mail Tap," *Wall Street Journal* (October 9, 2013), http://blogs.wsj.com/digits/2013/10/09/german-intelligence-admits-to-frankfurt-e-mail-tap/ ("the German weekly Der Spiegel reported in this week's issue that the German intelligence service . . . has been tapping the giant De-Cix exchange point in order to spy on foreign targets for at least two years"). The program was ended after the Snowden revelations become public. Von D. Liedtke, W. Löer, U. Rauss, and O. Schröm, "BND-Chef verschwieg lange Operation Monkeyshoulder," *Stern* (June 2, 2015), http://www.stern.de/investigativ/operation-monkeyshoulder—bnd-chef-verschwieg-umstrittenes-ausspaehprojekt-vor-kanzleramt-6206512.html.

33. Jacques Follorou and Franck Johannès, "Révélations sur le Big Brother français," *Le Monde* (July 4, 2013), http://www.lemonde.fr/societe/article/2013/07/04/revelations-sur-le-big-brother-francais_3441973_3224.html; Angelique Chrisafis, "France 'Runs Vast Electronic Spying Operation Using NSA-Style Methods,'" *The Guardian* (July 4, 2013), http://www.guardian.co.uk/world/2013/jul/04/france-electronic-spying-operation-nsa.

34. Amar Toor, "France's Sweeping Surveillance Law Goes into Effect," *The Verge* (July 24, 2015), http://www.theverge.com/2015/7/24/9030851/france-surveillance-law-charlie-hebdo-constitutional-court.

the law and practice of systematic access identified a number of common themes about the countries examined:

- *Lack of Transparency*: Even after the Snowden leaks, systematic access is difficult to assess.
  - The relevant laws are at best vague and ambiguous, and government interpretations of them are often hidden or even classified.
  - Practices are often opaque; it is sometimes in the interests of both governments and companies to proceed quietly, and the companies are often prohibited from public comment.
  - Oversight and reporting mechanisms are either absent or limited in scope when they exist, and generally do not reach voluntary data sharing.

    In the United States, the Snowden revelations altered this imbalance in a profound way by publicizing the legal and technical details of several highly classified surveillance programs. The same is true to a lesser extent in the UK. The Snowden leaks also led to some further revelations about surveillance programs in other countries.

    But leaking is by its nature episodic and incomplete; even the most extensive leaks of classified documents can be misleading and are no substitute for structural and ongoing transparency mechanisms rooted in constitutional, legal, and political norms and supporting vigorous democratic oversight and debate. Outside the United States and the UK, the picture still remains very murky, although it is clear that systematic access occurs in many countries.[35]

    The shock expressed not only by civil society but also by government officials at the scope of systematic access as revealed by the Snowden revelations demonstrates how deeply these programs and legal interpretations were hidden from public scrutiny and democratic debate.[36] In the United States at least, the revelations accelerated an already growing corporate movement to demand transparency, that is, greater legal authority to disclose at least the number and type of government demands received and complied

35. European Parliament Study, *National Programmes for Mass Surveillance of Personal Data in EU Member States and Their Compatibility with EU Law* (October 2013), http://www.statewatch.org/news/2013/oct/ep-study-national-law-on-surveillance.pdf.

36. Justin Sink, "Patriot Act author "extremely troubled" by NSA phone tracking," *The Hill* (June 6, 2013), http://thehill.com/blogs/hillicon-valley/technology/303937-patriot-act-author-extremely-troubled-by-nsa-phone-tracking; Letter from Congressman F. James Sensenbrenner to Attorney General Eric H. Holder, Jr. (June 6, 2013), http://www.scribd.com/doc/146169288/Sensenbrenner-Letter-to-Attorney-General-Eric-Holder-RE-NSA-and-Verizon.

with, and companies also started taking steps to make surveillance without their consent more difficult.[37]

- *Significant Commonality across Laws*: Although differences abound, and can be significant, there is some commonality across most of the countries we surveyed:
  - Almost all have privatized their telecoms and thus recognize some arm's length relationship between the government and the network operators.
  - Almost all recognize the right to privacy.
  - However, most of the countries surveyed either exempt data collection for law enforcement and national security purposes from general data protection laws or treat government access as a permissible use, subject to separate, varying restrictions.[38]
  - Most countries impose a variety of limits and controls on government access and surveillance requests, whether by courts, senior government officials, or committees or oversight bodies established for this purpose.

    A major question, of course, is whether those control and review mechanisms are strong enough in the face of technological change, the continuing trend of individuals storing more and more of their digital persona in cloud-based computing models, and more aggressive government demands.

    Finally, with the exception of mandatory reporting laws, the applicable laws and regulations in the countries surveyed generally focus on defining standards for requests for data regarding specific persons, and they seem to presume a world of limited and particularized access rather than systematic government access. (The UK's Investigatory Powers Act and Germany's G-10 law specifically

37. Claire Cain Miller, "Angry over US Surveillance, Tech Giants Bolster Defenses," *New York Times* (October 31, 2013), http://www.nytimes.com/2013/11/01/technology/angry-over-us-surveillance-tech-giants-bolster-defenses.html.

38. The sole binding international treaty on data protection is the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, CETS No. 108 (1981), http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm. Convention 108 also permits states to enact laws that derogate from data protection responsibilities the Convention would otherwise impose. According to Article 9 of the Convention, such laws must be both necessary in a democratic society and be in the interest of protecting national security, public safety, the monetary interests of the state, or for suppressing crime. Accordingly, the European Court of Human Rights has used the Data Protection Convention to address criminal matters including collection and use of biometric identifiers of arrestees (*S. and Marper v. The United Kingdom*, Application nos. 30562/04 and 30566/04, Judgment of 4 December 2008)), and retention and disclosure of records of crime (*Gardel v. France*, Application no. 16428/05, Judgment of 17 December 2009, and *M.M. v. The United Kingdom*, Application no. 24029/07, Judgment of 13 November 2012).

authorize non-particularized interception of communications to or from persons abroad.) The Snowden revelations show how one of these laws (Section 215) had been interpreted in secret to authorize bulk, ongoing disclosures.

China and India stand out due to almost total lack of protection and oversight in both law enforcement and national security. At the opposite extreme, Japan and Brazil are notable for the severe limits they impose on interceptions undertaken for foreign intelligence security purposes.

- *Inconsistency between Published Law and Practice*: In many countries, the published law appears to say something different from what governments are reportedly doing. Even after the Snowden revelations, we lack an accurate or comprehensive understanding of systematic access because both its legal basis and actual practice are hidden from public view.

  As the disclosures about the US government's telephony metadata program show, governments may be operating under secret interpretations of the applicable laws. In other cases, they may be operating "in the interstices of national regulation," obtaining access that is not specifically authorized but also not specifically prohibited.[39] In the United States and in other democracies (especially Israel), the inconsistencies between publicly available laws and reported practice suggest areas of struggle or tension between legal requirements and perceived national security necessities. In light of these responsibilities to protect the nation against external and internal threats, the executive branch does not so much ignore existing law as rely on executive orders, secret court opinions, and other nontransparent means to interpret the law in the pursuit of the executive branch's objectives.[40] Additionally, after 9/11, several countries—notably Canada, Germany, the United States, and the UK—modified their antiterrorist statutes, hereby granting intelligence agencies more expansive surveillance powers.

  Again, China and India are different: the former explicitly carves out broad exceptions for national security from both the constitution and relevant security and surveillance laws, whereas privacy protections under Indian law are weak, ambiguous, or non-existent.
- *National Security and Law Enforcement*: In every country we studied, even those nations with otherwise comprehensive data protection laws,

39. See Cate, Dempsey, and Rubinstein, above note 17, at 198.

40. One of the documents leaked by Snowden indicates that, starting in 2004, the executive branch in the United States began to seek and obtain court approval for its bulk collection programs, bringing them under statutory authority, but based entirely on secret interpretations of those statutes. See "Draft NSA Inspector General Report on Email and Internet Data Collection, Dated 24 Mar. 2009," *The Guardian* (June 27, 2013), http://www.theguardian.com/world/interactive/2013/jun/27/nsa-inspector-general-report-document-data-collection.

regulatory, law enforcement, and national security access are often excluded from such laws, or treated as accepted purposes for which such access is authorized under separate laws that may or may not provide adequate safeguards against possible abuses.[41] Moreover, almost everywhere, national security access is more sparingly regulated for data protection purposes than requests for law enforcement purposes.

- *The Declining "Wall" between National Security and Other Uses*: Prior to the terrorist attacks of 9/11, many of the countries we studied maintained a "wall" that prevented law enforcement and other government agencies from obtaining and using data collected by intelligence or national security agencies under relaxed data protection standards. In many countries, this wall has been dismantled, with the result that intelligence agencies may now, at least as a matter of legal authority, pass information to law enforcement officials, while data collected for law enforcement and other purposes may be shared with intelligence agencies. This is certainly the case in the United States post-9/11; in Canada, where antiterrorism policy explicitly calls out the importance of information sharing among law enforcement and intelligence agencies;[42] and (more surprisingly) in Germany, where, as Paul Schwartz notes, recent laws have eroded the wall somewhat, thereby permitting the creation of an "anti-terrorist database."
- *"Systematic Volunteerism:"* In some of the countries studied, the government obtains systematic access to private sector information through voluntary arrangements. In Brazil, for example, as Bruno Magrani notes in his chapter in this volume, many companies such as Mercado Livre include in their terms of service permission to voluntarily disclose information to law enforcement. Companies establishing such arrangements appear motivated by a variety of factors, Magrani states, including "patriotism, a desire for good relations with government agencies (both for regulatory and sales purposes), a lack of understanding that national law does not require compliance with such requests, fear of reprisals if they do not cooperate, and the ability to generate revenue by selling the government access to the data they possess." In China, notes Zhizheng Wang, "private-sector entities might provide government officials with voluntary broad access to data in seeking favorable policy or government investment." An additional

41. Although national law often excludes national security and law enforcement from the scope of data protection laws, regional human rights instruments such as the European Convention on Human Rights do cover, and constrain, such activities. Adequate standards based on human rights instruments are discussed below in Section VI(B).

42. See Jane Bailey and Sara Shayan's chapter in this volume.

motivating factor for bulk disclosure may be efficiency (easing the administrative burden of processing many individualized requests). In the United States, by contrast, it seems that concerns about liability discourage voluntary cooperation.

- *Importance of Trans-border Access and Sharing:* Although most of the countries appear to consider multinational access and sharing essential to national security and law enforcement activities, these arrangements received relatively little attention in the chapters commissioned. Difficult jurisdictional issues cut across a wide spectrum of areas in the globalized information society. The Snowden leaks have drawn major attention to the fact that, with the emergence of globalized services, access in one country can easily affect large numbers of people outside that country. Increasingly, governments are exploring mechanisms that would permit law enforcement officials in one country to gain access in some circumstances to data stored in another country without triggering the host country's legal processes. For example, the United States and the UK are negotiating an agreement that would permit such access, with limitations,[43] and the US Department of Justice has proposed legislation that would clear the way for such agreements.[44] Separately, even before the Snowden leaks, several authors duly noted the existence of the UK-US agreement (which also extends to Australia, Canada, and New Zealand) to share information obtained by electronic surveillance, and recent leaks have exposed further details about this and other sharing and cooperation agreements.[45]

43. See Ellen Nakashima and Andrea Peterson, "The British Want to Come to America—with Wiretap Orders and Search Warrants," *Washington Post* (February 4, 2016), https://www.washingtonpost.com/world/national-security/the-british-want-to-come-to-america—with-wiretap-orders-and-search-warrants/2016/02/04/b351ce9e-ca86-11e5-a7b2-5a2f824b02c9_story.html.

44. See letter from Peter J. Kadzik, Assistant Attorney General, to Hon. Joseph R. Biden, President of the US Senate, conveying proposed legislation that would amend US law to permit foreign governments to make surveillance demands directly on US providers for communications content (July 15, 2016), https://www.documentcloud.org/documents/2994379-2016-7-15-US-UK-Biden-With-Enclosures.html#document/p11.

45. See Peter Beaumont, "NSA Leaks: US and Britain Team Up on Mass Surveillance," *The Guardian* (June 22, 2013), http://www.theguardian.com/world/2013/jun/22/nsa-leaks-britain-us-surveillance; Linton Besser, "Telstra Storing Data on Behalf of US Government," *Sydney Morning Herald* (July 16, 2013), http://www.smh.com.au/it-pro/security-it/telstra-storing-data-on-behalf-of-us-government-20130716-hv0w4.html; Glenn Greenwald, Laura Poitras, and Ewen MacAskill, "NSA Shares Raw Intelligence including Americans' Data with Israel," *The Guardian* (September 11, 2013), http://www.theguardian.com/world/2013/sep/11/nsa-americans-personal-data-israel-documents.

VI. COMPARATIVE ANALYSIS: THE DESCRIPTIVE FRAMEWORK

This chapter now presents a more detailed comparative analysis, proposing a set of descriptive and normative frameworks that might help governments, the private sector, privacy advocates, and other stakeholders confront the issues associated with government access to privately-held data in general and the issue of systematic access in particular. We approach this assessment with considerable humility. Comparative legal analysis is always difficult without an in-depth knowledge of the systems at issue, and in the context of systematic government access the task is made more difficult by the ambiguity in laws and lack of transparency in practices that we have repeatedly mentioned. Nevertheless, in the spirit of contributing to a more nuanced international dialogue around standards for systematic government access, we offer some comparative observations.

We first offer a descriptive framework for government access laws. Using this framework, we have attempted to summarize the laws of the 12 of the 13 countries surveyed by TPP.

In Section VII, we offer a normative framework, drawing on widely-accepted understandings of "the rule of law" and on the case law of the European Court of Human Rights, which represents a comprehensive transnational body of law on government surveillance.

A. The Descriptive Framework

In researching governmental access rules and practices, we found that most legal systems had addressed separately the questions of government access to communications and metadata associated with communications, and to business records of various types. The laws relating to access to communications and communications metadata seem to have grown out of an almost universal recognition of two competing propositions: that communications privacy is an essential right, and that the ability to intercept communications in real time or to access communications and associated data in storage is an important investigative technique for both criminal investigations and the protection of national security interests. Accordingly, most countries seem to have laws addressing communications privacy and governmental access to communications. Whether those laws have kept pace with technological development is another question. However, we found that certain basic issues presented themselves time and again across different legal systems. For example: Are there separate rules for law enforcement and national security access? Is judicial or senior level executive approval required for access? Are companies subject to data retention or network design mandates?

As a framework for cross-border comparisons of government laws regulating access to communications and associated metadata, we identified nine recurring

factors. Table 1.1 outlines nine factors to consider in describing a country's legal system for government access to private-sector data:

Table 1.1. The Descriptive Framework

1. Source of authority, standards and limits a. Constitutional—Does the national constitution include a protection of privacy or other limits on governmental power to obtain communications or other customer data from private-sector entities? b. Statutory—Are standards for governmental access established in statute? c. Law enforcement versus national security—Does the legal system set separate rules for law enforcement access as compared to national security access?
2. Distinction between content and non-content—Does the legal framework draw a distinction between the content of communications and transactional data (addressing or routing data, subscriber identifying data, financial data, data about commercial transactions)?
3. Technology neutrality (same standards for different media)—Do legal standards apply consistently to data collected online and offline? To data in transit and data in storage?
4. Targeted versus bulk access—Does the legal framework (outside of the regulatory context) expressly draw a distinction between targeted collection and systematic or bulk collection? Is there express authorization for bulk collection?
5. Third party doctrine—Does the legal system treat data stored with a third party (for example, a cloud provider) differently from data stored locally?
6. Use, retention, disclosure limits—Does the law impose limits on the government's use, retention, and disclosure of data after the data is lawfully acquired?
7. Oversight mechanisms—What are the executive, judicial, legislative oversight, public transparency, and redress mechanisms?
8. Design mandates—Does the law require service providers to design their networks or activities to facilitate government access? Does the government regulate encryption?
9. Retention mandate—Does the law require entities to store certain data about customers for specified periods of time?

Of course, as we noted above, government demands for access to data, including for systematic access, are directed at many other sectors, particularly financial services and travel. Accordingly, we sought to analyze laws and practices in the 13 countries we surveyed in terms of standards for government access to other types of business records. This task proved much more difficult, because in many countries, even those with otherwise comprehensive privacy laws, rules on government access to data and on systematic reporting may differ sector by sector. Table 1.2 lists 14 factors that constitute a normative framework for assessing national laws and practices concerning access to personal data held by the private sector.

We summarize laws and practices considering the following factors:

Table 1.2. Government Access to Business Records

1. Different rules for different sensitivity of data a. Location b. Travel c. Financial d. Other (specify)
2. Systematic disclosure demands
3. Use, retention, disclosure limits
4. Oversight mechanisms
5. Redress/due process mechanisms
6. Transparency
7. Automatic disclosure mandates
8. Retention mandate

B. The Descriptive Analysis: Comparative Observations

The following section highlights the similarities and differences in the government access rules in the countries studied. The discussion touches on both standards for real-time access and standards for access to stored data, and focuses mostly on communications content and metadata, in part because of the ongoing intensive governmental, public, civil society, and media focus on these matters, rather than on other forms of business records, where the issues are also important and inherently transnational. Unless otherwise noted, the descriptions of each country's law are drawn from the country reports that follow in subsequent chapters of this volume.

1. Source of Authority, Standards and Limits

a. Constitutional Authority

The majority of countries surveyed recognize the right to privacy in their national constitutions, with the exception of Australia and the UK. Whereas the constitutions of some countries include an explicit privacy provision, in other countries, courts have inferred a right to privacy from other constitutional provisions. Both the United States and Canada apply a "reasonable expectation of privacy" test to define the scope of that right vis-à-vis the government. In Germany and Israel, the constitutional basis of information privacy is especially strong. Germany recognizes a constitutionally based "right of informational self-determination," and a highly engaged German public and press ensure that such rights are taken very seriously. In Germany, for example, intrusions on privacy require a valid basis in law and must satisfy a principle of proportionality. Similarly, privacy in Israel is a constitutional right subject to a "limitation clause," with the result that government access must be expressly authorized and pass constitutional muster, including a proportionality test.

However, in all of the countries studied, the application of constitutional standards is by no means an absolute bar against government access to private sector data. To the contrary, governments enjoy substantial powers to collect or intercept data, under a variety of laws and programs. In the United States, a major exception to the right to privacy is the third-party doctrine (discussed below), which leaves business records outside the Constitution's protection. In Germany and Israel, access laws have been upheld even after the courts applied balancing tests that heavily weigh the fundamental right to privacy. As noted above, article 8 of the European Convention tolerates secret surveillance in signatory states (Germany, the UK, France, and Italy) provided that national laws provide adequate safeguards against potential abuse. In Brazil, however, at least one judicial decision suggests, as Magrani explains, that article 5, item XII of the Constitution (secrecy of correspondence, telegraphic data, and telephone communications) protects the flow of data even against judicially authorized wiretapping.

In sharp contrast, China stands out among the 13 countries surveyed in two fundamental respects: first, it is the only non-democratic country; second, its constitution (and laws) grant extensive surveillance powers to the state for purposes of national and public security. Thus, the government has extensive authorities and "generous room for flexibility" in accessing private data in the name of maintaining state security and the social order.[46] In India, too, although India is a democracy, the constitution imposes few meaningful limits on the government's broad surveillance powers.

b. Statutory Authority

Australia, Canada, Israel, Japan, South Korea, and all of the European counties have comprehensive national privacy statutes. The United States has no omnibus privacy law, but rather follows a sector-specific approach, with separate laws protecting communications data, financial data, health data, and other categories. In addition, international treaties can also be an overlapping source of legal authority for privacy, including Article 8 of the European Convention on Human Rights and Article 11 of the Inter-American Convention on Human Rights.

However, in all the countries surveyed, whether the nation has a comprehensive privacy statute or sectoral laws, those statutes have exceptions permitting government surveillance of communications and government access to stored records. Real-time surveillance is addressed in the majority of countries (other than China and India) in surveillance laws whose principles and concepts generally fit within the descriptive and normative frameworks outlined above.

Against this commonality of approach, China and India stand out among the 13 countries surveyed. In China, it is very easy to override existing statutory restrictions on national security or public order grounds. Thus, Chinese law explicitly authorizes governmental access to privately held data and/or lacks explicit

46. As Zhizheng Wang explains, in his chapter in this volume, Chinese government access to private sector data is further strengthened by the Chinese Communist Party's "absolute control over the law" and the absence of an independent judiciary.

limitations on such access. Indeed, Chinese national security law allows for the inspection of electronic communication instruments belonging to "any organisation or individual" for purposes of state security with few if any limitations.[47]

Indian surveillance laws also have very limited or very weak restrictions on government access. Although a 1997 decision established certain safeguards under India's long-standing Telegraph Act of 1885 governing telephone interception, the Information Technology Act of 2008 substantially weakened existing standards. It permits interception of electronic communications to prevent "incitement" of any cognizable offense related to public emergency, public safety, and public order, or for investigation of any offense as well as for a range of cyber security purposes. Under the relevant rules, intermediaries must provide a high degree of assistance to law enforcement, agencies can freely share data, and the rules relating to the collection of traffic data also permit extensive monitoring for cyber security matters. India's ISP licensing system also permits extremely broad government access rights while neglecting well-established international safeguards such as requiring a court order, internal agency restrictions on access to intercepted materials, and individual redress.

Among the countries we studied, Israel faces unique national security concerns.[48] Both the courts and the attorney general (which in Israel is a nonpolitical and highly autonomous function) play a key role in interpreting a set of laws that deal with surveillance by both the police and by the various intelligence services (military intelligence, internal security (GSS), and foreign intelligence (Mossad). The Israeli intelligence services enjoy far more leeway than the police in conducting surveillance. For example, as Omer Tene explains, the Wiretap Act allows military intelligence and GSS to obtain wiretap permission from a very senior official without judicial oversight. The Communications Data Act regulates access to traffic data by the police under multiple tracks, some of which require judicial oversight and some of which do not. In contrast, GSS (which is regulated by a separate law) has much broader access without judicial scrutiny. This includes a requirement that fixed line and cell operators must transfer to GSS certain categories of communications data as determined by the prime minister.[49] Although concerns about law enforcement access have sometimes

47. Although security officials must follow their own internal procedures, these procedures are largely secret and give rise to no due process rights.

48. We agree with Omer Tene, who notes in his chapter in this volume that his account must be qualified by two distinctions: first, it concerns only "Israel proper" and not the occupied territories, which are subject to a military regime; second, Israel has been in a near constant state of war or armed conflict since its beginnings as an independent state, and therefore national security considerations "have a profound impact on Israeli constitutional and legal discourse."

49. These transfers to the GSS are subject to certain "secret annexes" setting out detailed procedures and protocols. Omer Tene notes in his chapter in this volume that, after examining the secret annexes in camera, a court denied a public records request seeking their release on the grounds that they "do not provide the GSS with surveillance powers, but rather set forth

spawned government inquires and public outcry, the press and the public seem more acquiescent with regard to access for internal security purposes. On the other hand, Tene notes, the law regulating GSS imposes certain accountability and transparency requirements.

c. Law Enforcement versus National Security

The majority of countries have enacted separate laws or separate procedures addressing access in the domestic law enforcement context as opposed to national security (or foreign intelligence) activity. In the UK and other countries, the rules for both arenas are set out in a single law (now the Investigatory Powers Act of 2016), whereas the United States applies quite different standards in the two arenas through separate statutes—the Wiretap Act and the Stored Communications Act for law enforcement and FISA for foreign intelligence. In India, there is no clear distinction between law enforcement and national security access, whereas China distinguishes them but imposes few if any restrictions on the latter. Although Australia,[50] Canada, and the United States apply special, arguably more lenient rules to national security access, these rules remain subject to constitutional limitations.

At the opposite extreme is Japan, where the government's statutory authority to engage in surveillance either for law enforcement or intelligence purposes is very limited as compared with all of the other countries studied. Although Japan enacted its first wiretap law in 1999, Japanese society strongly disfavors the use of wiretaps and the number of communications intercepts is miniscule. Moreover, Japanese law lacks any statutory basis for authorizing wiretaps for counterterrorism purposes. Similarly, the Brazilian constitution only authorizes interception of communications for criminal investigations, and although Brazil maintains an intelligence apparatus, the lead intelligence agency lacks both investigative and surveillance powers.

2. Content/Non-content Distinction

A number of countries (Australia, Brazil, Canada, Germany, Italy, Israel, South Korea, the UK, and the US) draw a legal distinction between the content of communications and various types of non-content,[51] establishing higher standards for government access to the former and lower standards for access to the

technical specifications for operating the 'pipe' through which the data are channeled strictly where access to data is authorised by law."

50. For example, federal police are entitled to obtain documents that are "relevant to, and will assist in, investigations of serious terrorism offenses," without any court order. Similarly, the Australian Security Intelligence Organization (ASIO) may obtain computer access by requesting the Minister to issue a warrant.

51. "Non-content" data, also referred to as "transactional," "connection," or "envelope" data, includes both (a) communications attributes such as the time, duration, and medium of communication; the technical parameters of the relevant transmission devices and software; and the identities and physical locations of the parties, and their electronic

latter. For example, Brazilian courts have ruled that "judicial authorisation is not required for the Police or the Public Prosecutor's Office to have access to subscriber-identifying data from companies," on the grounds that anonymous speech is constitutionally prohibited. British law imposes very few controls on access to non-content data (both communications attributes and subscriber data), which are easily accessible by a very large number of central and local officials, simply requiring that a senior official make a request. There were over half a million such requests in 2010.[52] Similarly, non-content requests are subject to lower standards in Australia, Brazil, Israel, Italy, South Korea, and the United States. On the other hand, it appears that neither India nor Japan distinguishes between content and non-content requests.

3. Technology/Business Model Neutrality

Most of the countries studied apply the same standards for real-time interception of content (voice communications, text messages, email, and so on) regardless of the technology on which the content is transmitted or the business model of the service provider, with three exceptions. China has enacted multiple, Internet-related laws regulating very specific services (e.g., traditional ISPs, telecoms, content providers, data centers, messaging services, news services, etc.). Germany follows a "layer model" that draws complex distinctions between the content of online communication, the services provided on the Internet, and the "levels" at which data transfer takes place, all of which are regulated under different laws. Finally, the United States distinguishes between communications in real time and in storage and protects them differently.[53]

4. Third Party Doctrine

In the United States, there is long-standing precedent that the Constitution's Fourth Amendment, which protects against unreasonable searches and seizures, does not apply to records held by third parties.[54] Accordingly, in the United States, privacy protection for business records mainly flows from statute.[55] The

addresses; and (b) subscriber data such as name, address, phone number, and/or credit card information.

52. Brown, above note 8, at 235.

53. A campaign is underway in the United States to reform ECPA by extending to stored communications content many of the protections that apply to content in transit. See Dustin Volz, "U.S. House Passes Bill Requiring Warrant to Search Old Emails," *Reuters* (February 6, 2017), http://www.reuters.com/article/us-usa-congress-emails-idUSKBN15L2N3.

54. Fourth Amendment protections are unavailable both for financial records, see *United States v. Miller*, 425 U.S. 435 (1976), and transactional information held by third parties that is associated with either phone calls or email, see *Smith v. Maryland*, 442 U.S. 735 (1979).

55. In 2010, a federal appeals court (covering four states) held that the Constitution does in fact protect the content of stored communications. See *United States v. Warshak*, 631 F. 3d 266 (6th Cir. 2010). In 2013, the US Department of Justice stated to Congress that it followed the Warshak rule nationwide, obtaining a warrant under the Constitution in order to compel

United States is more or less unique in affording no constitutional protection to third-party data, although a few other countries also handle third-party data somewhat differently. For example, in Canada, a reasonable expectation of privacy does not attach to information held by a third party with no obligation to maintain confidentiality.[56] China, on the other hand, seems to accord *higher* protection to data stored in the cloud, apparently in an effort to attract international investors who might otherwise be wary of the "golden shield" projects (discussed below).

5. Use, Retention, Disclosure Limits

The European countries in the survey have all implemented the 1995 EU Data Protection Directive,[57] which limits collection, retention, and disclosure of personal data by the public and private sectors. However, the Directive expressly does not apply to processing of data for law enforcement or national security purposes. Israel also has a comprehensive privacy law but it too does not apply to the activities of the police or internal or external security services. Canada and the United States have Privacy Acts that regulate the collection, use, and retention of personal data by federal governmental entities; those Acts apply to law enforcement and intelligence agencies, but the US law allows many exceptions for law enforcement and intelligence databases. Key provisions of South Korea's comprehensive data protection law do not apply to data collected for national security purposes. In 2014, Brazil enacted the Marco Civil law, which allows the government to require companies to retain connection records for Internet applications for one year, and other Internet connection records for six months.[58] A draft data protection law has been under consideration in India,

a service provider to disclose the contents of stored communications. In a 2011 decision, the US Supreme Court rejected the absolute claim that a person loses all constitutional interest in whatever is disclosed to a third party, see *United States v. Jones*, 565 U.S. 400 (2012); however, the majority's holding was much narrower and the third party doctrine is still being applied in full force to non-content data.

56. See the chapter by Jane Bailey and Sara Shayan in this volume, n. 55 at 209.

57. Available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:NOT. On January 25, 2012, the European Commission proposed a comprehensive reform of the data protection rules, to account for globalization, cloud computing, and other advances in communications technology. After four years of drafting and negotiation, the European Parliament voted to adopt the new General Data Protection Regulation [hereinafter "GDPR"] on April 14, 2016, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=EN. The GDPR entered into force on May 25, 2016, and will become directly applicable in all EU Member States two years after this date, on May 25, 2018.

58. Marco Civil da Internet (Law No. 12.965), Articles 13 and 15 (April 23, 2014); Diego Spinola, "Brazil Leads the Efforts in Internet Governance with Its Recently Enacted 'Marco Civil da Internet'. What's in It for Intermediary Liability?," *The Center for Internet and Society* (April 30, 2014), http://cyberlaw.stanford.edu/blog/2014/04/brazil-leads-efforts-internet-governance-its-recently-enacted-marco-civil-da-internet.

whereas the Chinese legislature in 2013 passed a data protection resolution. Although that Chinese law contains "significant and far-reaching requirements applicable to the collection and processing of electronic personal information via the Internet,"[59] it obviously does not impose any meaningful limits on government access for security purposes.

6. Oversight Mechanisms

Each country except China has some process of independent oversight of surveillance and government access. However, standards vary widely. In India, courts play a very limited role. Although older laws required a court order for access to letters and telegrams, Sunil Abraham finds that these safeguards are "no longer relevant in today's information society." More recent enactments in India offer much weaker protections and seem to minimize the role of courts in authorizing wiretaps, access to non-content data, and access for national security reasons. In particular, the Information Technology Act of 2008 dispenses with case-by-case authorizations for access to data in favor of blanket authorizations, and permits the use of such data for broad and generic purposes. India also suffers from problems with corruption, and there are reports that "law enforcement officials abuse their positions to dilute data access safeguards." In Germany, prior judicial approval is required for wiretapping by the police in criminal cases, but interception for intelligence purposes is conducted upon the approval of the Interior Minister and a commission appointed by Parliament.[60] Germany's Constitutional Court has played a key role in overseeing the surveillance activities of Germany's foreign intelligence agency, the BND, forcing several amendments to the G-10 statute that regulates so-called "strategic surveillance" for intelligence purposes. In the United States, prior court approval is required for both law enforcement and foreign intelligence surveillance conducted inside the United States, with one exception that has loomed large after the Snowden leaks: when surveillance conducted inside the United States targets noncitizens who are believed to be outside the United States at the time of the access, the courts approve only the broad outlines of the surveillance program, and individual targeting decisions are made by the NSA.

7. Design Mandates

As far as we know based on the country chapters and additional research, only a few of the countries studied have explicit design mandates. For example, Israel, Australia, Germany, and the United States have enacted laws authorizing

59. See "Chinese Legislature Passes Data Privacy Resolution," (January 2, 2013), *Privacy and Information Security Law Blog*, http://www.huntonprivacyblog.com/?s=china (also noting that "one provision . . . could actually erode the protection of personal privacy: ISPs must require that customers provide their real names on agreements for the provision of access- or information-related services").

60. § 3, § 5 Artikel 10-Gesetz, http://www.gesetze-im-internet.de/bundesrecht/g10_2001/gesamt.pdf.

government officials to seek changes to the design of telecom equipment, facilities, and services to ensure that they have built-in surveillance capabilities. In the UK, the government may impose obligations on public telecom services to ensure that they maintain interception capability.[61] China and India have sought to control network design without explicit statutory authority. Although China has undoubtedly succeeded, the results in India are more ambiguous.[62] In other countries, the issue has not surfaced in public debate, perhaps due to the close relationship between government authorities and service providers, with the latter voluntarily taking steps to ensure that their facilities are wiretap-ready.

8. Retention Mandates

A few of the countries studied have imposed data retention mandates on telephone companies, ISPs and other service providers. The UK, France, Italy, and Germany enacted data retention laws as required by the EU Data Retention Directive, but in 2014 the Court of Justice of the European Union invalidated the Data Retention Directive, finding it inconsistent with the European Charter of Fundamental Rights.[63] In 2016, the Court invalidated the specific data retention laws of the UK and Sweden. The German statute required telecommunication providers to store specific kinds of traffic and location data for a period of six months. In 2010, the German Constitutional Court struck down the statute. However, Germany in 2015 enacted a new law that requires the retention of phone and Internet metadata for 10 weeks.[64] China imposes extensive mandatory data retention on telecoms, ISPs, and content providers. In Brazil, companies must retain connection records for Internet applications for one year, and other Internet connection records for six months.[65] Our research indicated that Canada, Japan, and the United States lack generalized data retention mandates.

61. The British design mandates are part of the Investigatory Powers Act 2016, which has broad surveillance provisions, a design mandate akin to CALEA, and a data retention requirement.

62. India, as well as the United Arab Emirates and Saudi Arabia, threatened to block Blackberry enterprise service because the service uses encryption that thwarts communications monitoring. Barry Meier and Robert F. Worth, "Emirates to Cut Data Services of BlackBerry," *New York Times* (August 1, 2010), http://www.nytimes.com/2010/08/02/business/global/02berry.html?pagewanted=all&_r=0. In response, BlackBerry (then operating as Research In Motion, or RIM) established a facility in Mumbai to coordinate with the government on surveillance demands relating to BlackBerry devices. Amol Sharma, "RIM Facility Helps India in Surveillance Efforts," *Wall Street Journal* (October 28, 2011), http://online.wsj.com/news/articles/SB10001424052970204505304577001592335138870.

63. *Digital Rights Ireland v. Minister for Communications*, Joined Cases C-293/12 and C-594/12, Judgment of 8 Apr. 2014, http://curia.europa.eu/juris/document/document.jsf?docid=150642&mode=req&pageIndex=1&dir=&occ=first&part=1&text=&doclang=EN&cid=593504.

64. "German Parliament Votes for New Data Retention Law," *Deutsche Welle* (October 16, 2015), http://dw.com/p/1GpBZ.

65. Marco Civil da Internet (Law No. 12.965), Articles 13 and 15 (April 23, 2014).

VII. COMPARATIVE ANALYSIS: THE NORMATIVE FRAMEWORK

A. The Normative Framework

In this section, we turn from a description of government access rules to the normative question of how national rules measure up against the standards for surveillance identified by the European Court of Human Rights.

Government surveillance demands, whether for access to one account at a time or for systematic access, and whether for regulatory, law enforcement, or national security purposes, do not arise in a normative vacuum. A series of factors for assessing governmental demands can be derived from the concept of "rule of law" and from existing (although still evolving) international human rights jurisprudence.

The "rule of law" is an internationally recognized concept encompassing, at a minimum, principles of transparency, limits on the discretion of government officials, and accountability.[66] A leading legal philosopher, Joseph Raz, identified eight key principles of the rule of law, of which six are especially relevant to questions of government surveillance and access to data held by the private sector:

1. Laws should be prospective, open, and clear;
2. Laws should be relatively stable;
3. The rules for making particular laws should be open, stable, clear, and general;
4. The judiciary should be independent;
5. Courts shall have review power over all other principles; and
6. "The discretion of the crime-preventing agencies should not be allowed to pervert the law."[67]

These principles have been embodied in major international human rights instruments. In addition, major human rights instruments protect the right to privacy.[68] Of greatest relevance, because it has generated the largest body of

66. For a classic statement of these principles, see Lon Fuller, *The Morality of Law*, revised edition (1969).

67. Joseph Raz, 'The Rule of Law and Its Virtue,' in *The Authority of Law: Essays on Law and Morality* (1979). Raz's other two principles address the need for making courts easily accessible to all and the necessity of observing principles of natural justice.

68. In 2013, the UN General Assembly passed a resolution reaffirming the human right to privacy as provided in Article 17 of the International Covenant on Civil and Political Rights, and requesting the UN High Commissioner for Human Rights to present a report on the protection of privacy regarding "domestic and extraterritorial surveillance and/or interception of digital communications and collection of personal data, including on a mass scale." *The right to privacy in the digital age*, G.A. Res. 68/167, U.N. Doc. A/RES/68/167 (Dec. 18, 2013), http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/167. Data Protection officials meeting at a major conference in Warsaw, Poland, adopted a resolution calling for

interpretative case law setting out standards of global relevance, is Article 8 of the European Convention on Human Rights (1950), which states in relevant part:

1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.[69]

The Convention is in effect binding on EU Member States, as Article 6(3) of the Treaty on European Union states, "Fundamental rights, as guaranteed by the European Convention for the Protection of Rights and Fundamental Freedoms ... shall constitute general principles of the Union's law."[70] The European Court of Human Rights (Strasbourg Court), whose decisions are binding on the 47 Member States of the Council of Europe, has issued multiple rulings on the applicability of Article 8 to secret systems of surveillance.[71] Although the Convention preceded the Internet by many years and does not explicitly contemplate modern means of communication, the Strasbourg Court has successively applied Article 8-1 to telephone conversations,[72] telephone numbers,[73] computers,[74] and the Internet and email.[75] The Court has held that the existence of legislation that allows a system of secret monitoring entails a threat

governments to adopt an additional protocol to Article 17 to create global standards for data protection. See https://privacyconference2013.org/web/pageFiles/kcfinder/files/5%20International%20law%20resolution%20EN%281%29.pdf.

69. Article 8, *European Convention for the Protection of Human Rights and Fundamental Freedoms* [hereinafter the "Convention"], http://conventions.coe.int/Treaty/en/Treaties/Html/005.htm. Article 7 of the EU Charter reproduces but slightly updates the wording of article 8(1): "Everyone has the right to respect for his or her private and family life, home and communications." See *Charter of Fundamental Rights of the European Union of the European Parliament*, Dec. 7, 2000, *O.J.,* No. C 364, 20000, p. 1 et seq.

70. *Consolidated Version of the Treaty on European Union,* art. 6(3), October 26, 2012, 2012 O.J. (C 326) 19.

71. For an overview, see R. White and C. Ovey, *Jacobs, White and Ovey: The European Convention on Human Rights* 365–71 (2010).

72. *Klass and others v. Germany,* Application no. 5029/71, Judgment of 6 Sept. 1978, § 41.

73. *Malone v. United Kingdom*, Application no. 8691/79, Judgment of 2 Aug., 1984, § 84*; Copland v. the United* Kingdom, Application no. 62617/00, Judgment of 3 Apr., 2007, § 43.

74. *Leander v. Sweden,* Application no. 9248/81, Judgment of 26 Mar., 1987, § 48*; Rotaru v. Romania,* Application no. 28341/95, Judgment of 4 May, 2000, § 42–43.

75. *Copland*, above note 73, § 41.

of surveillance for all those to whom the legislation may be applied, and that this threat itself amounts to an interference with rights under Article 8, allowing persons to invoke the Court's jurisdiction even if they cannot prove that they themselves have been subjected to surveillance.[76] In addition, the Court has held that the sharing of data with other government agencies, which enlarges the group of persons with knowledge of the personal data intercepted and can lead to investigations being instituted against the persons concerned, constitutes a further separate interference with Article 8 rights.[77]

Once it is determined that surveillance of a given form of communication constitutes interference with the rights guaranteed by Article 8-1, the Court next considers whether the interference is justified under Article 8-2 by assessing it in light of three tests: First, is it "in accordance with the law"? Second, is it pursued with one or more legitimate aims (including national security) in mind? And, third, is it "necessary in a democratic society"? The Court's decisions have enumerated specific criteria for applying these standards.

A very clear statement of these criteria is found in the *Weber and Saravia* case,[78] which examined "strategic surveillance" under Germany's G-10 Act.[79] In deciding that the G-10 Act did not violate Article 8, the Strasbourg Court first reiterated that the expression "in accordance with the law" has two elements: It requires (1) "that the impugned measure should have some basis in domestic law." It also refers, the Court said, to (2) "the quality of the law in question, requiring that it should be accessible to the person concerned, who must, moreover, be able to foresee its consequences for him, and compatible with the rule of law."[80]

In *Weber and Saravia*, the Court found that the German law readily satisfied the "basis in law" requirement. As to the foreseeability requirement, the Court said that, in the context of surveillance, this does not require any self-defeating form of notification that would allow an individual to adapt his conduct accordingly to avoid interception of his communications. Rather, the Court said, in view of the risks of the arbitrary exercise of secret powers, it is essential to have detailed rules that are clear enough to give citizens "an adequate indication" as to

76. *Roman Zakharov v. Russia,* Application no. 47143/06, Judgment of 4 Dec., 2015, § 171. Such interference is conditioned on an individual being able to show that, due to his personal situation, he is potentially at risk of being subjected to such measures and that no effective remedies are available at the national level. See also *Association for European Integration and Human Rights and Ekimdzhiev) v. Bulgaria*, Application no. 62540/00, Judgment of 27 June, 2007 (examining the adequacy of Bulgaria's "Special Surveillance Means Act" (SSMA) and concluding that it violated Article 8 because it provided neither sufficient guarantees against the risk of abuse inherent in any system of secret surveillance nor effective remedies against the use of such special means).

77. See *Weber and Saravia v. Germany,* Application no. 54934/00, Judgment of 29 June 2006, §§ 78–79.

78. *Weber and Saravia,* Ibid.

79. See Paul Schwartz's chapter in this volume, at 66–68, 79–80.

80. *Weber and Saravia*, above note 77, § 83.

the circumstances and conditions under which government agencies are allowed to resort to surveillance measures.[81] The Court went on to specify certain minimum safeguards that must be set out by statute for surveillance laws such as the G-10 Act to avoid abuses of power and satisfy the "in accordance with law" standard. Specifically, a statute must specify:

> . . . the nature of the offences which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or the tapes destroyed.[82]

In another case, the Court made it clear that the requirement that conduct be prescribed by law also applies to the treatment of material after it has been obtained, meaning that the law must specify the "procedure to be followed for selecting for examination, sharing, storing and destroying intercepted material."[83]

Next in *Weber and Saravia*, the Court turned to the purpose and necessity tests. As the aim of the G-10 Act is to safeguard national security and/or prevent crime, its purposes squarely fit within the terms of Article 8(2). As to whether the interferences permitted by the G-10 Act are "necessary in a democratic society," the Court relied on a balancing test that weighs "all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided by the national law."[84] Under this balancing test, the Court concluded that although national authorities retain a degree of discretion over how best to structure a system of surveillance in response to terrorism and related threats, domestic surveillance laws may not grant unfettered power to law enforcement or intelligence agencies.

Based on the tests developed in earlier cases and reiterated in the *Weber and Saravia* case, the Strasbourg Court has developed fairly detailed guidelines for assessing national surveillance law.[85] For example, in *Weber and Saravia* itself,

81. Ibid., § 93.

82. Ibid., § 95.

83. *Liberty and others v. U,K*, Application no. 58243/00, Judgment of 1 Jul. 2008, § 69.

84. *Weber and Saravia*, above note 77, §106.

85. These guidelines have also influenced Council of Europe recommendations regarding law enforcement, including *Guidelines for the Cooperation between Law Enforcement and Internet Service Providers against Cybercrime* (2008), http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/cy_activity_interface2008/567_prov-d-guidelines_provisional2_3april2008_en.pdf and the *European Code of Police Ethics* (2001), http://polis.osce.org/library/f/2687/500/CoE-FRA-RPT-2687-EN-500. For example, Paragraph 41 of the Code of Police Ethics permits the police to interfere with privacy only when strictly necessary to obtain a legitimate objective, and Paragraph 42 advises that collection, storage, and use of

the Court found that an amended version of the G-10 Act authorizing strategic interception of international communications was consistent with Article 8 because the statute contained the following elements: The search terms had to be listed in the monitoring order, which also had to set out detailed rules on storing and destroying any data obtained using these search terms, and the authorities storing the data had to verify every six months whether the data was still necessary to achieve the purpose for which they had been obtained by or transmitted to them. If that was not the case, they had to be destroyed or deleted from the files, or access to them had to be blocked, and all of these steps had to be recorded and, in some cases, supervised by a senior official.[86]

In the *Klass* case, which concerned the targeted surveillance provisions of the German G-10 Act (distinct from those at issue in *Weber and Saravia*), the Court identified a series of limiting factors in the Act that led it to find those targeted surveillance provisions also to be in conformity with Article 8: the Act required a factual indication of suspicion; exhaustion of less intrusive means; particularity as to a specific suspect and his presumed contacts (hence "exploratory or general surveillance" is not permitted); a written application for a surveillance order from a senior official; decision by a senior official; limited duration of no more than three months; implementation by a an official qualified for judicial office; and oversight by an independent entity.[87]

More recently, in a unanimous Grand Chamber decision, the Court in *Zakharov* found serious and widespread faults with the Russian legislation regulating the surveillance of mobile communications. Among the more glaring defects in the Russian law were the fact that although the law requires prior judicial authorization for interception measures, Russian judges in practice only apply purely formal criteria in deciding whether to grant an authorization and "do not verify whether there is a 'reasonable suspicion' against the person concerned and do not apply the 'necessity' and 'proportionality' test";[88] and that Russian "courts sometimes grant interception authorisations which do not mention a specific person or telephone number to be tapped, but authorise interception of all telephone communications in the area where a criminal offence has been committed."[89] Additionally, the Court observed the security services and the police had the technical means to circumvent the authorization procedure and to intercept any communications without obtaining prior judicial authorization.[90]

personal data by the police must be limited to the extent necessary for the performance of lawful, legitimate, and specific purposes.

86. *Weber and Saravia*, above note 77, §§ 97–100.

87. *Klass*, above note 72, §§ 51–60.

88. *Zakharov*, above note 76, § 263.

89. Ibid., § 265.

90. Ibid., § 270.

Based on these cases assessing surveillance laws under Article 8, we have identified 14 normative factors that should be considered in evaluating laws for systematic assess:

Table 1.3. The Normative Framework

1. "In accordance with law"—Are surveillance standards spelled out in a public law or regulation precisely enough to protect against arbitrary application and to inform the public of which entities can conduct surveillance and under what criteria? Does the law specify the procedures to be followed for examining, using, and storing the data obtained?
2. Court order—Does surveillance (data acquisition) require authorization by an independent judicial officer (with possible exception for emergency circumstances)?
3. Approval of senior official—For surveillance in criminal investigations, is approval of a senior police or ministry official required? For national security matters, is approval of a senior intelligence official required, and is approval required from a senior official outside the security service (for example, the attorney general or a legislative body)?
4. Limited to serious crimes or serious threats—Is surveillance limited to the investigation of specified serious crimes? In the national security context, are the topics of surveillance narrowly defined and/or limited to specified serious threats or subjects, or is surveillance permitted, for example, for all matters affecting the national security?
5. Particularity as to target—Must each surveillance be limited to a specifically designated person or account, or is "strategic" or generalized monitoring permitted? (This question gets to the core of whether systematic access is clearly authorized or not.)
6. Showing of suspicion—In the criminal investigative context, does application and approval require a showing of a strong factual basis for believing that the target is engaged in criminal conduct? In the national security context, does application and approval require a showing of a strong factual basis for believing that the target is a foreign power, is engaged in terrorism or other activities that threaten the national security, or is otherwise suspected of being engaged in activities or having information of national security significance?
7. Exhaustion of less intrusive means—Does approval require a showing that other less intrusive means will not suffice or are unlikely to obtain the needed information?
8. Limit on duration—Is the duration of the surveillance limited (e.g., to 30 days, subject to renewal)?
9. Limit on scope ("minimization" of irrelevant data)—Is the government required to ensure that irrelevant data is not recorded or, if collected, is destroyed or is not searched or used?
10. Limit on use and disclosure—Are there limits on the use and disclosure of data that is collected? For example, in the criminal investigative context, does the relevant law specify that data collected can be used only for investigation of the crimes that justified the surveillance? Does the law prohibit disclosure to other entities? In the national security context, does the relevant law specify that data collected cannot be used for investigation or prosecution of crimes, or does the law prohibit disclosure to other entities?

(*Continued*)

Table 1.3. (Continued)

11. Retention limit/limit on storage—Is there a time limit set on how long the government can retain intercepted communications?
12. Notice to target—Must the target of the surveillance, or other persons whose communications are intercepted, be provided notice of the surveillance (normally after the investigation is concluded)?
13. Oversight by independent entity—Does an independent body (judicial, executive, legislative) oversee the actual implementation of surveillance procedures to protect against abuse?
14. Redress (remedy)—Can individuals obtain redress for violations of the established standards?

B. The Normative Analysis: Comparative Observations

With respect to the standards for real-time surveillance *in criminal investigations*, the laws in all of the countries we surveyed (except China and India) are broadly consistent with the normative factors set forth in Table 1.3. That is, the countries generally have statutes expressly authorizing ("in accordance with law") real-time interception of communications content only for the investigation of serious offenses and only upon the approval of both a senior executive branch official and an independent judicial officer. Such statutes generally place limits on the duration of the surveillance and the use of information obtained. The statutes seem to be premised on the principle of particularity—that is, they only authorize surveillance targeted at a specified person, device, or account. Also, almost half the countries studied do not have provisions expressly limiting the scope of the content that can be recorded (by requiring that government agencies not record irrelevant data or, if they do, that they do not retain such data) and almost the same number lack laws requiring notice of surveillance to the target of surveillance or other persons whose communications are intercepted. China meets none of the 14 standards identified in our normative framework, and India meets only one of the 14 (approval of a senior officer required) and somewhat addresses another standard (loosely tying surveillance to suspicion of criminal conduct by requiring that the surveillance be "necessary or expedient" for the investigation of an offense).

Although standards for real-time interception of communications are uniformly high, standards for access *to stored communications* held by third parties are less consistent. In France, for example, stored documents can be accessed in some circumstances by the judicial police or customs authorities and in other cases upon the approval of the public prosecutor. In the United States, the Electronic Communications Privacy Act (ECPA) provides that service providers can be forced to disclose stored content with a subpoena, issued without judicial approval, although an appellate court has held that process to be in violation of the Constitution, and service providers and the Justice Department now seem to agree that a judicial warrant is needed to compel third-party disclosure of

content. To the extent that any laws expressly address stored content, it is not clear whether any of them give attention to the questions of scope or minimization; that is, although real-time interception is normally approved for periods of limited duration and some laws limit the recording of irrelevant information, it is not clear whether orders for disclosure of stored communications contain any temporal scoping limitations, and it is not clear how rules on minimization of irrelevant data would be applied in the case of disclosure of stored data.[91] In Europe, however, under Article 8 of the Convention, acquisition of stored content might be subject to a requirement that the law authorizing the collection must specify the procedure to be followed for selecting the material to be collected.[92]

When it comes to transactional data regarding communications, standards are even weaker. In the UK, traffic data can be obtained upon the demand of a very wide range of government officials, including in non-criminal matters. In the United States, stored telephone metadata is available without a court order (but not cell site location information), whereas access to Internet metadata and real-time interception of telephone or Internet metadata require a court order. In Australia, the law permits voluntary disclosure of communications metadata to law enforcement and intelligence agencies while also providing for mandatory disclosure upon request. In South Korea, although it is clear that the government must obtain a court order to require a telecommunications service provider to disclose transactional data ("communications confirmation data"), the vagueness of the provisions seemed to allow ISPs to voluntarily disclose such data to the government without a court order and such voluntary disclosures used to be customary. However, a major court ruling in 2012 cast doubt on the legitimacy of voluntary disclosures.

With respect to the standards for government access to communications *in national security investigations*, the overall picture is very complex. For example, whereas most countries surveyed (again, leaving aside China and India) require a court order for surveillance in criminal investigations, almost half the countries studied do not have provisions requiring court orders for surveillance undertaken in the name of national security or for foreign intelligence gathering. Likewise, at least half do not pose limits on the scope of national security requests, or require notice to targets.

Although laws setting standards for interception in criminal cases generally require targeted surveillance, the rules for national security are much less consistent in imposing a particularity requirement. The statutes in Germany and the UK expressly allow large-scale, untargeted collection of communications with one leg originating outside the country. The US and French laws distinguish between communications carried by wire (including fiber) and communications transmitted over radio waves (including satellite transmission); in both

91. See Orin Kerr, "The Next Generation Communications Privacy Act," 162 *University of Pennsylvania Law Review* 373 (2013) (noting the absence of any scoping or minimization limits in ECPA, the US law regulating access to stored communications).

92. See *Liberty and others,* above note 83, at § 69.

countries, the relevant statutes permit non-targeted surveillance of radio communications where one end of the communication originates abroad. Canada and Australia have long collaborated with the United States and the UK in bulk collection programs.

In addition, it is worth noting the diversity of oversight mechanisms in both criminal and national security investigations. They include annual reports on the number of intercepts and other information, which are delivered either to senior government officials or to legislative committees; reviews by appointed oversight commissions; audits; and legislative investigations. The United States has multiple oversight mechanisms. Even warrantless surveillance under the now notorious PRISM program is overseen by the Foreign Intelligence Surveillance Court, which approves the targeting and minimization procedures and monitors implementation of the program. The Privacy and Civil Liberties Oversight Board is an independent agency established by Congress to review and analyze executive branch antiterrorism efforts and ensure both that they are balanced with the need to protect privacy and civil liberties and that liberty concerns are considered in the formulation of related law and policies.[93] As Paul Schwartz has suggested, however, many such formal oversight mechanisms are quite ineffective and amount to little more than what he calls "privacy theater."[94] In countries with an independent press and/or strong laws protecting the freedom of speech, informal oversight mechanisms, though raising their own complications under criminal and national security laws, also play an oversight role. The efforts of the press, advocacy groups, government watchdog groups, and various dissenters encourage public debate and enhance government accountability.[95]

In terms of location data, most of the countries studied permit location tracking subject to a weak standard. For example, location data may be tracked without a warrant in Australia, China, Germany, India, Israel, and the United Kingdom. In the United States, however, the relevant doctrine is more complex thanks to a recent Supreme Court decision, *United States v Jones*,[96] announcing a new,

93. For an overview of the Privacy and Civil Liberties Oversight Board (PCLOB), see http://www.pclob.gov/. On January 23, 2014, the Board released a comprehensive report assessing government bulk collection activities pursuant to Section 215 of the PATRIOT Act and the operations of the Foreign Intelligence Surveillance Report. See PCLOB Report, n. 35. The Board released a report focused on global surveillance and the US government's use of Section 702 of FISA, on July 2, 2014, https://www.pclob.gov/library/702-Report.pdf.

94. Paul M. Schwartz, "Reviving Telecommunications Surveillance Law," 75 *University of Chicago Law Review* 287, 310–12 (2008).

95. See Jack L. Goldsmith, *Power and Constraint: The Accountable Presidency after 9/11* 205–43 (2012) (arguing that the executive branch is forced to account for its actions by the constant gaze of "courts, Members of Congress and their staff, human rights activists, journalists and their collaborators, and lawyers and watchdogs inside and outside the executive branch" who together constitute a highly effective "presidential synopticon"). The Snowden revelations would seem to confirm this insight yet it remains highly debatable whether such informal mechanisms suffice.

96. 565 U.S. 400 (2012).

trespass-based test for what counts as a search under the Fourth Amendment. Although *Jones* applied the trespass test to find that the installation of a GPS device on a vehicle with the intent to use it was a search, the exact circumstances under which the use of such a device requires a warrant are not yet clear. The standards under which government agencies can compel disclosure of cell site location information are less settled. ECPA requires, at a minimum, a court order, and a majority of courts have held that a warrant is needed for real-time tracking, whereas a majority of courts have held that a full warrant is not necessary to compel disclosure of stored location records.

Most countries handle travel and financial data under laws requiring routine, bulk reporting for specified classes of data. For example, most countries require passenger data reporting for air travel (Australia, Brazil, Canada, China, Israel, South Korea, the UK, and the United States). International arrangements for sharing passenger data are more controversial.[97] All 13 countries also require anti-money-laundering reporting under generally similar national laws (under which large financial transactions must be reported). Italy and others require certain entities to notify the tax authorities of various other transactions; in Italy, this is a direct response to the high level of tax fraud and evasion.[98]

With respect to the normative standards for government access to business records, the results are more difficult to summarize. In Australia, for example, a police officer seeking documents (including in electronic form) may make an application to a federal magistrate for a "notice to produce" order. To grant such an order, the magistrate must be satisfied, on the balance of probabilities, by information on oath or by affirmation, that: (1) the person has documents (including in electronic form) that are relevant to, and will assist, the investigation of a serious offense; and (2) giving the person a notice under this section is reasonably necessary, and

97. In 2012, the European Parliament approved a passenger name record (PNR) agreement with the United States, under which US authorities are permitted access to EU citizens' airline records. See Kirsten Fieldler, "EU Parliament Agrees to EU-US PNR Agreement," *EDRI* (April 25, 2012), http://www.edri.org/edrigram/number10.8/ep-agrees-us-eu-pnr. A year later, the European Parliament rejected a proposal to create a pan-European system for sharing and storing passengers' phone numbers, addresses, and credit card details whenever they entered or departed the 27-country European Union, on the grounds that it breached citizens' fundamental rights; see Tedd Nykiel, "European Lawmakers Reject Passenger-Data Scheme," *Reuters* (April 24, 2013), http://uk.reuters.com/article/2013/04/24/uk-eu-data-idUKBRE93N0U020130424. However, in April 2016, following gun and bomb attacks by the Islamic State in Paris in 2015 and in Brussels in March 2016, the European Parliament and the European Council enacted a similar PNR directive, establishing detailed rules for EU national authorities to access PNR data collected by airlines for passengers on all flights to, from, and within the European Union. Estefania Narrillos, "EU Passenger Name Record (PNR) Directive: An Overview," *European Parliament News* (January 6, 2016), http://www.europarl.europa.eu/news/cs/news-room/20150123BKG12902/EU-Passenger-Name-Record-(PNR)-directive-an-overview.

98. Additionally, Italian hotels automatically report the identity of all hotel clients to the police.

reasonably appropriate and adapted, for the purpose of investigating the offense. However, if an authorized police officer considers on reasonable grounds that a person has documents (including in electronic form) that are relevant to, and will assist, the investigation of a serious terrorism offense, no prior court approval is required. Similarly, in the UK, Section 19 of the Counter-Terrorism Act provides that "A person may disclose information to any of the intelligence services for the purposes of the exercise by that service of any of its functions."[99] Most countries, with the exception of China and India, observe some limits on use, retention, and disclosure; provide oversight and redress mechanisms (ranging from complaints to a Privacy Commissioner to civil actions), and must satisfy various reporting requirements. However, limits on use and disclosure often have many exceptions. In Australia, for example, information obtained by one agency for a specific purpose may be available to a range of other agencies for quite different purposes. In Europe, the European Court of Human Rights has explicitly held that a transmission of data to and their use by other authorities constitutes "a further separate interference" with the right to privacy under Article 8 of the Convention. Such disclosures are not flatly prohibited but must be subject to the same principles of legality and necessity; in *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, the Court expressly declared Bulgaria's intelligence surveillance law to be inconsistent with the Convention because it did not place adequate limits on disclosure and use.

Of all the countries surveyed, Germany has most expressly addressed the issues associated with systematic access to business records and the application to those records of analytic techniques for law enforcement purposes. On the one hand, as Paul Schwartz noted, data mining is an established law enforcement technique in Germany. (The German term for the practice is "screening search.") On the other hand, the German Constitutional Court has set limits on the use of the technique. In Germany, laws at the federal and state levels distinguish between the use of "data screening" to (1) investigate past crimes, or (2) permit a preventive response to potential crimes. Data screening to investigate past crimes is regulated by various state laws and at the federal level by Section 98a of the Criminal Procedural Code. The federal statute permits screening searches only where there are "sufficient factual indications to show that a criminal offense of significant importance has been committed." However, there are state statutes that permit a *preventive* use of data screening. In 2006, the German Federal Constitutional Court established significant limits on such law enforcement use of this practice. In its *Data Screening* opinion, the Constitutional Court used a proportionality standard to find that data screening for preventative purposes was constitutionally permissible only when the police had concrete facts indicating that a serious crime was being planned. Further study of the use of screening searches in Germany since the Constitutional Court's decision may yield useful lessons.

99. Brown, above note 8, at 235.

VIII. RECOMMENDATIONS AND CONCLUSIONS

Our research into systematic access, augmented by the Snowden revelations, suggests at least four conclusions, each posing unresolved challenges.

First, technological developments associated with the digital revolution make it easier than ever for governments to collect, store, and process information on massive scale, and governments seem to be exploiting those developments—and responding to pressing threats such as terrorism—by demanding more and more information. At the same time, ongoing developments in the ability to analyze large data sets are leading governments to assert that they can extract crucial but otherwise unobtainable insights from big data. For example, in the context of defending its telephony metadata program, the US government has expressly argued that, in order to find "the needle in the haystack," it needs to acquire the entire haystack. Though governments have long required corporate entities to systematically report certain data, such as currency transactions over certain thresholds, that information used to remain "stovepiped." Government agencies today are under information-sharing imperatives, and modern analytic techniques are seen as offering increasingly powerful abilities to draw from data meanings that are unrelated to the purposes for which it was initially collected.

- Policy implications: The trend toward systematic collection poses challenges to the existing legal frameworks because many of the statutes regulating government access and data usage were premised on particularized or targeted collection, minimization, and prohibitions on information sharing and secondary use.[100]

Second, as Internet-based services have become globalized, trans-border surveillance—surveillance in one country affecting persons in another—has flourished. Gone are the days when intelligence agencies had to acquire data from a point within the country where the data originated (or with an antenna aimed at the targeted country). Now, in many instances, communications to or from people in one country pass through or are stored in other countries, where they are available to those governments. The United States is perceived as having unique advantages in this respect, both because a large percentage of the world's communications pass through or are stored in the United States and

100. A cornerstone of the privacy framework that has guided privacy laws globally for the past 30 years is the principle that data collected for one purpose should not be used for another purpose, yet big data analytics explicitly promises to find unanticipated meanings in data. Big data equally challenges other core privacy principles. Ira Rubinstein, "Big Data: The End of Privacy or a New Beginning?," *International Data Privacy Law* (2013) vol. 3, no. 2 pp. 74–87 ("when this advancing wave arrives, it will . . . overwhelm the core privacy principles of informed choice and data minimization"). See generally Christopher Kuner, Fred H. Cate, Christopher Millard, and Dan Jerker B. Svantesson, "The Challenge of 'Big Data"' for Data Protection," *International Data Privacy Law* (2012) vol. 2, no. 2 pp. 47–49.

because the United States has invested vast resources in collection capabilities, but the United States is not alone in exploiting global data flows. Moreover, the global flow of data and the popularity of US-based services not only means that the United States has access, inside the United States, to the communications of those living and working outside the United States, but it also means that the United States has access outside the United States to communications of persons living and working inside the United States, for those communications to and from people in the United States can be captured as they move among servers outside the United States.

- Policy implications: The rise in trans-border surveillance raises complex questions. To begin with, statutory frameworks for surveillance tend to be geographically focused and draw distinctions between communications that are wholly domestic and communications with one or both communicants on foreign soil. Moreover, statutory frameworks, as far as we can tell, often draw a distinction between the collection activities that an intelligence service performs on its own soil and the activities that it conducts extraterritorially. This is certainly true of the United States: the Wiretap Act and the Foreign Intelligence Surveillance Act do not regulate the conduct of the United States outside US territory (with a minor exception for intelligence surveillance outside the United States targeting US persons outside the United States). Lowered standards for trans-border surveillance have a substantial impact on companies that offer global communications services and want to be able to assure their customers worldwide that their communications are secure. It also raises human rights questions about the existence and scope of state duties to protect and respect privacy and free expression of people outside the state's territorial boundaries; although privacy is universally recognized as a human right, some governments (including the US) assert that their human rights obligations have a territorial limit.[101]

Third, national security legal authorities such as Section 12 of the Counter-Terrorism Act of 2008 have become increasingly powerful since 9/11 in the UK and some European countries, the United States, and globally. It has long been

101. As Frank La Rue, Special Rapporteur on the Promotion and Protection of the Right to Freedom of Expression, noted, there is "serious concern with regard to the extraterritorial commission of human rights violations and the inability of individuals to know they might be subject to foreign surveillance, challenge decisions with respect to foreign surveillance or seek remedies." *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank LaRue, to the Human Rights Council*, at 64 (April 17, 2013), http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf.

the case that governments have claimed greater powers to collect data in the name of national security than in ordinary criminal law enforcement cases.

- Policy implications: In the post 9/11 world, at precisely the time that technological capabilities are increasing, and at precisely the same time that global data flows are expanding exponentially, national security powers have been getting stronger, raising new questions relating to the trust that citizens, customers, and users vest in governments and corporations alike.

Fourth, this expansion in powers has been supported by extreme secrecy. In the United States, for example, a provision in the PATRIOT Act that seemed to authorize particularized disclosures had been interpreted by secret court order to authorize ongoing bulk collection. Moreover, judicial doctrines in the United States (and probably elsewhere) make it very difficult to obtain an effective remedy for possible violations of privacy, speech, and association rights.[102]

- Policy implications: The lack of transparency makes it very difficult to have a rational debate about governmental powers and concordant checks and balances. And the lack of openness is leading to proposals such as requiring local storage of data that could fragment the Internet, harming both innovation and access to information.

What we need, globally, is a robust debate about what the standards should be for government surveillance. That debate should be premised on much greater transparency about current practices and about the legal underpinnings of those practices. (Ironically, as a result of the Snowden leaks and of changes in the law, the United States may now have more transparency on its practices and rules than any other country in the world.)

Perhaps a useful framework for making progress on these issues can be found within the context of international human rights law.[103] As we explain above, the most fully developed body of international law on government surveillance and privacy is that of the European Court of Human Rights, which over the years has issued multiple decisions on wiretapping, including national security surveillance. The court has never suggested that secret surveillance is per se a violation of human rights. Instead, it has identified a set of checks and balances that could offer sufficient guarantees against the risk of abuse.

102. *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 185 L. Ed. 2d 264 (2013).

103. See, for example, *The Right to Privacy in the Digital Age, Report of the Office of the United Nations High Commissioner for Human Rights*, U.N. Doc. A/HRC/27/37 (June 30, 2014), http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf (The High Commissioner discusses the principles of legality, necessity, and proportionality, as well as procedural safeguards and remedies).

Among the questions to explore:

- How can we give meaning to privacy in an era of systematic collection and trans-border surveillance?
- If bulk collection is an inevitable reality of the digital age, how can we apply human rights principles such as necessity and proportionality to claims that it is necessary to collect all the data to serve certain compelling governmental needs?
- Given the widely held view that privacy is a universal right and the equally universal rule that governments have broad powers to protect themselves and their peoples from foreign threats, how should we regulate trans-border surveillance?

In a networked word, the standards for government access may be judged not so much in the context of a debate between EU and US laws but rather on the basis of international human rights standards. To at least some extent, there is underway today a movement toward global standards of digital privacy based on international human rights standards. The US government may argue that the PRISM standards actually comport with international law, but that will be an illuminating debate, in which Europeans must explain and defend their own laws by the same standards. If they can have this debate, then government officials in Europe and the United States can work with human rights institutions, civil society, and the Internet industry at large to move the rest of the world toward a set of principles based on transparency, proportionality, and accountability.

Europe and the Middle East

2

Systematic Government Access to Private-Sector Data in France

WINSTON J. MAXWELL

I. ABSTRACT

In regulating access to data by law enforcement and the intelligence services, France distinguishes between different levels of government intrusions into privacy. As is the case in most countries, real-time interception of private correspondence requires a higher level of safeguards than the disclosure of metadata.

Post-9/11 France enacted provisions to require providers of telecommunications and hosting services to retain significant amounts of traffic data and so-called "identification data," a requirement that went beyond the scope of the now-invalidated EU directive on data retention. Even though the EU directive on data retention was invalidated by the Court of Justice of the European Union (CJEU) and similar laws in the UK and Sweden have been held to violate the EU Charter of Fundamental Rights, the French data retention laws remain on the books today.

France's intelligence agencies have wide-ranging powers to collect data and conduct interceptions with no prior judicial approval. Those rights include the ability to analyze metadata of all French Internet users to detect suspicious patterns of behavior. In 2015 French lawmakers created an oversight committee, the CNCTR, to supervise data-collection activities by intelligence agencies, but privacy advocates argue that institutional safeguards are still insufficient.

II. INTRODUCTION

The French data protection authority, the *Commission Nationale de l'Informatique et des Libertés* (CNIL), is one of the world's most outspoken privacy advocates. Yet France's own laws give intelligence agencies far-reaching surveillance powers, including the power to collect and analyze massive amounts of metadata to detect suspicious patterns of behavior. Although approved by France's

Bulk Collection. Fred H. Cate and James X. Dempsey.

Constitutional Court, these provisions contribute to what some have called a "downward spiral"[1] in the protection of privacy rights of European citizens against government surveillance.

France's supreme courts (the *Conseil d'Etat* and the *Conseil Constitutionnel*) appear to accord flexibility to the French government and legislature when it comes to government surveillance laws, whereas the CJEU applies a strict proportionality test. Decisions by the CJEU and the European Court of Human Rights (ECtHR) will analyze in detail whether the surveillance measure results from a clearly drafted law, and is necessary in a democratic society. The "necessity" test generally requires a showing that the government measure is effective for its intended purpose, and is the least intrusive measure available to get the job done. By contrast, French decisions seem to limit their enquiry to whether the surveillance measures are limited in scope, and whether they are surrounded by procedural safeguards. The French decisions do not attempt to determine whether the relevant surveillance measure represents the least intrusive means available to achieve the desired objective. When reading French court decisions on government surveillance, one cannot help but think that French courts apply a lighter version of the proportionality test than do the CJEU or the ECtHR. This may only be an impression, as in theory French courts are required to apply the same test as their European counterparts. The difference may be attributable to the French courts' concise style of drafting—the analysis of proportionality may occur behind the scenes.

The remainder of this chapter will describe how French government access to private-sector data is regulated. Much of the discussion will concentrate on France's intelligence-gathering practices, which have significantly expanded as a result of the 2015 terrorist attacks in Paris. Like most democratic countries, France has two different legal frameworks for government surveillance. The first applies to criminal investigations by prosecutors and police authorities; the second applies to collection of data by intelligence agencies to protect the "fundamental interests" of France. As one would expect, fewer safeguards surround data collection in the context of intelligence activities. For example, intelligence authorities do not need a judge's permission to conduct data gathering, whereas similar data gathering by judicial police would require the authorization of a judge.

The sections below will describe the investigatory powers and countervailing safeguards that apply to data gathering by French authorities, both in the context of criminal investigations and in the context of intelligence-gathering for defense of the fundamental interests of France.

1. European Parliament resolution of October 29, 2015 on the follow-up to the European Parliament resolution of March 12, 2014 on the electronic mass surveillance of EU citizens (2015/2635(RSP)); see also, N. Muiznieks, "Europe Is Spying on You," *New York Times* (Oct. 27, 2015).

III. DATA COLLECTION IN THE CONTEXT OF CRIMINAL INVESTIGATIONS

The rules applicable to police investigations are contained in the French Code of Criminal Procedure. Those rules are similar to those in the United States and other democratic countries, requiring the prior authorization of a judge for the most intrusive forms of data searches. For example, any kind of real-time interceptions of private correspondence, whether a telephone conversation, email, or instant message, requires the prior authorization of an independent judge.[2] The independent judge is either the investigating magistrate (*juge d'instruction*) or the judge of liberty and detention (*juge des libertés et de la détention*). When police clone a computer terminal and monitor it at a distance, a practice referred to in France as "capturing of computer data," police must also seek authorization by a judge, and can only seek authorization for purposes of fighting serious crimes.[3] "Capturing of computer data" is particularly intrusive because it permits police authorities to hack into a computer system, access the stored data, monitor in real time every keystroke of the terminal, and see what is displayed on the screen.

Other forms of access to computer data are deemed less intrusive of privacy and therefore are surrounded by fewer safeguards. Police authorities can require disclosure of stored computer data with varying levels of approval, depending on the stage of the investigation. If police authorities have reason to believe that a crime is in the course of being committed (*flagrance*), then an officer from the judicial police can require disclosure of computer data immediately, as long as the officer informs simultaneously the public prosecutor.[4] If the request for computer data is made in the context of a preliminary investigation (*enquête préliminaire*), the public prosecutor must grant specific authority to the judicial police to proceed with the request.[5] The public prosecutor is trained as a magistrate but he or she is not a judge when acting in his or her capacity as public prosecutor. Finally, if the investigation has advanced to the stage where a *juge d'instruction* is appointed, then the investigating judge must authorize all measures to compel disclosure of computer data.[6]

All of these requests for data, whether ordered by the judicial police, the prosecutor, or investigating judge, are known under French law as *réquisitions*. The French Code of Criminal Procedure provides that a *réquisition* ordering access to computer data can permit access to data that is stored in servers outside of France as long as the *réquisition* involves a terminal that is located in France with authorized access to the relevant data located abroad, and as long as the access

2. Articles 100 and 706-95, Code of Criminal Procedure.

3. Article 706-102-1, Code of Criminal Procedure.

4. Articles 57-1, 60-1, 60-2, Code of Criminal Procedure.

5. Articles 77-1-1 and 77-1-2, Code of Criminal Procedure.

6. Articles 94 and 97, Code of Criminal Procedure.

is permitted under international law.[7] The location of the data itself is irrelevant. All forms of *réquisition* also permit access to so-called connection data and identification data stored by telecom operators and hosting providers under French law. These data storage obligations are described in Section VI below.

IV. DATA ACCESS BY CUSTOMS AUTHORITIES

Customs authorities have separate authority to issue requests for computer data in connection with investigation of potential customs or tax violations.[8] These *réquisitions* may be issued by a customs official having the rank of at least "controller," and do not need to be approved by a judge. Telecom operators, transport companies, and airlines are among the kinds of companies that can receive orders from customs authorities for the communication of data.

V. DATA ACCESS BY INTELLIGENCE AUTHORITIES

A. New Surveillance Law Creates Oversight Committee

The access to data by intelligence agencies is governed by the French Internal Security Code. The rules in the Internal Security Code provide less protection of individual rights than do the rules in the Code of Criminal Procedure. In the aftermath of the Paris terrorist attacks of January 11, 2015, France reformed its rules for intelligence gathering.[9] The main accomplishment of the reform was to create a single coherent framework for intelligence-gathering techniques. Previously, the provisions were scattered throughout different parts of the Internal Security Code, creating confusion and incoherence in how different kinds of data were collected.[10] Moreover, the previous oversight body for intelligence gathering activities, the CNCIS, lacked authority with regard to certain data-gathering activities, leaving those activities unsupervised by any independent body.

The July 24, 2015 Surveillance Law[11] (the "2015 Law") cures that defect by creating a new independent oversight body called the Commission for Oversight of Intelligence Gathering Techniques, the "CNCTR," which stands for *Commission Nationale de Contrôle des Techniques de Renseignement*. Under the 2015 Law, data collection for intelligence purposes can be implemented only when a specific authorization is given by the prime minister.[12] The prime minister's authorization may be granted only after the CNCTR has rendered an opinion on the compatibility of the

7. Article 57-1, Code of Criminal Procedure.

8. Article 65, Customs Code.

9. Law n° 2015-912 of July 24, 2015, O.J. July 26, 2015, p. 12735.

10. For a description of the previous rules, see W. Maxwell, "Systematic Government Access to Private-Sector Data in France," 4 *Int'l Data Privacy Law* 4 (2014).

11. Law n° 2015-912 of July 24, 2015, O.J. July 26, 2015, p. 12735.

12. Article L821-1, Internal Security Code.

measure with the principles set forth in the Internal Security Code. The CNCTR's opinion must be rendered within 24 to 72 hours, and is not binding on the prime minister.[13] Nevertheless, if the prime minister decides to ignore the recommendations of the CNCTR, the prime minister must give reasons for his or her decision.[14] Moreover, the CNCTR can file an appeal with the *Conseil d'Etat* to challenge the prime minister's decision if the prime minister disregards the CNCTR opinion.[15]

There are three situations where the CNCTR's opinion is not required. The first is where a terrorist or national defense threat requires urgent action. In that case, the prime minister can issue an authorization without waiting for the CNCTR's opinion.[16] Second, the CNCTR's opinion is not required for so-called "international" data collection, examined in Section IV(G) below. Finally, the opinion is not required for the general monitoring of radio transmissions, examined in Section IV(C) below.

The CNCTR has nine members: two are members of the French National Assembly, two are members of the Senate, two are members of the *Conseil d'Etat*, two are members of the Court of Cassation, and one is a person with expertise in telecommunications nominated by the French telecommunications regulatory authority, the ARCEP.[17] Each of the members of the CNCTR must receive security clearance. The CNCTR's decisions themselves are considered defense secrets.[18] Individuals who think they might be spied on by French intelligence agencies can ask the CNCTR to verify. The CNCTR will then check whether appropriate legal procedures have been followed, but will not reveal to the individual whether he or she is indeed the target of surveillance.[19] (This is similar to the role of the ombudsperson in the US-EU Privacy Shield arrangement.[20]) The CNCTR has authority to access surveillance records, except for data that has been transmitted to the French authorities by their foreign counterparts.[21] Civil liberties groups complain that this opens a loophole, because French agencies can sidestep internal oversight mechanisms simply by asking foreign intelligence agencies to collect data for them.[22]

13. Article L821-3, Internal Security Code.

14. Article L821-4, Internal Security Code.

15. Article L833-8, Internal Security Code.

16. Article L821-5, Internal Security Code.

17. Article L831-1, Internal Security Code.

18. Article L832-5, Internal Security Code.

19. Article L833-4, Internal Security Code.

20. Letter from U.S. Secretary of State Kerry to EU Commissioner Jourova dated July 7, 2016, Annex A: EU-U.S. Privacy Shield Ombudsperson Mechanism, Section 4(e).

21. Article L833-2, Internal Security Code.

22. See, Brief filed by La Quadrature du Net and French Data Network on May 10, 2016 before the Conseil d'Etat challenging the government decree n° 2016-67 adopted to implement

B. French Definition of "Fundamental Interests of the Nation"

The 2015 Law allows intelligence agencies to gather data when necessary for the "defense and promotion of the fundamental interests of the nation." "Fundamental interests of the nation" include national defense; major foreign policy interests; major economic, industrial, and scientific interests; the prevention of terrorism; immediate threats to public order; organized crime; and the proliferation of weapons of mass destruction.[23] France's "major economic, industrial and scientific interests" are recognized as part of the fundamental interests of the nation, thereby permitting data gathering for purposes of economic espionage. Civil liberties groups have argued that the concept of "fundamental interests of the nation" is so broad as to violate European principles of proportionality, which require among other things that laws interfering with fundamental rights be clear, understandable, and predictable.[24] Many drug investigations could be considered as part of "organized crime," making it difficult to distinguish between matters that should be subject to criminal investigations governed by the Code of Criminal Procedure, and matters that relate to intelligence activities governed by the less-stringent Internal Security Code.

C. General Monitoring of Radio Transmissions

The 2015 Law maintains a 25-year-old provision in the Internal Security Code that allowed the general monitoring of over-the-air radio transmissions without any oversight.[25] Under these provisions, intelligence authorities may conduct untargeted surveillance of radio transmissions without prior authorization or any other form of supervision, as long as the reasons for doing so relate to "defending national interests." At the request of French civil liberties groups, the *Conseil d'Etat* recently sent a question to the French Constitutional Court, asking about this provision's constitutionality.[26] The Constitutional Court found the provision unconstitutional because of the lack of guidance given by lawmakers on what "general monitoring of radio transmissions" consists of, and the total lack of institutional oversight for the practice.[27] The Court nevertheless allowed the law to stay in effect until December 31, 2017.

the July 24, 2015 law, available at https://exegetes.eu.org/recours/renseignement/CEtat/2016-05-06-Quadrature%20du%20net_%20FDN%20et%20FDNN%20%28Renseignement%20-%20Decret%202016-67%29%20-%20MC.pdf [hereinafter, the "Quadrature du Net Brief"].

23. Article L811-3, Internal Security Code.

24. Quadrature du Net Brief, above note 22.

25. Article L811-5, Internal Security Code.

26. Conseil d'Etat decision of July 22, 2016, case n° 394922.

27. Constitutional Court decision n° 2016-590 QPC of October 21, 2016.

D. Access to Metadata

The Internal Security Code permits intelligence agencies to obtain access to metadata retained by telecom operators and hosting providers. As explained in Section VI, both telecom operators and hosting providers must retain broad categories of metadata for 12 months. The 2015 Law permits intelligence agencies not only to require telecom operators and hosting providers to deliver access to stored metadata,[28] but also to allow collection of metadata, including location data, in real time. The real-time collection of data must be preceded by a non-binding opinion of the CNCTR, and is only permitted for the prevention of terrorism, not for the defense of France's other "fundamental interests."[29]

E. Interception of the Content of Communications

The 2015 Law maintains the ability for intelligence agencies to intercept the content of private communications for purposes of defending France's fundamental interests, after an authorization by the prime minister and a non-binding opinion of the CNCTR.[30] These so-called "security interceptions" can be implemented using otherwise illegal interception equipment, such as "IMSI catchers" that pretend to be a mobile phone base station. A recent amendment to the 2015 Law allows intelligence agencies not only to listen to communications of the targets themselves, but also to the communications of anyone in the target's circle of contacts if those persons may provide information in connection with the intelligence objective identified in the authorization.[31] After consulting the CNCTR, the prime minister must fix the maximum number of security interceptions that intelligence agencies can conduct during a given year.

F. Untargeted Analysis of Metadata

One of the most controversial provisions in the 2015 Law relates to the so-called black boxes (*boîtes noires*) that intelligence agencies can require telecommunications operators and hosting providers to install on their networks. After authorization from the prime minister, intelligence agencies may deploy algorithms to analyze all metadata from users of French telecommunications or hosting services in order to identify suspicious patterns revealing potential terrorist threats. When it originally presented the black box provision, the French government argued that the metadata was anonymous and that its analysis therefore presented no threat to privacy. The French data protection authority disagreed, stating that the analysis of metadata involves the processing of personal data and therefore presents a risk

28. Article L851-1, Internal Security Code.

29. Article L851-2, Internal Security Code.

30. Article L852-1, Internal Security Code.

31. Article 17, Law n° 2016-987 of July 21, 2016.

for privacy that had to be justified under strict rules on proportionality.[32] The provision seemed to contradict the CJEU's *Digital Rights Ireland* decision, which states that the retention of traffic data involving the entire population of users in a country constitutes a disproportionate infringement of privacy.[33] Similarly, in the *Schrems* decision,[34] the CJEU found that massive surveillance is incompatible with the EU Charter of Fundamental Rights. Consequently, many observers thought that France's black box provision would also be considered disproportionate because it permits analysis of metadata involving all users of telecom services or social media services in France, including persons who are not suspected of any illegal activity.

The French Constitutional Court reviewed the provision and affirmed its constitutionality.[35] The court pointed out that the algorithm used by intelligence authorities only deals with metadata and does not permit the identification of individuals (although when suspicious activity is detected, officials can request permission to identify the person in order to set up more targeted surveillance). Moreover, the court said that the procedure can only be implemented after an authorization from the prime minister and an opinion from the CNCTR. The authorization is only granted for a period of two months and its renewal is subject to certain conditions to ensure that the algorithm does not create too many false positives. Finally, the court pointed out that the black box measure is only allowed in connection with antiterrorism activities. On balance, the court found that the black box provision did not represent a disproportionate interference with the right to privacy.

For an outside observer it is frustrating that the French Constitutional Court provided no guidance on why it considered the French black box provision compatible with the principles set down by the CJEU in its *Digital Rights Ireland* decision. The court did not even mention the existence of the CJEU decision. The French court's lack of analysis of the CJEU's *Digital Rights Ireland* decision contrasts with the UK High Court decision dated July 17, 2015, in which the High Court directly confronted the UK Data Retention and Investigatory Powers Act 2014 (DRIPA) with the principles set forth in the *Digital Rights Ireland* decision.[36] In the UK decision, the High Court found that DRIPA created a disproportionate infringement of citizens' rights to privacy.

32. CNIL deliberation n° 2015-078 of March 5, 2015.

33. CJEU decision of April 8, 2014, Case C-293/12, *Digital Rights Ireland v. Ministry for Communications et al.*

34. CJEU decision of November 13, 2015, Case C-362/14, *Schrems v. Data Protection Commissioner.*

35. Constitutional Court decision of July 23, 2015 n° 2015-713 DC.

36. UK High Court decision of July 17, 2015, Cases n° CO/3665/2014, CO/3667/2014 and CO/3794/2014.

Several French civil liberties groups are challenging the French decree implementing the black box provision. They argue that the provision is incompatible with the case law of the CJEU and of the ECtHR.[37]

G. Collection of Data Relating to "International Communications"

Previously, collection of data outside of France by French intelligence agencies fell into a legal no man's land. French intelligence agencies took the position that French law did not apply to their data-gathering activities outside France. The 2015 Law originally contained a provision on so-called international data collection, but the Constitutional Court annulled the provision because it contained insufficient institutional safeguards.[38] A new law was passed on November 30, 2015, which corrected the defects identified by the Constitutional Court. The November 30, 2015 law[39] expressly authorizes the collection of data relating to communications received or sent outside of France, including the collection and analysis of both metadata and content. These international data collection measures must be authorized by the prime minister, although he or she does not need to seek the prior opinion of the CNCTR. The CNCTR is nevertheless informed and is allowed to have access to interception records.

A curious aspect of the law is that it creates different levels of protection based on whether the communication involves a person located in France. Intelligence authorities may collect and analyze metadata and content data involving communications by persons outside France with minimal supervision. But if the authorities stumble upon a French telephone number, or a French IP address, then the data must be destroyed and a domestic procedure involving more safeguards must be followed. The purpose of the law is to allow monitoring of communications not involving French residents. French civil liberties groups argue that the provision allows mass surveillance incompatible with the CJEU's *Schrems* decision, and that the measure illegally discriminates against non-French residents (including residents of other EU Member States). Under the EU Charter of Fundamental Rights, the protection of privacy accrues to "everyone,"[40] which makes the difference in treatment in the November 30, 2015 law surprising. One of the complaints of European authorities with regard to US surveillance laws was that Europeans did not benefit from the same institutional protections as US citizens and residents.[41] The French law appears to suffer from exactly the same defect.

37. Quadrature du Net Brief, above note 22.

38. Constitutional Court decision of July 23, 2015 n° 2015-713 DC.

39. Law n° 2015-1556 of November 30, 2015.

40. Article 8, EU Charter of Fundamental Rights.

41. Communication from the European Commission on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU, November 27, 2013, COM(2013) 847 final, paragraph 7.2.

H. Hacking into Computer Systems

Where "the information cannot be collected through other legal means," the prime minister can authorize, after the CNCTR's opinion, use of equipment to access data stored in computer systems, as well as to install clone spyware that permits agents to see the screen and follow keystrokes of a computer.[42] Unlike Article 57-1 of the French Code of Criminal Procedure, this provision of the Internal Security Code does not state expressly that the "computer systems" involved may be located inside or outside France.

I. Encryption

Any provider of encryption technology must provide to intelligence authorities the keys for decrypting messages. Alternatively, intelligence authorities can order the provider to decrypt the message within 72 hours, "unless the provider demonstrates that it is unable to comply with these orders."[43] When making these orders, intelligence authorities must be acting in the context of a data-gathering mission authorized by the prime minister.

VI. RETENTION OF TRAFFIC DATA AND IDENTIFICATION DATA

France transposed the now-invalidated European directive on retention of traffic data,[44] but went beyond the minimum required by the directive. French law not only requires telecommunications operators to retain for one year traffic data (including location data and Internet logs[45]), but also requires hosting providers to retain similar logs relating to persons who create or store data using their hosting service.[46] The definition of hosting provider is similar to that in the European E-Commerce Directive,[47] and broad enough to include many cloud providers, social media services, blogs, and video sharing platforms. Under the French data retention decree, a hosting provider must retain all the information provided by the user when he or she registers for the service, including the user's name, pseudonym, address, telephone number, email address, password, information permitting the user to change the password, and payment information.[48]

42. Article L853-2, Internal Security Code.

43. Article L871-1, Internal Security Code.

44. Directive 2006/24/EC of March 15, 2006.

45. Decree n° 2006-358 of March 24, 2006.

46. Decree n° 2011-2019 of February 25, 2011.

47. Directive 2000/31/EC of June 8, 2000.

48. Decree n° 2011-219 of February 25, 2011.

When a user uploads content, the hosting provider must keep logs regarding the user's connection to the service. All the foregoing data are considered "identification data" and are subject to government access, either through a *requisition* under the French Code of Criminal Procedure, or through requests made by intelligence agencies under the Internal Security Code. France's data retention law goes beyond the requirements of the now-invalidated EU data retention directive by including hosting providers within its scope. France has not attempted to modify its laws since the CJEU's *Digital Rights Ireland* decision, which led a parliamentary commission to assert that France's laws on data retention violate Articles 7 and 8 of the EU Charter of Fundamental Rights.[49] As noted above, the Constitutional Court decision relating to the 2015 Law[50] made no mention of the *Digital Rights Ireland* decision. And on February 12, 2016, the *Conseil d'Etat* found that the provisions relating to access to metadata as they existed *before* the 2015 Law were surrounded by sufficient safeguards to satisfy European and French proportionality tests.[51]

The February 12, 2016 Conseil d'Etat decision suggests that the French data retention rules would be considered, at least by the French *Conseil d'Etat*, as satisfying the European proportionality test. Yet for this author, it is unclear that the CJEU and the ECtHR would agree, particularly after the recent CJEU decision finding UK and Swedish laws on data retention incompatible with the EU Charter of Fundamental Rights.[52]

VII. CONCLUSION

This chapter has shown that French procedures permitting government access to data in the context of criminal investigations are similar to those in other countries. The level of judicial oversight increases with the level of intrusion into privacy. Real-time interceptions of content require a prior judicial authorization whereas access to stored metadata can often be achieved without a prior authorization. One interesting aspect of the French Code of Criminal Procedure is that it expressly permits French authorities to obtain access to data stored in servers outside of France, as long as an authorized access point exists in France.

The French regime for intelligence data gathering was modified in 2015 in reaction to the heightened terrorist threat in France. The reform permitted a long overdue cleanup of the provisions applicable to intelligence data gathering. The previous provisions dated from early 1990s and related to traditional wiretaps.

49. French National Assembly, Commission de réflexion et de propositions sur le droit et le libertés à l'âge numérique, Rapport n° 3119 (2014), p. 166.

50. Constitutional Court decision of July 23, 2015 n° 2015-713 DC.

51. Conseil d'Etat decision of February 12, 2016, case n° 388134.

52. CJEU, Cases C-203/15 and C-698/15, *Tele2 Sverige v. Post-och telestyrelsen* and *Secretary of State for the Home Department v. Tom Watson and others*, December 21, 2016.

The new regime has the merit of creating a single coherent framework for data collection by intelligence authorities, including the creation of a single independent oversight body, the CNCTR. The new reform also makes certain intelligence-gathering techniques more explicit, such as the interception of communications of persons outside of France. Previously those practices existed, but had no legal framework. Among the new provisions is one permitting intelligence authorities to use algorithms to analyze large volumes of metadata in order to detect suspicious patterns of activity.

The French *Conseil d'Etat* and Constitutional Court have reviewed, or are in the course of reviewing, the constitutionality of most of these provisions. The 25-year-old provision allowing general monitoring of radio transmissions was recently declared unconstitutional by the French Constitutional Court, but other provisions have so far survived constitutional challenge. The French court decisions analyzing these provisions do not appear to apply the same kind of proportionality test as European courts do with regard to similar measures. It is unclear whether this is simply because the French courts provide less explicit reasoning in the text of their decisions, or whether French courts in fact apply a lighter version of the proportionality test. The recent CJEU decision invalidating UK and Swedish laws on data retention suggests that certain aspects of the French laws may violate the EU Charter of Fundamental Rights.

3

Systematic Government Access to Private-Sector Data in Germany

PAUL M. SCHWARTZ

I. ABSTRACT

German law has long been strongly committed to information privacy. Its protections are found at the constitutional and statutory levels. At the same time, legislation over the last two decades has expanded the ability of the government, including police and intelligence agencies, to process, store, and share personal information. The resulting databanks create elements of systematic data access for government to personal data in Germany. The leading examples of such access concern "strategic searches" by intelligence agencies, data mining by the police, the structured statutory system for access to the contents of the "Anti-Terror File," and the police's "radio-cell inquiries" pursuant to the Code of Criminal Procedure, § 100g. At the same time, German unease with systematic data access is shown by the ongoing controversies with data retention and the abandoned ELENA process. Complex questions have also been raised by private sector attempts to create a Germany-only "Cloud" as well as the significant and ongoing collaboration between German and US intelligence agencies.

II. NATIONAL LEGAL CONTEXT AND FUNDAMENTAL PRINCIPLES

Germany has a strong commitment to the rule of law and to information privacy. Its concept of the "rule of law" is best summed up in the idea of the *Rechtsstaat*. The *Rechtsstaat* is a "legal state" that is based on civil liberties as well as the expression and protection of constitutional rights. For example, Article 1(1) of the German Constitution, the Basic Law, states that human dignity is inviolable, and that the duty of all state authority is to respect and protect it.[1] Article 2(1)

1. Grundgesetz für die Bundesrepublik Deutschland [GG] [Basic Law for the Federal Republic of Germany, Basic Law], Bundesgesetzblatt III. [BGBl. III.] 100-1 (1949) (most recently amended by Law of Dec. 23, 2014, BGBl. I., 2438).

Bulk Collection. Fred H. Cate and James X. Dempsey.

guarantees the right of free development of the personality. Article 20(3) of the Basic Law, the German Constitution, explicitly binds all three branches of government to the constitutional order and to law and justice.

As for information privacy, it has constitutional status in Germany. The constitutional protections derive both from specific and more general constitutional provisions. These are Article 10 (privacy of communications), Article 13 (inviolability of the home), and Articles 1(1) and 2(1) (the basis for a judicially created "right of informational self-determination" and "right of trust and integrity in information systems"). Many decisions of the Federal Constitutional Court interpret and develop these provisions.

Federal and state data protection commissioners also play an important role in privacy policymaking in Germany. These officials are established under the Federal Data Protection Law (*Bundesdatenschutzgesetz*, or BDSG). They monitor the data use of the government and of the private sector, and they direct public attention to violations of privacy. The law of the European Union and German law provide strong protections for the independence of data protection commissioners.

Great public attention in Germany is directed to privacy issues. The constitutional complaint against a data retention law set a record in Germany for public participation in constitutional litigation; it was brought by 35,000 citizens. As another indication of this public interest, over 244,000 Germans opted out from Google Street View before it went live in 2010.[2] By 2011, Google had stopped updating Street View because of the cost of blurring images of buildings whose inhabitants objected to their residence appearing in this service. Finally, the media covers privacy and surveillance issues heavily, and there have been numerous popular general audience books on these topics, such as *Sie kennen dich! Sie haben dich! Sie steuern dich!* (2014) (They Know You! They Have You! They Control You!), *Finger Weg von Unseren Daten!* (2014) (Hands Off Our Data!), *Digitale Diktatur* (2014) (Digital Dictator), *Die Datenfresser* (2011) (The Data Eaters), and *Die Facebook Falle* (2011) (The Facebook Trap).

In reaction to terrorist attacks in the United States on 9/11 and subsequent terrorist actions throughout Europe, the Federal Parliament, or Bundestag, has enacted a wide-reaching series of laws that modified the structure under which German law enforcement agencies and intelligence organizations gather and share information. The trend of increased legislation about national security and crime had already started before 9/11; an initial round of legislation was driven by post-Cold War concerns about new threats to Germany in a Europe without traditional borders and the traditional postwar power blocs.

Although many in Germany emphasize the protection of informational self-determination and data protection, other views exist on how much to emphasize

2. For the statistics from Google, see "How Many German Households Have Opted-out of Street View?," *Google Europe Blog* (Oct. 21, 2010), http://googlepolicyeurope.blogspot.com/2010/10/how-many-german-households-have-opted.html.

information privacy. The founders of the Federal Republic structured it as a "militant democracy" (*wehrhafte Demokratie*). This idea meant that the liberal democratic order would be capable of protecting itself against those who would destroy it. From this idea, a core one in modern German politics, a series of interior ministers have stressed the importance of the state's protection of security and provided strong policy leadership for greater data sharing among government agencies and, under certain circumstances, between the private sector and government.

It was a small step after 9/11 to build on this idea of "militant democracy" and to advocate a "right to security." One of the leading advocates of this idea has been Manfred Baldus, a German law professor. In 2008, he warned, "A minimum of State leads not in the least to a maximum of freedom."[3] He argued that "real freedom depended as well on the exclusion of private violence" and "that the security function of the state, that is, the security of freedom from private violence that the state provides, counts as one of the essential and indispensable components of a state centered on freedom and based on the rule of law."[4] Less controversially, the historian Eckart Conze argues that the long-standing mission of the Federal Republic is a "search for security" for the German people after the destruction of World War II. Conze observes, moreover, that the terrorist threat post-9/11 served as a kind of "legal, political and moral 'unlocking action' " that acted to "strengthen the imperative of security."[5]

Thus, there has been a division in German politics and public policy discussions between the supporters of privacy and those more concerned about security. The revelations of Edward Snowden further heightened this division. Beginning in June 2013, Snowden leaked classified information from the National Security Agency about the global surveillance activities of the United States as well as European government agencies. In Germany, the matter was brought home by news that the NSA had monitored the cell phone of Chancellor Angela Merkel, the leader of the country. At this juncture, even some politicians from the CDU and CSU, the two conservative parties, joined in anti-American rhetoric. The widespread uproar was reflected by the cover of *Stern* magazine, a popular weekly, showing Uncle Sam with his fingers crossed behind his back with the headline: "The False Friend."

For some in Germany, Snowden is a folk hero. One pro-Snowden book, published in 2014, is titled: "111 Reasons to Support Edward Snowden."[6] Others are far from fans of Snowden. As an example of the latter view, Hans-Georg Maaßen, head of the Federal Bureau for Protection of the Constitution, sees Snowden as serving the interests of Vladimir Putin's Russia by driving "a wedge between the

3. Manfred Baldus, "Freiheitssicherung durch den Rechtsstaat des Grundgesetzes," in *Vom Rechtsstaat zum Präventionsstaat* 107, 109 (Stefan Huster & Karsten Rudolph, eds., 2008).

4. Ibid. at 109.

5. Eckart Conze, *Die Suche nach Sicherheit* 906 (München: Siedler, 2009).

6. Marc Halupczok, *111 Gründe Edward Snowden zu Unterstützen* (Berlin: Schwarzkopf, 2014).

US and its closest European ally, the Federal Republic."[7] The Snowden revelations and subsequent investigations have inspired political and public pressure in Germany to limit or restructure shared US-Germany intelligence activities. A goal upon which a majority of German politicians likely agree would be to place these activities on a stronger legal basis and to institute additional procedural safeguards. This task is proving to be a highly complex one. One difficulty has been the intertwined nature of the activities of US and German intelligence agencies, which will be explored below.

III. CONSTITUTIONAL, STATUTORY, AND REGULATORY OVERVIEW

A. Law

1. Constitutional Provisions

There is a significant body of constitutional law in Germany concerning information privacy. The specific constitutional protections for privacy include the Basic Law's Article 10, which creates constitutional norms regarding the government's ability to carry out the surveillance of communications, including letters and telecommunications. In addition, Article 13 protects the inviolability of the home and creates constitutional norms for the government's ability to carry out wiretaps within a residence. As Francesca Bignami observes regarding telecommunications privacy law, "At the constitutional level [in Europe] . . . only in Germany is the privacy of communications and data related to communications afforded protection under a separate article of the Constitution and a separate line of cases."[8]

The Basic Law's general provisions that safeguard privacy are Article 2(1) in conjunction with Article 1(1). The German Constitutional Court has read these provisions as protecting a general right of personality. In its *Data Screening* opinion of 2006, the Federal Constitutional Court observed that the general right of personality "is a gap-filling guarantee" that "is especially required against the background of novel dangers for the development of personality that appear in accompaniment to the progress of science and technology."[9] From this general right, the Constitutional Court has identified other important individual privacy rights. These are the right to a private sphere in which one is to be free to shape her life, a right to one's spoken word, and a right to informational

7. Hans-Georg Maaßen, 102. Meeting of Committee of Inquiry (102. *Sitzung des Untersuchungsausschusses*) (June 9, 2016). For media coverage, see Andre Meister, Live-Blog aus dem Geheimdienst-Untersuchungsausschuss: "Ob Snowden russischer Agent ist, kann ich nicht beurteilen," *netzpolitik.org* (June 9, 2016), at https://netzpolitik.org/2016/live-blog-aus-dem-geheimdienst-untersuchungsausschuss-verfassungsschutz-praesident-maassen-und-vorgaenger-fromm/#zeuge2.

8. Francesca Bignami, "European versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining," 48 *B.C. L. Rev.* 609, 639 (2007).

9. 115 BVerfGE 320, 341–66 (2006) [*Data Screening*].

self-determination. In 2008, the Court identified a new related interest, which was the right to "trust and integrity in information systems."[10]

As a general matter, the German constitutional law of information privacy, as established in the *Census* decision of 1983, permits a public sector entity to collect, process, and transfer personal information subject to a limited set of conditions.[11] One of the most important of these is the requirement that there be a statutory basis for this informational activity. Such a legal basis requires that all personal data processing have a valid legislative basis, clearness of norms, and observance of the "principle of proportionality" (*Verhältnismäßigkeitsprinzip*). The principle of proportionality consists of a three-prong test for evaluating the constitutionality of legislation. First, the Court asks whether the means chosen are suitable (*geeignet*). Second, it inquires whether the means chosen are necessary (*erforderlich*). Finally, the Court examines whether the means chosen are reasonable (*zumutbar*).

Building on the existing constitutional framework, the right to trust and integrity in information systems safeguards the right of citizens to trust their digital networks. The Constitutional Court has termed this interest "a guarantee of confidentiality and integrity in information systems." Invasions of this right are permitted only within narrow borders. Thus, an invasion of it for a "preventive governmental purpose" requires actual indications of a concrete danger to a predominately important legal interest.[12]

Due to these important provisions of the Basic Law, and the extensive case law of the Constitutional Court, this Court plays a central role in deciding questions relating to the boundaries of governmental access to private-sector data. The Constitutional Court's significant involvement in these matters is one of the most visible manifestations in the context of data protection of the German commitment to the rule of law. Regarding the topic of systematic government access to data, there are important constitutional decisions concerning strategic searches (the *G-10* opinion) (1999), data screening (2006), automated number plate recognition (2008), data retention (2010), the counterterrorism database (2013), and the counterterrorism role of the Federal Criminal Police (the *BKA* opinion).[13]

In addition, decisions of the Constitutional Court concern the protection of a "core area of life formation."[14] These opinions examine acoustic wiretaps within

10. 120 BVerfGE 274, 302 (2008) (*Online Search*).

11. 65 BVerfGE 1 (1983) (*Census*).

12. 1 BvR 370/07, ¶ 242 (2008) (Right to Trust and Integrity in Information Systems).

13. 100 BVerfGE 313, (1999) (*G-10*); 115 BVerfGE 320, (2006) (*Data Screening*); 125 BVerfGE 260 (2010) (*Data Retention*), subsequently BGH, Decision July 3, 2014 (III ZR 391/13) (Data retention constitutional for seven days, because retention is not meant for law enforcement purposes).

14. 109 BVerfGE 279 (2004) (*Great Eavesdropping*); 113 BVerfGE 348 (2005) (*Preventive Telecommunications Surveillance*); Case 1 BvR 1215/07 (2013) [Bundesverfassungsgericht]

residences (2004), preventive telecommunications surveillance (2005), the counterterrorism database (2013), and the counterterrorism role of the Federal Criminal police (the *BKA* opinion). The Constitutional Court of Germany has been involved in a profound effort to draw on the nation's constitutional norms to develop standards for systemic data use.

a. The *G-10* Opinion (1999)

The *Bundesnachrichtendienst*, or BND, and other German intelligence agencies are permitted to engage in surveillance of letters, conversations, or telecommunications through two kinds of legal processes. First, the surveillance can take place as an "individual investigation," which involves the collection of personal data to investigate criminal behavior that threatens the survival of Germany or its democratic order. Second, the surveillance can take place as "strategic surveillance." Later in this chapter, I discuss the current statutory requirements regarding strategic surveillance for the BND and the other institutions that are part of the German intelligence community. This section will examine the constitutional requirements before such activity can occur. These standards must then be reflected in the applicable statutory framework.

In the Constitutional Court's *G-10* opinion, the strategic surveillance in question involved observation of telegram, fax, and, to a lesser extent, telephone traffic transmitted via satellite.[15] The government admitted during oral argument that the BND had plans for surveillance of emails, but the Court did not provide further details in its opinion about this activity. Today, such searches extend to emails as well as to web fora.[16]

In its *G-10* opinion, the Constitutional Court found that the protections of the Basic Law's Article 10 were not limited exclusively to communications that took place entirely within the national borders of Germany. As long as enough of a nexus existed between the surveillance and German territory, the protections of Article 10 were applicable.[17] The Court identified such a nexus in the *G-10* case, where the governmental surveillance activity occurred from within Germany and at least part of the communications ended or originated from within Germany.

The Constitutional Court also found that the dangers of such surveillance were considerable. Most important, it pointed to the risk that such surveillance would lead to "a nervousness in communication, to disturbances in communication, and to behavioral accommodation, in particular to avoidance of certain

(*Counter-Terrorism Database*); Case 1 BvR 966/09 (2016) [Bundesverfassungsgericht] (*BKA-Opinion*).

15. 100 BVerfGE 313 (1999) (*G-10*).

16. Unterrichtung durch das Parlamentarische Kontrollgremium, Deutscher Bundestag, 17. Wahlperiode, Drucksache 17/4278, p. 7 (2010).

17. 100 BVerfGE 313, 363–64 (1999) (*G-10*).

content of conversations or terms." For the German Court, the threat was to social communication. In American terms, this idea is similar to that of a chilling impact on speech.

After noting the dangers posed by the data collected in the *G-10* case, the Constitutional Court nevertheless found the surveillance to have a strong justification. The activity to be placed under observation "affected the foreign and security politics of the Federal Republic . . . to a significant extent."[18] Moreover, the law permitted the collection of information necessary to detect dangers to Germany. As a result, the Constitutional Court declared that the G-10 statute was generally "not improper."

Although the Court did not declare the entire statute to be void, it did find several aspects of it to be unconstitutional.[19] Among the elements of the law that it struck down were certain provisions concerning the BND's transfer of personal data to other agencies. These transfers were only permissible when the controlling legislation was consistent with the principle of proportionality. Judicial review pursuant to a proportionality analysis is one of the Constitutional Court's most important tools when confronted with statutes that infringe upon privacy. In the *G-10* case, in a demonstration of this technique, the Constitutional Court decided the applicable statute did not limit these data transfers in a permissible fashion.

To be sure, the Court found, as a general matter, that it was constitutional for the BND to share with other agencies information gained from its surveillance of telecommunications traffic to the extent that the data in question revealed criminal behavior. The failing of the statute was, however, that it did not restrict data sharing to instances in which serious crimes had been committed, as opposed to more minor delicts. This lowered threshold did not meet the proportionality test. The Court also found that the statute allowed a sharing of the BND's information in a manner that was too widespread. The Court required the enactment of new statutory standards for the BND and other intelligence agencies that restricted transfer of information in a manner similar to limits placed on domestic law enforcement agencies when engaged in the "individual investigation path."[20]

These new requirements do not present major obstacles to strategic searches, which are regulated in the G-10 Statute, Sections §§ 5–8. I discuss this statute later in this chapter; here, however, one might briefly consider the recent statistics concerning use of this technique by the German intelligence services. According to the 2014 statistics from the Parliamentary Control Panel (*Parlamentarische*

18. Ibid. at 382.

19. For example, the statute's § 3(1) no.5 permitted international surveillance for investigations of the counterfeiting of currency. The Constitutional Court found that the statutes allowing surveillance to prevent this crime did not follow the principle of "proportionality." Ibid. at 385. It noted, however, that such surveillance would be constitutionally permissible if the strategic surveillance was limited to cases that threatened "the stability of the value of the currency of Germany and thereby the economic power of the country." Ibid.

20. 100 BVerfGE 313, 385–386 (1999) (*G-10*).

Kontrollgremium) on the use of relevant statutory authorities, German intelligence agencies relied upon the statutory justification regarding "international terrorism" in searching 14,604 examples of "telecommunications traffic."[21] The official report explained that this number resulted in the capturing of one fax, four telexes, one email, 197 voice communications, and 13,329 text messages. In regard to "proliferation and conventional armaments," 11,670 searches were ordered. These searches were made of 10,588 examples of telecommunications traffic.

b. The *Data Screening* Opinion (2006)

Data mining is an established technique of law enforcement authorities. Its use in Germany dates back to the 1970s and the country's struggle against the Red Army Faction (RAF). The German term for this practice is "*Rasterfahndung*," or a "screening search."[22]

In its *Data Screening* opinion of 2006, the German Constitutional Court found that data screening posed a significant infringement of the right of informational self-determination. In this opinion, the Court used its existing proportionality test as a constitutional yardstick for evaluating the permissibility of data screening. The *Data Screening* opinion involved a search carried out after the terrorist attacks in the United States on 9/11. The German data mining search was made in hopes of discovering "sleeper terrorists" in Germany.

The criminal police collected personal data from universities, the Registration Office for Inhabitants, and the Central Register for Foreigners. According to the Constitutional Court, the different police headquarters received "data batches" with information on 5.2 million persons. The information collected at the state level was then transferred to the Federal Criminal Police Office (*Bundeskriminalamt*, or BKA), where it was incorporated into a federal database termed "Sleepers." The data screening was notably unsuccessful, and the government erased all information in the "results file" by 2004.

In Germany, laws at the federal and state levels distinguish between the use of "data screening" to (1) investigate past crimes, or (2) permit a preventive response to potential crimes. Data screening to investigate past crimes is regulated by various state laws and at the federal level by Section 98a of the Criminal Procedural Code (*Strafprozeßordnung*).[23] The federal statute applies when the BKA takes a lead role in investigating crimes considered to be a federal matter.[24]

21. Unterrichtung durch das Parlamentarische Kontrollgremium, Drucksache 18/7423, p. 7 (2016).

22. In this discussion of the Data Screening opinion, I draw on my article, "Regulating Governmental Data Mining in the United States and Germany," 53 *William & Mary Law Review* 351 (2011).

23. Strafprozeβordnung [StPO] [Criminal Procedure Code], Bundesgesetzblatt I. [BGBl. I.] 1074, 1319 (1987) (most recently amended by Law of Dec. 22, 2011, BGBl. I., 3044), § 98a.

24. The Criminal Procedure Code's basic approach reflects the approach the different state laws take, and our discussion will, therefore, concentrate on the federal statute.

In Section 98a, the Criminal Procedure Code regulates the "automatic comparison and transfer of personal data." It requires "sufficient factual indications to show that a criminal offense of significant importance has been committed." Thus, this statute squarely requires proof of the existence of a crime.

In contrast to this federal law, there are state statutes in Germany that permit a preventive use of this practice.[25] In 2006, in its *Data Screening* opinion, the German Federal Constitutional Court established significant limits on such law enforcement use of data screening.[26] The Court found that the state's activity raised issues concerning the threat of modern means of surveillance to an individual's underlying communicative ability. It also acknowledged that individuals were obligated to accept limitations on their right of informational self-determination that were justified by weightier public interests. In its use of proportionality review, the Constitutional Court found that data screening statutes are constitutionally permissible only when there was "a concrete danger" to a legal interest. Through this aspect of the *Data Screening* opinion, the Constitutional Court did more than invalidate the state law before it. It also raised significant questions about the majority of the other state laws that permitted preventive data searches.[27]

At the same time, however, the Constitutional Court did *not* declare data screening to be per se disproportionate and, hence, facially unconstitutional. Its decision was that law enforcement officials had to demonstrate the existence of a certain risk of danger before using this technique. At this juncture, the Court placed a significant limit on preventative use of data screening. As the Constitutional Court stated, a concrete danger was "a prognosis of probability" based on facts that the predicted harm would occur. The Constitutional Court added, "Vague clues or bare suppositions are not sufficient."[28] Rather, data screening required proof of actual preparations for a terrorist attack. Such evidence showing a concrete danger would include, for example, "factual clues for the preparation of terrorist attacks or the presence in Germany of persons who are preparing terrorist attacks that in the near future will be perpetrated in Germany or elsewhere."

c. *Automatic Number Plate Recognition (ANPR)* Opinion (2008)

Beyond the use of data screening by the intelligence agencies in Germany, another type of systemic data use concerns automatic number plate recognition

25. See, for example, Polizeigesetz des Landes Nordrhein-Westfalen [PolG NW] [North Rhine-Westphalia Police Statute], Gesetz- und Verordnungsblatt für das Land Nordrhein-Westfalen [GV NRW] 410 (2003), § 31.

26. 115 BVerfGE 320 (2006) (*Data Screening*).

27. Winfried Bausback, "Fesseln für die wehrhafte Demokratie?," 59 *NJW* 1922 (2006), p. 1922, 1924.

28. 115 BVerfGE 320, 339 (2006) [Data Screening].

(ANPR) systems.[29] Indeed, law enforcement agencies throughout Europe use these systems to detect and track criminals and terrorists. In 2008, the German Constitutional Court invalidated two state ANPR laws and identified constitutional norms for statutes authorizing the collection and storage of such information.

For the Constitutional Court, there was a threshold question of when the police's automatic detection of motor vehicle license plates implicated the right of informational self-determination. Such constitutional protection was compromised whenever law enforcement did not make its comparison of a plate number immediately and did not at once erase non-matching information. For the Court, the protections of the Basic Law extended to the collection and storage of ANPR data in databanks. As the Constitutional Court stated, "Even if the acquisition of a larger dataset is ultimately only a means to the end for a further reduction of the number of hits, the collection of information can be invasive in making the information available to the authorities and in creating the basis for the subsequent comparison with search terms."[30] The Court also found that constitutional protections attach to information that is publicly viewable—such as the license plate number of a vehicle that is being driven. The right of information self-determination protects such information from "automated information collection for storage with a possibility of further use."

The *ANPR* Opinion then turned to the established constitutional test regarding proportionality. It found that the nature and intensity of the invasion of a constitutional interest depended on the specific context of the use of the ANPR system. A heightened interest was present where the ANPR system was used for further purposes beyond finding a specific motor vehicle or when it collected a "movement profile." The Constitutional Court found that the state legislation under review failed to create sufficient limited and clear norms for constitutional use of ANPR.

d. The *Data Retention* Opinion (2010)

Pursuant to its obligations under the European Union's Data Retention Directive, Germany enacted a data storage obligation in its "Act for the New Regulation of Telecommunications Surveillance" (*Gesetz zur Neuregelung der Telekommunikationsüberwachung*) on December 21, 2007. This statute amended the Telecommunications Act, or TKG. On March 11, 2008, the Constitutional Court issued a temporary injunction that suspended certain parts of the statute. In 2010, the Court issued an opinion that struck down the statute.

29. For a legal discussion of online services such as Google Street View, see Thomas Dreier and Indra Spiecker genannt Döhmann, *Die systematische Aufnahme des Straßenbildes: Zur rechtlichen Zulässigkeit von Online-Diensten wie "Google Street View"* (Baden-Baden: Nomos, 2010).

30. Case 1 BvR 2074/05 (2008) [Bundesverfassungsgericht] (*Automatic Number Plate Recognition*).

The German data retention statute required suppliers of telecommunication services to store specific kinds of traffic and location data for a period of six months. By choosing this term of a half year, the Bundestag opted for the minimum retention period then required by the European Data Retention Directive. The newly drafted statutory provisions were inserted into the Telecommunications Act at §§ 113 a, 113 b TKG. The first provision, § 113 a, TKG, contained the obligation for a six-month retention period and specified the kinds of data that were to be stored. The second, § 113 b TKG, set out the conditions under which law enforcement officials could gain access to the stored data.

In its 2010 opinion, the Constitutional Court declared that storage of telecommunications data, including traffic data, constituted a serious encroachment on individual rights. Even though the storage was not of content, it was still possible to use the data to make "content-related conclusions that extend into the users' private sphere."[31] The result might even permit the drawing of "personality profiles of virtually all citizens." Nonetheless, the Constitutional Court found that data retention could be made compatible with Article 10(1) of the Basic Law. Despite the potential dangers of data retention, access to information about telecommunications connections was of particular importance for "effective criminal prosecutions and prevention of danger."

Despite the potential of this information to assist law enforcement and intelligence agencies, the Constitutional Court decided that the data retention statute had fatal flaws. To be constitutional, such a statute needed well-defined provisions for data security, limits on the use of data to investigations of particularly serious crimes, sufficient transparency about its use for the public, and judicial control of transmission and use of the stored data.[32] In addition, statutory prohibitions were required on obtaining access to certain kinds of privileged professional data, such as communications with religious officials or lawyers.[33] Interestingly enough, the Constitutional Court explicitly declared that IP addresses were subject to less stringent constitutional standards. Although the question of accessing IP addresses would impact on the extent to which anonymous communication could take place, the Court nonetheless found that such information could be disclosed based on "a sufficient initial suspicion or a concrete danger," or even for a significant regulatory offense, that is, a non-criminal matter.

Subsequent to the *Data Retention* opinion, the Bundestag enacted another data retention directive, which the *Bundesgerichtshof* upheld in 2014.[34] Further muddying the waters, the European Court of Justice (ECJ) in its *Digital Rights Ireland* decision (2014) found the European Data Retention Directive to violate

31. 125 BVerfGE 260 (2010) (*Data Retention*).

32. See ibid. at 260–61.

33. See, for example, German criminal procedure provision StPO § 160a.

34. Federal Court of Justice, Case III ZR 391/13 (2014) [Bundesgerichtshof].

the European Charter of Rights.[35] The ECJ struck down this Directive as violative of the Charter's Article 7 (privacy), Article 8 (data protection), and Article 52 (proportionality). The European Commission announced in September 2015 that it would not develop any further data retention measures, but would permit Member States to establish their own rules.[36] In 2015, the Bundestag enacted another data retention bill, which, among other provisions, requires telecommunications providers to store all data required by the law within Germany.

e. *Counter-Terrorism Database* Opinion (2013)

The Constitutional Court returned to the issue of the constitutional requirements for data mining in its *Counter-Terrorism Database* opinion.[37] This decision found that the Counter-Terrorism Database Act was "in its fundamental design compatible with the right to informational self-determination."[38] The counter-terrorism database itself had a legitimate aim and the challenged provisions of the Act were "suitable and necessary" to achieve its goal "of a limited facilitation of information transfer" among security agencies and law enforcement authorities.[39] Yet, the Constitutional Court also found that the challenged provisions were subject to heightened constitutional requirements because they involved a sharing of information between the police and intelligence services. The legal order in Germany distinguished between the function of the police and the intelligence services, and held that they necessarily must limit their sharing of personal information with each other. Since the end of World War II and the creation of the Federal Republic of Germany, this idea has been a fundamental one in German law; the doctrine is called the "*Trennungsgebot*," or "Separation Rule."

As part of the right of informational self-determination, German constitutional law creates a related concept to the "Separation Rule," which is that of a "principle of separation of information" (*informationelles Trennungsprinzip*). Due to this principle, the exchange of information between intelligence services and the police is generally forbidden and permitted only by exception. The Constitutional Court found numerous aspects of the Counter-Terrorism Database Act that did not meet its heightened scrutiny. These pertained to the range of persons included in the database as "affiliated with terrorism," the way

35. Joined Cases C–293/12 and C–594/12 *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and others*, and *Seitlinger and others* [2014] ECLI:EU:C:2014:238.

36. European Commission Statement on National Data Retention Laws (Sept. 16, 2015), at http://europa.eu/rapid/press-release_STATEMENT-15-5654_en.htm. For an overview of the data retention laws of Member States, see EU Agency for Fundamental Rights, Data Retention across the EU, at http://fra.europa.eu/en/theme/information-society-privacy-and-data-protection/data-retention.

37. Case 1 BvR 1215/07 (2013) [Bundesverfassungsgericht] (*Counter-Terrorism Database*).

38. Ibid. at ¶ 105.

39. Ibid. at ¶¶ 106–107.

in which "contact persons" were included, the way in which "extended basic data" were included, and the lack of a guarantee of effective supervision by data protection commissioners. The law also interfered with constitutional guarantees for the privacy of correspondence and telecommunications (Article 10, Basic Law) and the right to the inviolability of the home (Article 13, Basic Law).[40]

f. *Federal Criminal Police Office (BKA)* Opinion (2016)

In 2009, the Bundestag assigned a significant role combatting international terrorism to the BKA. The legislation authorized the BKA to carry out covert surveillance in the context of protecting against threats from international terrorism and the prevention of criminal offenses and to transfer data to other authorities both inside and outside of Germany. In 2016, the Constitutional Court found that the legislation was unconstitutional in part.[41] For the Constitutional Court, the resulting powers were not objectionable "in principle," but these powers were "to be restricted to the protection of sufficiently weighty legally protected interests"[42] and to be used "only in those cases in which there is a sufficiently specific foreseeable danger to these interests."[43]

The *BKA* opinion provided highly detailed requirements for the BKA's covert surveillance. For example, the Court found that the requirements for the use of data beyond the original investigatory purpose were not entirely sufficient. There were also flaws in the protection of professional confidentiality, in particular regarding the communications of defense counsel and other lawyers. The Court also identified shortcomings in the statute's provisions on transparency, on transfer of data to other domestic authorities, and on transfers to other countries.

In separate dissents to the *BKA* opinion, Justice Michael Eichberger and Justice Wilhelm Schluckebier argued that the majority of the Constitutional Court was interfering with the legislative role by articulating excessively detailed requirements.[44] Justice Eichberger also drew a distinction between investigations that were targeted and those that collected data more broadly. In his view, many of the challenged statutory provisions did not "authorize a general collection of data affecting a wide range of persons."[45] He felt that individuals affected by instances of more specific targeting could constitutionally be expected to sacrifice some of their privacy as part of "a citizen's duty for the public guarantee of security."[46]

40. Ibid. at ¶ 224.

41. Case 1 BvR 966/09 (2016) [Bundesverfassungsgericht] (BKA-Opinion).

42. Ibid. at ¶ 156.

43. Ibid. at ¶ 109.

44. Dissenting Opinion Justice Schluckebier, Case, 1 BvR 966/09 (5, 7) (2016) [*Bundesverfassungsgericht*] (BKA Opinion).

45. Dissenting Opinion Justice Eichberger, Case 1 BvR 966/09 (4, 5) (2016)

46. Ibid.

g. Protecting the Home: the *Great Eavesdropping* Opinion (2004), *the Preventive Telecommunications Surveillance* Opinion (2005), the *Counter-Terrorism Database* Opinion (2013), and the BKA Opinion (2016)

In four important decisions, the Constitutional Court assessed the nature of Article 13's protection of the home and the "core area of life formation." These opinions followed amendments to the Basic Law in 1998 that explicitly permit acoustic and visual surveillance of the home. Until then, there had been some open questions about the extent of Article 13's protection of the privacy of private residences. Article 13(1), which dates to the enactment of the Basic Law in 1949, states, "The home is inviolable." Yet, the Basic Law's Article 13(2), also found in its original text, permits judges to order searches. The debate had been about whether surveillance was permissible within the home and whether such surveillance could occur in bedrooms and other areas associated with intimate activities.

The 1998 amendment to the Basic Law resolved certain but not all aspects of this debate. This constitutional amendment added new subsections to Article 13 of the Basic Law. Of these, the critical new section, Article 13(4), states, "To avert acute dangers to public safety, especially dangers to life or to the public, technical means of surveillance of the home may be employed only pursuant to judicial order." Thus, the Basic Law after 1998 explicitly permits at least some surveillance within the home while also continuing to protect "the inviolability of the home." In a series of subsequent decisions, the Constitutional Court assessed the extent to which such surveillance could occur consistent with the Basic Law.

First, in its *Great Eavesdropping* opinion (2004), the German Constitutional Court upheld the 1998 amendments as constitutional.[47] In its view, the Basic Law does not provide absolute protection for the *space* of private residences. Rather, its absolute protection was provided to *behavior* in this space that "depicts individual development in the core domain of private life formation."[48] In the Court's view, the constitution's protection of physical spaces turned on how people used these areas. In particular, its ruling held that "the greater the probability of capture of highly personal content, the stricter the requirements for lawfulness of surveillance of living quarters."[49]

Second, the Constitutional Court elaborated on the nature of these requirements in its *Preventive Telecommunications Surveillance* opinion (2005). It stated that preventative surveillance would be constitutionally acceptable only when "there was an especially high ranking endangered legal interest and a designated situation with concrete stopping points and a connection through direct references to the future carrying out of a criminal offense."[50] Moreover, it was

47. 109 BVerfGE 279 (2004) (Great Eavesdropping).

48. Ibid.

49. Ibid. at 328.

50. 113 BVerfGE 348, 392 (2005) (Preventive Telecommunications Surveillance).

sometimes not possible to know when a conversation might touch on the core domain of private life formation.[51] As a result of law enforcement not being able to predict the content of conversations in advance, the Constitutional Court required these officials to actively monitor their surveillance and to stop it immediately if the private domain of life formation was implicated. As an additional safeguard, there was a need for specific protections to guarantee that communications from the "highly personal domain" would not be stored and subject to further use. As an example of such protection, if such material was collected, it was to be immediately erased.[52]

Third, in the *Counter-Terrorism Database* opinion (2013), the Constitutional Court noted that personal information to be included in the database could be obtained in ways that impinge on the inviolability of the home. Such information, as well as that data which interferes with telecommunications privacy, were to be labeled as such in the database. The Court observed, "The recognisability of such data is intended to ensure that the specific limits on data use are obeyed even after the data may have been forwarded to other agencies."[53] The law must then "ensure specific thresholds" for any transfers and use of this information. Without such metadata labeling on this sensitive information, its collection would not be constitutional. Moreover, the data were only to be collected subject to strict standards and an elevated showing of need, "such as an especially dangerous situation or a specific suspicion of an offence, a threat to especially significant legally protected interests, or the prosecution of especially serious criminal offences."[54]

Fourth, the *BKA* opinion, also discussed above, evaluated the statutory powers of the Federal Criminal Police Office to covertly collect personal data from private homes. The Court noted that the surveillance of private homes represented a "particularly serious interference with privacy" and could, therefore, be justified only when it focused "exclusively on the communications of the target person from whom the threat emanates."[55] The Court found that the legislation

51. Some information would fall on one side of the constitutional dividing line—other, on the constitutionally-protected side. As an example of kind of information that could be collected without concerns about the "core domain of private life formation," the Court pointed to content that made "direct reference to concrete criminal actions, such as statements about the planning of approaching criminal offenses, or reports about perpetrated criminal offenses." Ibid. at 391.

52. Ibid. at 392; see also Case 2 BvR 1513/14 (2014) [Bundesverfassungsgericht] (unconstitutional to broadly interfere with a custodian's direct and unrestricted communication with third parties, without balancing on a case-to-case basis the individual's right to privacy against such limitations).

53. Case 1 BvR 1215/07 (¶ 225) (2013) [Bundesverfassungsgericht] (*Counter-Terrorism Database*).

54. Ibid. at (¶ 226) (2013).

55. Case 1 BvR 966/09 at (¶ 151) [2016] [*Bundesverfassungsgericht*] (BKA Opinion).

expanding the BKA's authority failed to take such a step, as well as neglected to assign an independent person, one not charged with security tasks, to screen access to the BKA's "information technology systems."[56]

2. Statutory Law

German privacy law regulates information privacy through an omnibus law, the BDSG,[57] and sectoral laws.[58] As a general matter, the BDSG controls as far as there is not a more specific sectoral statute that is applicable. For online communications and other forms of telecommunications, there is the added legal wrinkle of the "*Schichtenmodel*," or "Layer Model."

The "Layer Model" functions through different legal requirements for content, services, and the technical level of transmission. As for the *content* of an online communication, it is regulated either by the BDSG or any applicable legislation. As for *services* that are provided on the Internet, these are regulated by the *Telemediengesetz*, or Telemedia Law.[59] Concerning the *level* at which the transfer takes place, it is regulated by the *Telekommunikationsgesetz*, or Telecommunication Law.[60] As a further matter, the law uses a different range of statutory authorities to govern the access to communications by domestic law enforcement and intelligence agencies (see below).

Not surprisingly, it can be quite difficult to determine which statute applies to a given dimension of an online service or communication. As Thomas Hoeren notes, "Due to the acceleration of legislative activity in recent years, more and more special laws have been added to data protection law, without careful coordination of the application areas of the resulting statutes."[61] Voice over Internet Protocol (VoIP) and other aspects of technical convergence have only added to the difficulty in maintaining a distinction, for legal purposes, among the layers.

56. Ibid. at ¶ 30.

57. Bundesdatenschutzgesetz [BDSG] [Federal Data Protection Statute], Bundesgesetzblatt I. [BGBl. I.] 66 (2003) (most recently amended by Law of August 14, 2009, BGBl. I., 2814).

58. For example, there are special data protection provisions for prisoners. See Strafvollzugsgesetz [StVollzG] [Criminal Penalty Enforcement Statute], Bundesgesetzblatt I. [BGBl. I.] 581, 2088 (1976) (most recently amended by Law of July 29, 2009, BGBl. I., 2274), §§ 179–187.

59. Telemediengesetz [TMG] [Telemedia Law], Bundesgesetzblatt I. [BGBl. I.] 179 (2007) (most recently amended by Law of May 31, 2010, BGBl. I., 692). For a discussion of the "Layer Model," see Wissenschaftliche Dienste des Deutschen Bundestags, *Die Verletzung datenschutzrechtlicher Bestimmungen durch sogenannte Facebook Fanpages und Social-Plugins* (October 7, 2011), p. 10, https://www.datenschutzzentrum.de/facebook/material/WissDienst-BT-Facebook-ULD.pdf.

60. Telekommunikationsgesetz [TKG] [Telecommunication Law], Bundesgesetzblatt I. [BGBl. I.] 1190 (2004) (most recently amended by Law of December 22, 2011, BGBl. I., 2958).

61. Thomas Hoeren, Wenn Sterne kollabieren, entsteht ein schwarzes Loch—Gedanken zum Ende des Datenschutzes, ZD 145–46 (2011).

An evaluation of German statutory law regarding the government's systematic data access is, therefore, quite complex. As a basic matter, however, German data protection law itself represents a considerable hurdle to systematic data access. The use of and access to personal data generally requires a legal basis. German law expresses this concept as a "*Verbot mit Erlaubnisvorbehalt*," or a "prohibition with conditional permission." German law starts by forbidding the collection, processing, or use of personal data. This prohibition is lifted, however, once a statute authorizes the data collection, processing, or use in question. This statute must, of course, also fulfill the proportionality requirement of German law.

Under the BDSG, moreover, data can be processed, shared, and transferred only under a limited set of circumstances. BDSG, § 14(1) provides one of the most important of these restrictions for public entities. It limits the "storage, alteration, or use of personal data" by private bodies to circumstances when it is "*necessary* to carry out the tasks for which the controller is responsible and for *the purpose for which the data were collected*" (emphasis added). Thus, this passage sets a standard of necessity as well as a requirement of "original purpose specification." BDSG, § 15(1) places similar kinds of restrictions on data transfers to public bodies.

B. Law Enforcement, Regulatory, and National Security Access

1. Basic Organizational Concepts and the "Anti-Terror File"

As in US law, German law distinguishes between law enforcement and intelligence agencies. The two countries also share a distinction between domestic intelligence and foreign intelligence agencies. Law enforcement agencies are generally tasked with enforcing the criminal code and policing violations of it. Intelligence agencies gather and analyze information that is needed to protect national security.

The *Bundesnachrichtendienst,* or BND, is the German agency for foreign intelligence. Unlike the United States, however, Germany has a separate domestic intelligence agency: the Federal Office for the Protection of the Constitution, or the *Bundesamt für Verfassungsschutz*. This agency is dedicated to threats against the democratic order of Germany; it also has counterparts in each German state. The federal and state offices for the protection of the constitution have traditionally lacked police powers, such as the ability to perform arrests. Finally, the federal investigative police authority is the Federal Criminal Police Office, the *Bundeskriminalamt*, or BKA.[62]

The development of the federal police, the BKA, and its role in Germany have long been controversial issues. The Gestapo, the centrally-organized police force of the Nazis, casts a long dark shadow. In addition, East Germany's *Ministerium für Staatssicherheit*, or Stasi, provided a later negative example from German

62. An important organizational distinction can be made with the United States, where the Federal Bureau of Investigation (FBI) has traditionally functioned as both the federal police authority, like Germany's BKA, and as a domestic intelligence agency, such as Germany's Federal Office for the Protection of the Constitution.

history of a centrally-organized agency for domestic security. Another factor in the debate about the proper role of a federal police force has been the desire of the German states to keep their own independent authorities for policing and gathering intelligence.

As a result of these factors, since the end of World War II and the creation of the Federal Republic of Germany, a fundamental legal concept has been the "*Trennungsgebot*," or "Separation Rule." The *Trennungsgebot* expresses a legal norm for organizational and informational divisions between intelligence and law enforcement agencies. For example, this legal concept would prevent the creation of a single German agency with borderless law enforcement and intelligence capacities, or the limitless sharing of information between law enforcement agencies and intelligence agencies. The rough analogy would be with the concept of "the wall" in the US regulation of the intelligence community. In both countries, legal limits on information sharing between intelligence agencies and law enforcement organizations are viewed as necessary for the protection of civil liberties.

Nonetheless, German law does not require a total ban on law enforcement agencies and intelligence agencies working together and sharing information. Indeed, a significant development in Germany, and one pre-dating 9/11, has been a stream of legislation that expands the powers of the BKA, BND, and Federal Office for the Protection of the Constitution, as well as related agencies, and increases their ability to work together and to share information.

One of the best examples of this trend is provided by the creation of an "*Anti-Terrordatei*," or "Anti-Terror Database." Through enactment of federal legislation in 2006, Germany established this databank, which consists of a common data source with an extended index. Already by 2011, the information in the Anti-Terror Database was collected from 38 different security authorities and concerned approximately 18,000 individuals considered to require scrutiny.[63] Although a number of different agencies can search the databank, and do so electronically, the database is constructed to distinguish information in "open" and "concealed storage."

If information in the database is in "open storage," a match to a suspect's name will reveal information about him. If information is in "concealed storage," the inquiring agency will receive a negative result to its search for data about a person. At the same time, however, the agency that has stored the information in "concealed storage" will receive data about the inquiry. That agency is then to decide whether the applicable legal rules permit it to share further information with the inquiring agency. In 2006, German civil libertarians awarded a Big Brother Award to the Conference of Interior Ministers for their role in establishing the Anti-Terror database.[64]

63. Drucksache 17/6233, Deutscher Bundestag, 17. Wahlperiode 8 (2011), http://dipbt.bundestag.de/dip21/btd/17/062/1706223.pdf.

64. Big Brother Awards, Politics II: Interior Ministers, http://www.bigbrotherawards.de/2006/.pol/pol-02.

As noted above, the Constitutional Court has identified flaws in legislation assigning the BKA a role opposing terrorism and in the statute establishing the Anti-Terror Database. Most critically, and as part of the right of informational self-determination, the Court identified the concept, that of a "principle of separation of information" (*informationelles Trennungsprinzip*). This principle serves to create strict limits on the exchange of information between intelligence services and the police.

2. Intelligence Agencies

a. Strategic Surveillance: The Basic Structure

German constitutional law permits the BND to engage in so-called strategic surveillance. Subsequent to the Constitutional Court's *G-10* decision, the Federal Parliament, the Bundestag, amended the applicable statutory authorities to make the law conform with the Basic Law. In 2009, the Bundestag again amended the relevant statute, the "G-10 Statute," or, more formally, the "*Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses,*" to provide additional surveillance powers to the BND. In addition, as noted above, federal and state intelligence agencies, as well as police authorities, can also gain access to electronic data in the Anti-Terror Databank.

The G-10 Statute is, however, the main statute regulating the BND's access to letters and telecommunications. This law's §§ 5–8 contain the provisions applicable to strategic surveillance. Its § 5(1) lists the nature of the dangers that justify the use of strategic surveillance. These include the risk of an armed attack on Germany, the committing of international terrorist attacks with a direct relation to Germany, international trafficking in weapons of war, drug trafficking, or a limited set of other significant dangers. The statute also sets obligations for the BND to check whether the collected personal data are "necessary" to one of the Article 5(1) purposes. If not, such data are to be immediately erased.

Following the enactment of statutory amendments in 2009, the G-10 Statute contains a specific section that protects a "core area of private life formation" in the context of both individual surveillance and preventive surveillance. The 2009 amendments to the G-10 Statute reflect the constitutional safeguards that the Constitutional Court identified in its *Great Eavesdropping* opinion (2004) and *Preventive Telecommunications Surveillance* opinion (2005). In particular, the G-10 Statute, § 5 a contains an absolute prohibition on capture of communications from the core area of private life formation.[65] Should such information, nonetheless, be collected, authorities may not use them and these data are to be erased at once.[66] A protocol for the erasure is to be maintained for purposes of

65. Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses, Artikel 10-Gesetz [G-10] [G-10 Statute], Bundesgesetzblatt I. [BGBl. I.] 1254, 2298 (2001) (most recently amended by Law of November 17, 2015, BGBl. I., 1938), § 5a.

66. Ibid.

"the oversight of data protection."[67] Finally, strategic surveillance may not use "search terms" (*Suchbegriffe*) that contain "identifying features" that (1) will lead to a "targeted acquisition of determined telecommunication connections," or (2) that "concern the core area of private life."[68]

The G-10 Statute also contains mechanisms for oversight of the intelligence agencies. It establishes the Parliamentary Control Panel as well as the G-10 Commission. Most important, the G-10 Commission has a central role in deciding on the permissibility of surveillance by intelligence agencies. It plays an analogous role to the Foreign Intelligence Surveillance Act (FISA) court of the United States. To begin, however, with the Parliamentary Control Panel, it consists of members of the Bundestag, the German Parliament. The government (*Bundesregierung*) is required by law to "inform the Parliamentary Control Panel extensively" about "general activities" of the intelligence agencies and about "events of particular importance."[69] The Parliamentary Control Panel may also request files and other papers of intelligence agencies. It publishes an annual report about its oversight activities, which includes highly useful statistics about the use by intelligence agencies of surveillance powers. A 2009 law heightened the Parliamentary Control Panel's constitutional status and its powers to gather information from the government and intelligence agencies.[70]

As for the G-10 Commission, the Parliamentary Control Panel names the members of this entity. The G-10 Commission decides on the "permissibility and necessity" of surveillance carried out by intelligence agencies pursuant to the G-10 Statute.[71] As the Parliamentary Control Panel explains, "the supervisory power of the Commission extends to the entire collection, processing and use of personal data by federal intelligence agencies pursuant to the G-10 Statute."[72]

b. The Role of Telecommunication Providers

Telecommunications Law §§ 110–113 provide a particularly important statutory example of systematic data access. These sections require that telecommunication providers collect certain data about their customers, such as name, address, and telephone number, before the service is established. This information is termed *Bestandsdaten*, or "inventory information," and is sent to an automated databank of the *Bundesnetzagentur*, or Federal Network Agency.

67. Ibid.

68. Ibid. at § 5(2).

69. Kontrollgremiumgesetz vom 29. Juli 2009 (BGbl. I S. 2346), § 4(1).

70. Bertold Huber, "Die Reform der parlamentarischen Kontrolle der Nachrichtendienste und des Gesetzes nach Art. 10 GG," 28 *NVwZ* 1321 (2009).

71. G-10 Statute, § 15(5).

72. Unterrichtung durch das Parlamentarische Kontrollgremium, Drucksache 17/4278, p. 3.

Pursuant to Telecommunications Law § 112, governmental agencies can make automated requests for this information from the databank. The legal standard for justifying such access to "inventory information" is quite low. Law enforcement and intelligence officials can request the information when it is required for discharge of their "legal functions."[73]

3. Domestic Law Enforcement Agencies

The Code of Criminal Procedure § 100g(2) contains important legal provisions for systematic data access. It allows law enforcement agencies to gain information about "a sufficiently specific spatial and temporal description of telecommunications" in cases of a serious criminal offense, and when the investigation of the matter would otherwise be made significantly more difficult. Under this authority, the police in Berlin, Dresden, and many other locations have made massive requests for cell tower data about any person located in a given area during a specific time period. One attorney has called this action "the equivalent of data mining through the cell phone."[74] There are no national statistics regarding this activity, but only occasional requests for information made within state parliaments. Thus, a Berlin newspaper, the *taz*, reported in 2012 that the Berlin police since 2008 had made 410 "Funkzellenabfragen," or "radio-cell inquiries" and, thereby, collected information pertaining to 4.2 *million* cell phone connections.[75] These requests had been made to combat an epidemic of vandals setting automobiles on fire. In 2011, the same newspaper revealed that the police had gathered similar kinds of information after an anti-Nazi protest in Dresden.[76] Another report states that 11,474 radio cell inquiries had been made in the state of North Rhein-Westphalia from December 2010 to March 2014.[77] In Berlin there were 1,408 inquiries between 2009 and 2012.[78] In 2013 alone, at least 50 million sets of data were acquired in Berlin, of which 36 million sets originated from a single

73. Already in 2003, I had observed about the previous statutory provision creating this process for access to inventory information: "In Germany, it is quite easy to obtain 'inventory information.' Law enforcement officials can request it when required for discharge of 'their legal functions,' and judicial review of this request does not occur." Paul M. Schwartz, "German and US Telecommunications Privacy Law," 54 *Hastings L.J.* 751, 781 (2003).

74. Paul Wrusch, "Mal eben ausgespäht," *taz* (June 19, 2011), http://taz.de/Demo-berwachung-per-Mobilfunk/!72708/.

75. Konrad Litschko, "Polizei sammelte Handydaten," *taz* (January 23, 2012), http://www.taz.de/Autobrandstiftung-in-Berlin/!86239/.

76. Paul Wrusch, "Mal eben ausgespäht," *taz* (June 19, 2011), http://taz.de/Demo-berwachung-per-Mobilfunk/!72708/.

77. Constanze Kurz, "Erneut steigende Zahl von Funkzellenabfragen," *netzpolitik.org* (July 8, 2015), https://netzpolitik.org/2015/erneut-steigende-zahl-von-funkzellenabfragen/.

78. "Funkzellenabfrage in Berlin: Vielleicht werden Sie gerade überwacht," *netzpolitik.org* (September 14, 2015), at https://netzpolitik.org/2015/funkzellenabfrage-in-berlin-vielleicht-werden-sie-gerade-ueberwacht/.

proceeding.[79] A report from the state of Schleswig-Holstein in 2016 found that the number of "radio-cell inquiries" had gone up more than five times since 2009.[80]

C. Rejection of the ELENA Project

A controversy concerning systematic data access involved the government's termination of the ELENA project, which was a planned database of employee data. ELENA stands for the "*Elektronische Entgeltnachweis-Verfahren*," or "Electronic Payment Verification Process," and had its basis in a statute enacted in March 2009.[81] It was intended to afford German companies significant savings in their human resource departments by streamlining the collection of a wide variety of employee data. A government agency was to maintain the resulting centralized database of information, which consisted of name, data of birth, insurance number, home address, time missing work, and "possible misbehavior." The information was to be shared for purposes of unemployment insurance, housing benefits, parental benefits, and other kinds of social insurance. According to the *Spiegel* magazine, ELENA, was to be "the largest official collection of data in Germany."[82]

In July 2011, the German government abandoned the ELENA project. The project failed because of the lack of an adequate electronic signature for use within the ELENA process and a series of contested data protection issues. In addition, local political authorities and small and medium-sized businesses, an economic sector termed the "*Mittelstand*," had complained about their costs under the project.

D. Voluntary Access to Data

As noted above, German data protection law permits a private or public sector entity to collect, process, and transfer personal information only subject to a limited set of conditions. As a fundamental matter, there must be a statutory basis for such informational activity. There are also strong and numerous protections in place in the relevant constitutional law. As a result, informal or cooperative agreements are permissible under German law only if they comport with constitutional and statutory requirements.

79. Ibid.

80. Markus Reuter, "Zwei Funkzellenabfragen am Tag alleine im Schleswig-Holstein," *netzpolitik.org* (April 13, 2016), at https://netzpolitik.org/2016/zwei-funkzellenabfragen-am-tag-alleine-in-schleswig-holstein/.

81. "Das Ende von ELENA: Arbeitnehmer-Datenbank wird 'schnellstmöglich' eingestellt," *MMR-Aktuell* 321105 (2011).

82. "Abschied von "Elena": Regierung stoppt umstrittene Arbeitnehmer-Datenbank," *Spiegel* (July 18, 2011), http://www.spiegel.de/netzwelt/netzpolitik/0,1518,775145,00.html.

E. Role of the Courts

As the discussion above of constitutional law has already indicated, German courts have a central role interpreting the relevant legal norms when personal information is processed, collected, and transferred. Indeed, this area of German law functions as a textbook illustration of Alec Stone Sweet's idea of "constitutional politics" in Europe. Drawing on "the "privileged status" of fundamental rights in the Basic Law, the Federal Constitutional Court in the area of information privacy can be seen as constructing "a discourse, a set of dialogues and collective conversations, about the capacities and limits of the use of state power."[83] The resulting rules then draw a variety of state officials into discourse around constitutional concepts as developed by the Court in a reconfigured policymaking environment.

There have been general complaints, to be sure, about an "overconstitutionalizing" of constitutional law as well as objections to a "Karlsruhe Republic," that is, a Germany run from the Constitutional Court's headquarters in Karlsruhe, Germany.[84] Nonetheless, among both elites and the general public, there is a high level of acceptance of the role of the Constitutional Court—and one that it has exercised in numerous cases by limiting systemic data access.

F. Data Retention

Following the Constitutional Court's decision in 2010 voiding the data retention statute and the ECJ's decision invalidating of the Data Retention Directive in 2014, Germany enacted a new law, which came into force in 2015 and requires full compliance by 2017 at the latest.[85]

One rejected policy proposal was to replace mass data retention with a "Quick Freeze" process.[86] Under it, law enforcement and intelligence agencies would obtain an order for targeted data preservation relating only to a person under suspicion. If a crime was, in fact, committed, there would then be a "thawing" of the data, that is, access provided to it, to aid in the prosecution of the party. The current data retention requirement does not, however, take this approach. It requires storage of location data (*Standortdaten*) for mobile telephones for 4 weeks, storage of location data for mobile Internet use for 4 weeks, and the storage of call

83. Alec Stone Sweet, *Governing with Judges: Constitutional Politics in Europe* (Oxford: Oxford University Press, 2000), 22.

84. For a discussion of the over-constitutionalizing of German politics and law, see Michael Zürn, "Ist die Karlsruher Republik demokratisch?," in *Herzkammern der Republik* 258 (Michael Stolleis, ed., 2011).

85. Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten 10.12.2015 BGBl. I S. 2218.

86. Quick Freeze/Datensicherung, Bundesministerium der Justiz, http://www.bmj.de/DE/Buerger/digitaleWelt/QuickFreeze/quickfreeze_node.html.

numbers and the time and duration of all calls for 10 weeks. The Data Retention statute also requires storage of "assigned IP addresses" of Internet users and the time and duration of Internet use for 10 weeks. This information can be released without a judicial order for purposes of criminal prosecution and prevention of significant concrete danger. Finally, this statute mandates telecommunication providers to store mandated data in Germany. The European Commission has criticized these data residency requirements as violating European Union principles concerning freedom of services.[87]

As another example of the ongoing controversy around the topic of data retention, the Max Planck Institute for Foreign and International Criminal Law published an expert opinion in January 2012 finding the absence of a negative impact on the solving of crimes due to the lack of stored data since 2010.[88] The Justice Ministry had authorized this report and welcomed it as proof that data storage was unnecessary.[89] In contrast, the Interior Ministry and the BKA criticized the methodology of the report.[90]

G. Cross-Border and Multi-Jurisdictional Issues

In its *G-10* opinion, the Constitutional Court found that the protections of the Basic Law's Article 10 were not limited exclusively to communications that took place only within the national borders of Germany. As long as enough of a nexus existed between the surveillance and German territory, the protections of Article 10 were applicable.[91]

There is an open question, however, regarding the regulation of surveillance of satellite communications. According to the BND, its capture of information from satellite connections is limited neither by statutory nor constitutional law. This idea is termed the "space theory" (*Weltraumtheorie*). Distinguished legal experts have disagreed with it, but the matter remains unresolved.[92]

87. For a discussion, see Lothar Determann and Michaela Weigl, "Data Residency Requirements Creeping into German Law," 15 *PVLR* 529 (March 14, 2016).

88. Max-Planck-Institut für ausländisches und internationales Strafrecht, *Schutzlücken durch Wegfall der Vorratsdatenspeicherung*, p. 219 (2d ed. 2011), https://www.mpg.de/5000721/vorratsdatenspeicherung.pdf.

89. "Studie bestreitet Sinn von Vorratsdatenspeicherung," *Focus* (January 27, 2012), http://www.focus.de/politik/deutschland/aufklaerungsquote-nicht-beeinflusst-studie-bestreitet-sinn-von-vorratsdatenspeicherung_aid_707398.html.

90. "Vorratsdatenspeicherung: Friedrich stellt Studie infrage," *Focus* (January. 27, 2012), http://www.focus.de/politik/deutschland/vorratsdatenspeicherung-friedrich-stellt-studie-infrage_aid_707678.html.

91. 100 BVerfGE 313, 363–64 (1999) (*G-10*).

92. See Baldus, *Beck'scher Online-Kommentar Grundgesetz*, Territorialer Schutzgehalt, Article 10, ¶¶ 20–21 (Epping, Hillgrubered ed. 29, 2015) (constitutional protection does not differentiate between where the German government acts or where the effects of the action

IV. RECENT CONTROVERSIES

Two controversies of current relevance have already been discussed, namely the abandonment of the ELENA database of employment data and the ongoing debate about data retention. Further controversies concern the proposal for Germany-based cloud services and the collaboration between the National Security Agency and the *Bundesnachrichtendienst*.

There has been considerable discussion in Germany about privacy and security issues relating to data processing in the cloud. In the judgment of the Federal Data Protection Commissioner, for example, cloud computing represents a form of "contract data processing" (*Auftragsdatenverarbeitung*).[93] Such activity requires that the party carrying out the processing in the cloud "comply with technical and organisational measures to ensure privacy."[94]

The policy debate in Germany about the cloud has also considered the potential for US government access to German data stored in this fashion. The introduction of Microsoft's Office 365 in Germany marked an early moment in which such concerns were raised. In response to a question, a Microsoft executive discussed the obligation of his company to share data from European data centers with US officials if requested pursuant to appropriate legal authorities.[95] According to an analysis in a German law review, however, such a transfer, even if pursuant to statutory authorities in the United States, would violate the Federal Data Protection Law of Germany.[96] In that article, Benno Barnitzke observes that "a transfer to US authorities is not covered by an authorization in the German federal data protection statute (BDSG)." As a consequence, "the release represents an improper and illegal data processing in the sense of the BDSG." Moreover, BDSG § 43 would provide sanctions against it.[97]

Another window into German attitudes about cloud services and storage is offered by a White Paper from the Conference of Federal and State Data

occur, provided that the act represents the power of the German government); Hans-Jürgen Papier, Opinion on 1. Committee on Inquiry of the Parliament of the Federal Republic of Germany 18. Legislative Period, p. 7 (May 24, 2014), https://www.bundestag.de/blob/280842/9f755b0c53866c7a95c38428e262ae98/mat_a_sv-2-2-pdf-data.pdf ("an act of intervention has to be attributed to German authorities whenever it is conducted from German soil or with the approval and tolerance of German authorities"). For media coverage of the issue, see Thorsten Denkler, "NSA Untersuchungsausschuss: Juristen werfen BND Verfassungsbruch vor," *Süddeutschen Zeitung* (February 5, 2015) at http://www.sueddeutsche.de/politik/nsa-untersuchungsausschuss-juristen-werfen-bnd-verfassungsbruch-vor-1.1972477.

93. Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, Tätigkeitsbericht 2009 und 2010, Drucksache 17/5200, pp. 63–64.

94. Ibid.

95. Benno Barnitzke, "Microsoft: Zugriff auf personenbezogene Daten in EU-Cloud auf Grund US Patriot Act möglich," *MMR-Aktuell* 3211103 (2011).

96. Ibid.

97. Ibid.

Protection Commissioners of Germany. The White Paper raises concerns regarding the lack of transparency for individuals regarding data processing in the cloud. [98] In reference to non-EU nations, or so-called "Third Countries," the White Paper also warns that "when a public cloud is used in Third Countries, access to the data of the company using the cloud is possible and cannot be controlled."[99] Finally, a law review article in Germany has warned, "The solution to this problem should certainly not be that European clouds are moved to the United States . . . [and] lawfully subject to the access of US authorities."[100]

One specialized German concern about cloud services run by US companies relates to the storage of governmental information in them. Already in 2012, the Minister of the Interior, Hans-Peter Friedrich, called for development of "a Federal cloud" as part of a plan to consolidate the IT infrastructure of the German government. The "*Bundes-Cloud*" is intended to keep "sensitive governmental and enterprise data from landing with US officials."[101] In 2015, the Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnik)* published a resolution with criteria for the procurement and use of cloud services by the federal German administration.[102] Among the Resolution's key requirements is that information such as business secrets and sensitive data about the federal IT infrastructure were to be processed exclusively in Germany. Cloud providers were to implement appropriate technical and organizational measures to keep data subject to secrecy provision from disclosure to unauthorized third parties.

Beyond the public sector's effort to build the *Bundes-Cloud*, the private sector has also responded to these German concerns. One major step has involved data localization. Tech companies are now building cloud centers throughout Germany and developing technical solutions to keep information localized within that country. Microsoft has developed an innovative "data trustee" approach for the German market.[103] First, it opened data centers in Frankfurt-am-Main and Magdeburg and offered business clients the option of storing data exclusively in these German centers. Second, it partnered with Deutsche Telekom's independent subsidiary T-Systems, which will act as data trustee for

98. Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, *Orientungshilfe—Cloud Computing* 16 (Sept. 26, 2011).

99. Ibid.

100. Christian Schröder and Nils Christian Haag, "Neue Anforderungen an Cloud Computing für die Praxis," 1 *ZD* 147, 150 (2011).

101. Jürgen Berke, "Innenminister Friedrich will Bundes-Cloud aufbauen," *Wirtschaftswoche* (January 20, 2012).

102. IT Board Resolution, No 2015/5 (2015) (Beschluss des Rates der IT-Beauftragten der Ressorts, July 29, 2015).

103. Michael Rath et al., "Die neue Microsoft Cloud in Deutschland mit Datentreuhand als Schutzschild gegen NSA & Co.?," *Computerrecht* 98, p. 100 (2016).

information in these centers. Although Microsoft operates the data centers, T-System controls access to all stored information. Through a web of contracts and trusts, Microsoft limits its access to data on the German servers and assigns T-Systems exclusive legal authority to release information stored on them.[104] This service is available only to business customers of Microsoft and not private ones.

The trustee model is intended to bolster Microsoft's legal arguments against disclosure when faced with data demands from US courts, whether in criminal, intelligence, or civil settings. The idea is that Microsoft cannot share the German cloud data of its customers because to do so would violate the applicable law of German trusts and contracts.[105] This legal theory is untested before US courts; use of Deutsche Telekom as a data trustee may or may not shelter information from US legal processes. At any rate, Microsoft has demonstrated its willingness to litigate these kinds of issues in the United States. In 2016, for example, it won a victory in the Second Circuit against a US government request for information stored in an Irish data center. The Second Circuit ruled that the Stored Communications Act lacked extraterritorial reach.[106]

Other companies are exploring the use of encryption in their EU data centers. In this model, customers are given keys to their information and have the sole ability to decrypt stored data.[107] This approach is analogous to the San Bernadino iPhone case where Apple argued that it lacked the ability, at least not without considerable additional effort, to unlock information stored on the phone seized by US authorities.[108]

As for the collaboration between the NSA and BND, a single location perhaps best symbolizes this work: Bad Aibling, a small town in Bavaria, in the south of Germany. Bad Aibling is best known today in Germany not as a luxury health resort, but for its satellite tracking station. Until the early years of the twenty-first century, the NSA ran this listening post. After its official departure date, the NSA continued to have a physical presence at the station and worked in close collaboration with the BND by supplying it with so-called "selectors" ("Selektoren").

104. Ibid. at p. 101. For an analysis of this legal model, see Paul M. Schwartz & Karl-Nikolaus Peifer, "Datentreuhändermodelle—Sicherheit vor Herausgabeverlangen US-amerikanischer Behörden und Gerichte?," *Computer und Recht* 165 (3/2017).

105. Ibid. at p. 103.

106. *Microsoft Corporation v. United States*, 2016 US App. LEXIS 12926 (2d Cir. 2016). Extraterritorial requests for information are possible, of course, under other legal authorities other than the SCA. Paul M. Schwartz, "Microsoft, Ireland and a Level Playing Field for US Cloud Companies," 15 *PVLR* 1549 (August 1, 2016).

107. Peter Maushagen, "Erfolg mit der Wolke: Deutsche Cloud-Dienste werden bei US-Konzernen immer beliebter," *Businessinsider.de* (March 17, 2015), at http://www.businessinsider.de/cebit-us-konzerne-schuetzen-daten-in-deutschen-cloud-diensten-4785413?IR=T.

108. Matter of Search of an Apple iPhone Seized during Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203, No. ED 15-0451M, 2016 WL 618401 (C.D. Cal. Feb. 16, 2016).

As the *Zeit* magazine explains, these are "something like search terms."[109] The NSA sent the BND IP addresses, telephone numbers, email addresses, MAC-Addresses, URLs, and geo-coordinates.

Over the years, the NSA provided the BND with some 14 million "selectors." The process took place automatically with a BND server downloading the terms several times a day from an NSA server. The BND turned over the results of these searches to the NSA for storage in its own databanks. In carrying out data searches for the NSA, the BND in many cases engaged in activities forbidden by German law. For example, although it was supposed to filter out forbidden searches according to a so-called G-10 Filter, this process did not function completely or accurately. In 2015, a Big Brother Award went to the BND and its then president Gerhard Schindler for its involvement in "a whole range of scandals and violations of privacy and civil rights."[110]

A special committee of the Bundestag is investigating NSA-BND activities. In October 2015, the expert's report to the committee found that the activities at Bad Aibling violated bilateral agreements between Germany and the United States as well as German law.[111] According to the *Zeit* magazine, moreover, there are secret agreements in place among the NSA, BND, and the Federal Office for the Protection of the Constitution, under which the NSA provides technologies and goals for data gathering and analysis, and the German intelligence agencies collect the information.[112] One fear, as expressed by the then Federal Data Protection commissioner, Peter Schaar, is that the intelligence agencies will engage in "competence hopping" (*Befugnis-Hopping*).[113] Schaar was concerned

109. See Kai Biermann and Patrick Beuth, "Was sind eigentlich Selektoren?," *Zeit* (April 24, 2015), http://www.zeit.de/digital/datenschutz/2015-04/bundesnachrichtendienst-bnd-nsa-selektoren-eikonal.

110. Big Brother Awards 2015 (bigbrotherawards.de 2015), at https://bigbrotherawards.de/en/2015/authorities-administration-federal-intelligence-agency-bundesnachrichtendienst-bnd.

111. The German government had refused to share the "selectors" with the German parliament; the compromise reached was to share them with an expert, Kurt Graulich, a former federal judge. The resulting report by Graulich also found evidence of economic espionage against European as well as German companies. The expert report was, in turn, widely criticized as placing too much blame on the NSA, the Americans, and too little on the BND, the Germans. See, for example, Kai Bermann, "Ein Versuch, den BND freizusprechen," *Die Zeit* (October 30, 2015), at http://www.zeit.de/digital/datenschutz/2015-10/selektoren-nsa-bericht-graulich-bnd/komplettansicht; BND/NSA-Affäre, *Heiseonline* (October 30, 2015), at http://www.heise.de/newsticker/meldung/BND-NSA-Affaere-Sonderermittler-deckt-erhebliche-Maengel-und-Rechtsbruch-auf-2866243.html.

112. See Kai Biermann and Patrick Beuth, "Was sind eigentlich Selektoren?," *zeit.de* (April 24, 2015), http://www.zeit.de/digital/datenschutz/2015-04/bundesnachrichtendienst-bnd-nsa-selektoren-eikonal.

113. Unterrichtung durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, Deutscher Bundestag, 18. Wahlperiode, Drucksache 18/59 (15.11.2013).

that the German and other foreign intelligence services, such as the NSA, will engage in a division of labor to strategically evade legal and constitutional restrictions on their work.

In addition to the investigation by the special Bundestag Commissioner, the Federal Data Protection Commissioner carried out its own investigation of the BND. This effort was started by Peter Schaar and continued by the current Commissioner, Andrea Voβhoff. *Netzpolitik*, a German blog, has now leaked the Commissioner's full report. The Data Protection Commissioner identified 18 violations of law by the BND and filed 12 complaints.[114] According to *Netzpolitik*, this number represented the largest amount of complaints ever directed at a single time against a German authority by the Federal Data Protection Commissioner. Perhaps most critically, the Commissioner found, "Contrary to its explicit legal obligation, the BND had created databases without an establishing order and used them (for many years), thus disregarding fundamental principles of legality." The report also found that the BND had "collected personal data without a legal basis and has processed it systematically." Finally, the Commissioner objected to the BND's illegal and massive restrictions of her supervisory authority. As *Netzpolitik*'s noted, the Bad Aibling station was only one of five BND listening stations in Germany. The Commissioner demanded that the BND take into account her power under federal data protection law to carry out on-site investigations not only in Bad Aibling but at other BND sites.

The United States historically has shared a special intelligence relationship with the so-called Five Eyes: the United States, United Kingdom, Canada, Australia, and New Zealand. As the Snowden revelations and subsequent investigations have shown, beyond the Five Eyes, Germany and the United States have negotiated the terms for their own intelligence cooperation. The final report of the special investigatory committee, the report of the Federal Data Protection Commissioners, as well as attempts by the Bundestag to introduce new legislation to reform the BND are unlikely to change the basic elements of this US-German arrangement, or to make all aspects of the relationship transparent to the public.

The relationship between these intelligence agencies also has importance for efforts to create German clouds. One reason for such data localization is to put the data beyond the reach of US intelligence agencies. In the assessment of

114. The report is entitled: Betreff: Datenschutzrechtliche Beratung und Kontrolle gemäβ §24 und §26 Absatz 3 Bundesdatenschutzgesetz der Erhebung und Verwendung personenbezogener Daten in bzw. in Zusammenhang mit der Dienststelle des BND in Bad Aibling (May 15, 2016). For the *Netzpolitik* report on it, see Andre Meister, "Geheimer Prüfbericht: Der BND bricht dutzenfach Gesetz und Verfassung—allein in Bad Aibling," *Netzpolitik.org* (September 1, 2016), at https://netzpolitik.org/2016/geheimer-pruefbericht-der-bnd-bricht-dutzendfach-gesetz-und-verfassung-allein-in-bad-aibling/. For an English translation of the *Netzpolitik* reporting, see Andre Meister, "Secret Report: German Federal Intelligence Service BND Violates Laws and Constitution by the Dozen," *Netzpolitiki.org* (September 2, 2016), at https://netzpolitik.org/2016/secret-report-german-federal-intelligence-service-bnd-violates-laws-by-the-dozen/.

Lothar Determann and Karl Guttenberg, the close cooperation between intelligence agencies in the United States and other European countries means that "data stored and transmitted exclusively on European territory is not safer from US cyberspying than it would be in the United States."[115] Determann and Guttenberg also note that the law of the European Union "does not impose any meaningful limitations on government surveillance because the EU has limited jurisdiction over the foreign intelligence activities of its member states."[116]

V. CONCLUDING OBSERVATIONS

German law has devoted significant attention to the regulation of systemic government access to private-sector data. German lawmakers have enacted numerous statutes and amended these laws frequently. The Federal Constitutional Court has accompanied every step of this process and developed highly detailed constitutional standards to make such access comport with the Basic Law. It has sought to protect informational self-determination and to preserve the roles of law enforcement and intelligence agencies in enforcing the criminal laws and protecting the public from terrorism.

German officials and experts have been skeptical of the standards of US information privacy law and, as a result, deeply concerned about systematic data access on the other side of the Atlantic. At the same time, German intelligence agencies have assisted in some of the efforts of US intelligence services, both before and after 9/11.

After revelations that the NSA had eavesdropped on her cell phone, Angela Merkel, the Federal Chancellor, complained in 2013 about Americans: "Spying among friends—that just is not done." ("*Ausspähen unter Freunden—das geht gar nicht*"). By 2015, however, Chancellor Merkel was praising the cooperation between German and American intelligence services in defending against terrorism. Chancellor Merkel called for identification of mistakes and deficiencies in this collaborative work. At the same time, her bottom line was clear: "[W]e need the cooperation with the American services."[117] German law will continue to develop constitutional and legal standards for systemic data access. An important part of this task will be to establish appropriate procedures and legal norms for the collaboration by German intelligence agencies with allied services, including their American counterparts.

115. Lothar Determann and Karl T. Guttenberg, "On War and Peace in Cyberspace: Security, Privacy, Jurisdiction," 41 *Hastings Const. L.Q.* 878, 886 (2014). Karl Guttenberg is the former Minister of Defense of Germany.

116. Ibid. at 885.

117. "Wir brauchen die amerikanischen Geheimdienste," *Frankfurt Allgemeine Zeitung* (August 31, 2015), at http://www.faz.net/aktuell/politik/merkel-wir-brauchen-die-amerikanischen-geheimdienste-13778270.html.

4

Systematic Government Access to Private-Sector Data in Israel

Balancing Security Needs with Democratic Accountability

OMER TENE

I. ABSTRACT

Israel is a democracy committed to the protection of human rights while at the same time trying to contain uniquely difficult national security concerns. One area where this tension is manifest is government access to communications data. On the one hand, subscriber privacy is a constitutional right protected by legislation and Supreme Court jurisprudence; on the other hand, communications data are a powerful tool in the hands of national security and law enforcement agencies. In this chapter I examine Israel's attempt to balance these competing interests by empowering national security agencies while at the same time creating mechanisms of accountability. In particular, Israel utilizes the special independent status of the attorney general as a check on government power.

II. NATIONAL LEGAL CONTEXT AND FUNDAMENTAL PRINCIPLES

Israel is a parliamentary democracy with a system of checks and balances between the legislative branch (the "Knesset," or Parliament); the executive branch (the "Memshala," or government); and a strong judiciary. Its constitution is compiled of a series of "Basic Laws" setting forth the structure of and relations among the institutions of power as well as the fundamental human rights. Under a 1995 Supreme Court decision, these Basic Laws enjoy constitutional status, enabling the judiciary to strike down inconsistent legislation.[1] Also sharing constitutional

1. C.A. 6821/93 *Bank Ha'Mizrachi Ha'Meuchad Ltd. et al. v. Migdal Kfar Shitufi*, 49(4) P.D. 221 (1995).

status are a number of fundamental human rights not enumerated in the Basic Laws, including equality, freedom of speech, and freedom of religion.[2]

When analyzing human rights in Israel, two important preliminary observations must be made: first, a distinction must be drawn between "Israel proper" and the territories that it occupies since 1967. Although Israel proper is a democracy strongly committed to human rights, the occupied territories are in a state of belligerent occupation and subject to a military regime. In this chapter, I analyze the legal situation strictly in Israel proper, an analysis that has no bearing on the situation in the occupied territories. It is important to note that although described as a Jewish state in its Declaration of Independence, Israel includes large religious and ethnic minorities, namely Muslims (approximately 20 percent of the population and 80 percent of non-Jews), Christians, and Druze, some of which claim de facto discrimination.[3]

Second, since its inception in 1948, Israel has been in a state of war with some or all of its neighbors, and has undergone waves of fierce terrorism targeting civilian population. This means that more than most Western democracies, Israel had to balance its pursuit of human rights with a need to defend national security, fight terrorism, and occasionally engage in full-scale war. Accordingly, national security considerations have had a profound impact on Israeli constitutional and legal discourse; at the same time, they have neither upended the rule of law nor completely displaced fundamental rights. On more than one occasion, the Israeli Supreme Court reaffirmed its commitment to the rule of law even in cases pitting strong national security interests: for example, outlawing torture in interrogations,[4] or displacing the military erected security barrier.[5] In one landmark case, Supreme Court Chief Justice Aharon Barak wrote: "there is no security without law, and the rule of law is a component of national security."[6]

2. See for example HCJ 721/94 *El-Al Israel Airlines v. Danielowitz*, 48 P.D. 749 (1994) (equality); HCJ. 73/53 and 87/53 *Kol Ha'am v. Minister of The Interior*, 7 P.D. 871 (1953) (freedom of speech); HCJ 5016/96 *Horev v. Minister of Transportation*, 51(4) P.D. 1 (1997) (freedom of religion).

3. For resources see, for example, Association for Civil Rights in Israel, *Arab Minority Rights*, http://www.acri.org.il/en/category/arab-citizens-of-israel/arab-minority-rights/.

4. HCJ 5100/94 *Public Committee Against Torture v. The State of Israel.*

5. HCL 7957/04 *Zaharan Yunis Muhammad Mara'abe et al. v. Prime Minister of Israel et al.* (Supreme Court, Sept. 15, 2005), https://ihl-databases.icrc.org/applic/ihl/ihl-nat.nsf/caseLaw.xsp?documentId=FF996DAFB177F6ECC12575BC004899A5&action=openDocument.

6. HCJ 428/86 *Barzilai v. Government of Israel*, 40(3) P.D. 505 (1986), available in English at http://elyon1.court.gov.il/files_eng/86/280/004/z01/86004280.z01.pdf (petitioner attacked a decision by the president of Israel to pardon before trial officers of the General Security Service, who allegedly executed two terrorists who hijacked a bus and took hostages).

III. CONSTITUTIONAL AND STATUTORY OVERVIEW

A. The Constitutional Right to Privacy

Section 7 of Basic Law: Human Dignity and Freedom (1992) (Basic Law) states:

(a) All persons have the right to privacy and to intimacy.
(b) There shall be no entry into the private premises of a person who has not consented thereto.
(c) No search shall be conducted on the private premises or body of a person, nor in the body or belongings of a person.
(d) There shall be no violation of the confidentiality of the spoken utterances, writings or records of a person.[7]

In several key decisions, the Israeli Supreme Court stressed that the right of privacy is a basic constitutional right.[8]

Like all fundamental rights, the right to privacy is not absolute. It is subject to the so-called "limitation clause" in Section 8 of the Basic Law, which states: "There shall be no violation of rights under this Basic Law except by a law befitting the values of the State of Israel; enacted for a proper purpose; and to an extent no greater than is required." Any legislative or executive action is subject to this constitutional instruction; if it restricts the right to privacy, it will survive only if it passes scrutiny under the limitation clause.

For example, in *Association for Civil Rights in Israel v. Minister of Interior* (2004), the Israeli Supreme Court struck down as unconstitutional public sector data-sharing practices although such data sharing had been authorized by statute.[9] The Supreme Court ruled that data transfers were overly broad and had disproportionate effect on individuals' privacy rights. It ruled that data transfers must be restricted by regulations specifying the precise recipients of data, data uses, and data security measures. It provided that transfers of data from government to private-sector financial institutions must be expressly authorized by primary legislation; anti-money laundering provisions in secondary regulations did not suffice.

In *Plonit v. National Rabbinical Court* (2006), the Israeli Supreme Court held that "the right to privacy is one of our most important fundamental rights. It is

7. The Basic Law: Human Dignity and Freedom (5752-1992), passed by the Knesset on the 21st Adar, 5754, March 9, 1994, http://www.mfa.gov.il/mfa/go.asp?MFAH00hi0.

8. Civ. App. 1697/11 *A. Guttsman Architects v. Vardi* (Sup. Ct. January 23, , HCJ 6650/04 *Plonit v. National Rabbinical Court* (Sup. Ct., May 14, 2006); HCJ 8070/98 *Association of Human Rights v. Ministry of Interior*, 58(4) S.CT. 842 (2004); see also Omer Tene, "Israeli Data Protection Law: Constitutional, Statutory and Regulatory Reform," 8(1) *Privacy and Data Protection* 6 (2007); Alon Kaplan & Paul Ogden eds., "Israeli Business Law: An Essential Guide" (1997), at 30.01.

9. HCJ 8070/98 *ACRI v. Ministry of Interior*, 58(4) S.CT. 842 (2004).

one of the freedoms shaping the democratic character of Israel's legal system. Its roots run deep in our Jewish heritage. It is mandated by Israel's values as a Jewish and democratic state."[10] These holdings were reiterated in *Rami Mor v. Barak ETC* (2010), a case in which the Supreme Court refused to order an ISP to unmask a John Doe defendant, holding that the constitutional right to privacy entails a right to anonymity.[11] Justice Eliezer Rivlin stated:

> The shattering of the "illusion of anonymity" in a reality where a user's sense of privacy is a myth may raise associations of a "big brother." Such an infringement of privacy must be minimised. Anonymity shelters must be preserved within reasonable boundaries as they constitute an important aspect of Internet culture. To a great extent, anonymity makes the Internet what it is, and without it freedom in the virtual space would be mitigated. The prospect of tracking those in the virtual space would have a stifling effect on their behavior.

In *Issakov Inbar v. State of Israel* (2011), the Israeli National Labor Court severely restricted employers' ability to monitor their employees' email correspondence, holding that given the constitutional status of the right to privacy, exemptions to the Privacy Protection Act, 1981 (PPA), must be interpreted narrowly.[12] In its opinion, the Court made clear statements concerning the suspect nature of employee consent and mandated implementation of principles of legitimacy, transparency, proportionality, purpose limitation, access, accuracy, confidentiality, and security. This decision has recently been reaffirmed by the Supreme Court.[13]

B. The Statutory Right to Privacy

Israel has not only constitutional protections for the right of privacy but also an omnibus privacy protection statute, the PPA. The PPA applies to both the private and public sector and confers civil, administrative, and criminal rights and obligations. Section 1 of the PPA prohibits infringement of an individual's privacy without that individual's consent. Chapter A of the PPA deals with general privacy protection, listing 11 alternative causes of action for infringement of privacy.[14] Especially pertinent in the context of communications data are Section 2(1) of the PPA, which refers to "*spying on or trailing a person in a manner likely to harass him* (. . .);" Section 2(2): "*listening-in prohibited under any law;*" Section 2(5): "*copying or using, without permission from the addressee or writer, the contents of a letter or any other writing not intended for publication* (. . .);" and

10. HCJ 6650/04 *Plonit v. National Rabbinical Court* (Sup. Ct., May 14, 2006).

11. RCA 4447/07 *Rami Mor v. Barak ETC* (Sup. Ct., March 25, 2010).

12. Lab. App. 90/08 *Issakov Inbar v. State of Israel* (Nt'l Lab. Ct. February 8. 2011).

13. Civ. App. 3661/16 *Remet Ltd. v. Rami Shamir Civil Engineering Ltd.* (Sup. Ct. August 23. 2016).

14. Privacy Protection Act, § 2(1)–(11) (1981).

Section 2(9): "*using, or passing on to another, information on a person's private affairs otherwise than for the purpose for which it was given.*" An infringement of privacy constitutes a civil tort and, if intentional, a criminal offense.

Section 19 of the PPA provides an exemption from liability under Section 2 for "security services," defined to include the police, military intelligence (known according to its Hebrew acronym "Aman"), the Israeli Security Agency (ISA) (known according to its Hebrew acronym as "Shin Bet" or "Sahabak"),[15] and the Institute for Intelligence and Special Operations (known according to a shorthand version of its Hebrew name, "Mossad").[16] It states:

(a) No person shall bear responsibility under this Act for an act which he is empowered to do by law.
(b) A security authority or a person employed by it or acting on its behalf shall bear no responsibility under this Act for an infringement reasonably committed within the scope of their functions and for the purpose of carrying them out.

Nongovernment entities cooperating with a security service while compromising the privacy interests of their customers can rely for a defense on Section 19(a) above as well as on Section 18(2)(b) of the PPA, which states that "[i]n any criminal or civil proceeding for infringement of privacy, it shall be a good defence if (. . .) (2) the defendant or accused committed the infringement in good faith and in any of the following circumstances: (b) the infringement was committed in circumstances in which the infringer was under a legal, moral, social or professional obligation to commit it."

Informational privacy is further regulated by Chapter B of the PPA, Israel's data protection statute. Recognized by the European Commission in 2011 as providing "adequate" protection under EU data protection law,[17] Chapter B of the PPA establishes a procedure for database registration[18] and sets forth informational privacy principles including transparency,[19] purpose

15. The ISA is responsible for internal security, domestic intelligence and counter-intelligence, and the fight against terrorism.

16. The Mossad is responsible for foreign intelligence and covert missions beyond Israel's borders.

17. Commission Decision of 31 January 2011 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by the State of Israel with regard to automated processing of personal data, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:027:0039:0042:EN:PDF. It is interesting to note in this context that Ireland attempted to undermine Israel's adequacy decision, arguing that Israeli security services are likely to access personal data shipped from the EU to Israel. See Laurence Peter, "Ireland Delays EU Deal with Israel on Data Transfers," BBC, September 3, 2010, http://www.bbc.co.uk/news/world-europe-11176926.

18. §§ 8–10 of the PPA.

19. § 11 of the PPA.

limitation,[20] security,[21] confidentiality,[22] access and rectification,[23] and restrictions on transborder data flows.[24]

Significantly, Section 32 of the PPA provides an exclusionary rule pursuant to which (subject to certain narrow exceptions) "material obtained by the commission of an infringement of privacy shall not be used as evidence in court without the consent of the injured party." This provision was used to quash evidence obtained from a suspect by use of force,[25] by a party illicitly copying the counterparty's computer hard disk,[26] and by a husband covertly photographing his wife having intercourse with another man.[27] A separate provision is used to disqualify evidence obtained through an illicit or improperly authorized wiretap.[28]

IV. GOVERNMENT ACCESS

A. Facilitating Government Surveillance

Similar to the Communications Assistance for Law Enforcement Act (CALEA) in the United States, Section 13 of the Israeli Telecommunications Act (Telephone and Broadcast), 1982 (Telecommunications Act) empowers government officials to provide instructions to telecommunications operators to modify and design their equipment, facilities, and services to ensure that they have built-in surveillance capabilities.

Under Section 13 of the Telecommunications Act, the prime minister, after consulting with the Minister of Communications and based on a request by the Minister of Defence, Minister of Domestic Security, the ISA, or the Mossad, can issue instructions to a telecommunications licensee with respect to "the installation of equipment, performance of a telecommunications service, or ensuring technological compatibility to telecommunications equipment (. . .) including the provision of access to equipment, as much as necessary to perform the roles of the security services or exercise their legal authority."[29] Section 13(a) of the Telecommunications Act defines a "security service" to include the Israel Defence

20. § 8(b) of the PPA.

21. § 17 of the PPA; as well as the Privacy Protection Regulations (Conditions for Data Storage and Security and Public Sector Data Sharing), 1986.

22. § 16 of the PPA.

23. §§ 13–15 of the PPA.

24. The Privacy Protection Regulations (Transfer of Data to Databases Outside of Israel), 2001.

25. Add. Hear. 9/83 *Oiknine v. Military Court of Appeals*, 42(3) P.D. 837 (1988).

26. BSE (TA) 1614/02 *Multilock v. Rav Bariach* (Tel Aviv Dist. Ct. February 7, 2002).

27. *Plonit* case, above note 10.

28. See analysis in Crim. App. 1302/92 *State of Israel v. Nachmias*, 49(3) P.D. 309 (1995).

29. Telecommunications Act (Telephone and Broadcast), 1982, § 13(b)(2).

Forces, ISA, Mossad, police, and prison service. A licensee is defined broadly through a complex set of definitions in Section 1 of the Telecommunications Act[30] to include any fixed line or cellular operator, and ISPs, as well as broadcast licensees (cable and satellite operators).

Under Section 13(d) of the Telecommunications Act, the prime minister's instructions under Section 13(b) must remain secret. Section 13(e) of the Telecommunications Act provides immunity from civil or criminal liability (for example, for infringement of privacy) to a licensee and its employees for complying with an obligation under the same section. The payment by the government to the licensee for services rendered in accordance with Section 13(b), always a contentious issue, is regulated by Section 13(c) of the Telecommunications Act, which provides:

> The payment for services rendered or actions taken according to subsection (b) . . . will be determined in an agreement between the relevant security service and the licensee based on reasonable expense reimbursement and taking into account the existing price for the services rendered; in the absence of an agreement, the payment will be determined by a person appointed by the Attorney General. . .

B. Wiretapping

Wiretapping, or lawful intercept, is regulated in Israel under the Wiretap Act, 1979 (Wiretap Act). The Wiretap Act generally prohibits wiretapping and sets rules for lawful intercept by law enforcement and national security agencies. It defines a "conversation" as including not only voice communication but also communications between computers. It defines a wiretap as listening in to a conversation using a device without the consent of *either* party to the conversation.

A series of court decisions and instructions by the attorney general weighed whether the capture or interception by the police of certain synchronous or asynchronous communications such as email messages, text messages, and voicemails constitute a "wiretap" or rather a "search," which is subject in Israel to less legal process. The general thrust of these cases is that the capture of voicemail,[31] text messages[32] or emails *on a suspect's device* constitutes a search, whereas the interception of messages *in transit*, for example on the servers of an ISP, constitutes a wiretap.[33] Nevertheless, the Supreme Court has not yet confronted these

30. The nuances of the definition of a licensee are beyond the scope of this chapter, given the complexity of the Israeli licensing system, which comprises of "general" and "special" licenses as well as "general permits" under Section 4A1 of the Telecommunications Act.

31. Crim. App. 10343/01 *Badir v. State of Israel* (Supreme Court April 30, 2003).

32. BSP 3544/07 *Adar v. Israel Police* (Tel Aviv District Court September 18, 2007).

33. Crim. 40206/05 *State of Israel v. Philosoph* (Tel Aviv Dist. Ct. February 5, 2007).

issues and the attorney general continues to view the capture of any asynchronous communications, even on an ISP's servers, as a search.

Lawful intercept by the police is allowed pursuant to a warrant issued by a President of a District Court.[34] A broader mandate is provided to security services, defined as military intelligence or the ISA. A security service may obtain a permit for a wiretap from the prime minister or the Minister of Defence (in this Act, the "Minister") without judicial oversight. Under Section 4 of the Wiretap Act, "the Minister may authorise a wiretap in writing if requested to do so in writing by the head of a security service and if he is convinced, after giving due weight to the infringement of privacy, that it is necessary for national security." Sections 4(b)–(c) of the Wiretap Act describe the specifics that must be found in a Minister's permit, including the identity of the individual *or* device whose communications will be intercepted, the location of the conversations, and the duration of the monitoring (not to exceed three months, subject to periodic extension). However, the requirement to specify such details is qualified by the phrase "all if they are known in advance." This implies that the Minister may well issue general wiretapping permits. In urgent cases, the head of a security service may himself authorize a wiretap for a period no longer than 48 hours; immediate notice must be sent to the Minister who is authorized to revoke such a wiretap.[35]

Although not subject to judicial oversight, national security wiretap permits are reported quarterly to the attorney general;[36] and the number of such permits is reported annually to a special parliamentary committee convening behind closed doors.[37] Additional issues regulated by the Wiretap Act include the manufacturing, import, and possession of wiretapping equipment;[38] data retention and deletion requirements;[39] the wiretapping of communications subject to evidentiary privileges;[40] and the admissibility of evidence obtained through an illegal or improperly authorized wiretap.[41] Generally, such evidence is inadmissible; yet certain exemptions apply, namely "in a criminal proceeding for a serious felony, if a court decided to admit the evidence after having been convinced . . . that the interest in reaching the truth outweighs the interest in privacy."[42] An additional

34. A president of a District Court in Israel is a senior judge who ranks junior to only Supreme Court justices.

35. The Wiretap Act, § 5.

36. The Wiretap Act, § 4(d).

37. The Wiretap Act, § 4(e).

38. The Wiretap Act, § 11.

39. The Wiretap Act, § 9B.

40. The Wiretap Act, §§ 9-9A.

41. The Wiretap Act, § 13.

42. The Wiretap Act, § 13(a)(2).

requirement for admissibility in these cases is that "an improperly authorised wiretap performed by a person who is in place to obtain legal authorisation will be inadmissible, except if performed in good faith due to an error based on apparent legal authorisation."[43] A 1995 amendment to the Wiretap Act provides that "evidence obtained by a lawful wiretap will be admissible in a criminal proceeding to prove any offense," meaning not just the offense for which the permit was sought but any other offense discovered in the process.[44]

In the past few years, two high level inquiries were conducted into police (but not national security) use of wiretapping, one by a parliamentary committee and the other by the State Comptroller. These investigations were motivated, among other reasons, by high profile irregularities in the police use of wiretapping, including in the case of a government minister suspected of sexual misconduct. The parliamentary committee issued a public report in January 2009, proposing legislative amendments as well as putting in place internal rules and regulations on quality control, data deletion, incidental capture of a call subject to evidentiary privilege, transparency, and more.[45] Some of the proposed amendments were included in a government-sponsored bill submitted to Parliament in 2009 and still making its way through the legislative process.[46] The State Comptroller issued its report in June 2010, sharply criticizing the police for their lack of sufficient guidelines and violations of those guidelines that do exist.[47] The State Comptroller's report included detailed information about the volume of wiretapping permits issued to the police (but not the security services). For example, in 2004, the police petitioned the courts 962 times for wiretap permits, only 3 of which petitions were rejected; similar numbers were revealed for the next four years.[48] These figures appear high compared to those in other Western democracies such as the United States, which has a population 50 times larger than Israel's yet had only 1,773 wiretap permits in 2005; or the UK, with a population 10 times larger than Israel's, and 1,983 wiretap permits.[49] In addition, the State Comptroller expressed concern with the common police practice of obtaining

43. The Wiretap Act, § 13(a)(2).

44. The Wiretap Act, § 13(c1).

45. Summary of Parliamentary Committee Hearings for Investigation of Wiretapping, 26 Jan. 2009, http://bit.ly/GAmJrs.

46. Wiretap Act Bill (Amendment No. 6), 2009, http://www.justice.gov.il/NR/rdonlyres/BD69535B-EC59-45AA-AE63-6DB0C65112F4/16891/455.pdf.

47. State Comptroller Opinion, Wiretapping in Criminal Investigations, June 2010, http://www.mevaker.gov.il/he/Reports/Pages/156.aspx.

48. 2005: 996 petitions, 14 rejected; 2006: 1255 petitions, 7 rejected; 2007: 1484 petitions, 11 rejected; 2008: 1797 petitions, 16 rejected.

49. These figures are derived from the State Comptroller's report, at p. 62. Other Western democracies had a much higher instance of wiretapping authorizations. For example, Italy had 100,000 and Germany 42,000.

authorization for a wiretap based on investigation of a serious felony, only to use the evidence to prosecute a lesser offense.

C. Communications Data

In 2007 the Knesset enacted a new statute regulating the authority of law enforcement agencies to access communications data, the Criminal Procedure Act (Enforcement Powers—Communications Traffic Data), 2007 (Communications Data Act). Until then, law enforcement access to communications (non-content) data was moderated by an arcane provision of a criminal procedure statute dating back to the 1930s titled "seizure of an object."[50]

Notice, however, that access by the ISA to communications data is regulated by a specific provision in the General Security Service Act, 2002 (ISAA). The passage of the Communications Data Act was accompanied by intense public debate, including more than a dozen multi-stakeholder parliamentary hearings. In the process, the new statute was dubbed the "Big Brother Law" in the press and its validity is currently being challenged on constitutional grounds in the Supreme Court. This stands in stark contrast to the ISAA, which confers far broader powers to the ISA and does so without any judicial scrutiny. Several reasons could potentially help explain the relative public acquiescence with the ISAA: First, in 2002 the mobile age was just dawning; the public was unaware of the magnitude of the privacy impact of communications data, which up to that point were perceived as a simple "pen register" of calls.[51] Second, the ISAA was enacted in the midst of the second Intifada; Israel was awash with horrifying terrorism and the public sought a strong ISA. Third, the ISA, like the Mossad and Aman, have always enjoyed special status in Israeli society and are less prone to public criticism than the police.

1. Law Enforcement Access

The Communications Data Act defines "communications data" as "location data, subscriber data, and traffic data; as long as these do not include contents data."[52] As discussed above, access to contents data is regulated by the Wiretap Act. The Communications Data Act sets forth three tracks for law enforcement access to communications data. First, under Section 3 of the Communications Data Act, the police, as well as a list of enumerated law enforcement agencies, can petition a Magistrates Court for authorization to obtain communications data in order to save or protect the life of an individual; to uncover, investigate, or

50. Criminal Procedure Ordinance (Arrest and Search), 1969, § 43.

51. This is the hypothesis of Avi Dichter, the Head of the ISA at the time of legislation, in a conference on "A Decade for the ISAA," College of Management School of Law, March 20, 2012.

52. Communications Data Act, § 1. Each of the terms "location data," "subscriber data," and "traffic data" is further defined in § 1.

prevent a crime; to apprehend and prosecute a criminal; or to confiscate property under the law.[53] The term "crime" is defined broadly to include "a felony or a misdemeanor"—drawing sharp criticism from privacy and human rights activists. Section 3(g) of the Communications Data Act provides that "in its decision and in determining the period of time for access to communications data, the court will bring into consideration . . . the degree of infringement of individual privacy, the severity of the crime, whether the individual is a professional benefiting from an evidentiary privilege, and the type of communications data sought."

The second track allows for access in urgent cases without a court order. Under Section 4 of the Communications Data Act, a senior police officer may issue an urgent order effective for 24 hours "if such an order is necessary to prevent a felony or apprehend a felon or to save the life of an individual and there is insufficient time to petition a court for a Section 3 order."[54] The Communications Data Act requires the police to report periodically to the attorney general and to a parliamentary committee about the number of Section 4 orders issued.[55] Both Section 3 court orders and Section 4 urgent orders are addressed at telecom operators and telecom operators must comply with them promptly. Section 3(i) provides that the reasons specified by a court for a Section 3 order will not be disclosed to the telecom operator. Telecom operators are bound to secrecy under Section 5 of the Communications Data Act, which provides that "[a] telecom provider or its employee will not disclose to a subscriber or any other person the transfer of communications data to the police or any other enforcement agency, except if ordered to do so by a court."[56] Section 15 of the Communications Data Act amended the Wiretap Act, authorizing the court or an officer issuing a wiretap permit to also authorize access to communications data.[57]

The third track, which sparked fierce public controversy, authorizes the police to require a telecom operator, defined for the purposes of this section as strictly a fixed line or cellular operator (i.e., not an ISP), to turn over an updated file containing (1) the identifying details of all of its subscribers[58] including unique device identifiers for their phones or parts thereof, and (2) information concerning the mapping of its cellular antennas, including identifying details for each antenna and its area of coverage.[59] Under Section 7 of the Communications Data Act, the police must maintain the security and confidentiality of the database

53. Communications Data Act, § 3(a).

54. Communications Data Act, § 4(a).

55. Communications Data Act, §§ 4(e) and 14(a)(2).

56. Communications Data Act, § 5.

57. Communications Data Act, § 15, adding § 9C of the Wiretap Act.

58. "Identifying details" is defined as name, ID number, address, and telephone number. Communications Data Act, § 1.

59. Communications Data Act, § 6.

established under Section 6, including logging access and not using the data for any purpose except those authorized under Section 3.

The Communications Data Act authorizes the Minister of Domestic Security to issue regulations governing the maintenance of the Section 6 database. Such regulations must be approved by the parliamentary Constitution, Law and Justice Committee. In August 2008, the Minister of Domestic Security presented the draft regulations to the parliamentary committee; yet his proposal was met by stiff resistance when the hearing surfaced apparent abuses of power by the police. For example, Cellcom, Israel's largest cellular operator, revealed that as a matter of practice the police required access to data items not explicitly enumerated in the Communications Data Act and generously exercised its authority to issue urgent Section 4 orders.[60]

In April 2008, the Association for Civil Rights in Israel (ACRI) petitioned the Supreme Court to invalidate parts of the Communications Data Act, arguing they constituted a disproportionate infringement of the fundamental right to privacy. The Supreme Court heard the case, *ACRI v. Israeli Police*, in an expanded panel, usually reserved for weighty constitutional issues.[61]

In its petition, ACRI focused its criticism on three aspects of the law: First, it argued that permitting access to communications data in the context of misdemeanors is overly broad; it requested that the court limit access to cases involving serious felonies. Second, ACRI argued that the test for providing a judicial order under Section 3 is too loose, enabling the police to obtain orders for the purpose of intelligence gathering without probable cause for a specific crime. Third, ACRI argued that a police officer's power to issue an urgent order under Section 4 must not extend to cases involving a professional benefiting from an evidentiary privilege (e.g., a lawyer or physician). Finally, ACRI argued that the database established under Section 6 of the Communications Data Act must exclude details of individuals who opted-out of caller ID.

Pursuant to the submission of the ACRI's petition, the Israeli Press Council and the Israeli Bar, which enjoys the membership of more than 50,000 lawyers, asked to join ACRI as petitioners. In its petition, the Israeli Bar emphasized the need to craft a specific solution for urgent orders addressed at professionals subject to evidentiary privileges. In addition, it argued that unlike the PPA and the

60. See Protocol No. 639 from meeting of the Knesset Constitution, Law and Justice Committee, August 13, 2008. Cellcom's representative said: "I don't know if this is the time or place to say this, but this statute takes the telecom operators out of the game of data transfers. The police have the authority and ability to cross the data whichever way they want. They'll have the antenna's area of coverage; they'll have the subscribers' database; they can do many things with this information." The regulations were adopted in Dec. 2008. Criminal Procedure Regulations (Enforcement Powers—Communications Traffic Data) (Database of Identifying Communications Data), 2008.

61. HCJ 3809/08 *Association for Civil Rights in Israel v. Israeli Police* (Sup. Ct. May 28, 2012).

Wiretap Act, the Communications Data Act lacks a provision rendering improperly obtained evidence inadmissible at trial.

In May 2012, the Israeli Supreme Court denied the petitions and upheld the validity of the Communications Data Act, despite recognizing its infringement on privacy. In an 82-page decision, the court analyzed the legislation under the constitutional limitation clause, finding that it was enacted for a proper purpose and restricted constitutional rights to an extent no greater than is necessary. At the same time, the Court set forth strict criteria for implementing law enforcement access to communications data under each of the statutory tracks. The court emphasized the accountability of law enforcement authorities to the attorney general and to Parliament. In approving the validity of the law, the Court set forth guidelines, particularly around access to communications data of professionals benefitting from an evidentiary privilege.

2. Security Services Access

As discussed above, the ISA enjoyed broad access to communications data even before the enactment of the Communications Data Act. In the 1990s, the government of Israel decided to enact a law regulating the status and powers of the ISA, which until then operated based on government decisions and without legislative mandate.[62] Years of preparatory work by the legal department of the ISA and the Ministry of Justice led to the enactment of the ISAA in 2002.[63] The ISAA treads a middle path between "skeletal" national security agency statutes, such as the UK's,[64] and voluminous, detailed statutes, such as Australia's.[65] Although not addressing thorny issues such as the use of force in interrogations, the ISAA does introduce a specific section for communications data.[66] Section 11 of the ISAA provides:

> (a) in this section—'Licensee'—as defined in Section 13 of the Telecommunications Act (Telephone and Broadcast), 1982. 'Data'—including communications data, except contents data as defined in the Wiretap Act, 1979.

62. The decision to legislate was motivated by a series of public scandals, such as the execution without trial of two Palestinian terrorists by ISA operatives and later attempt of cover-up (the "Line 300 Scandal"); as well as the Supreme Court decision in the *Public Committee Against Torture* case, supra note 4, outlawing the use of force in interrogations.

63. For a thorough review of the legislative process and rationale see Arye Rotter, The General Security Service Act—Anatomy of Legislation, Mar. 2010. (Rotter was Legal Counsel for the ISA during the legislative process).

64. Security Service Act 1989, c. 5, which has only seven sections.

65. Australian Security Intelligence Organisation Act 1979, Act No. 113 of 1979.

66. General Security Service Act, § 11.

(b) The Prime Minister may set forth rules determining that categories of data found in databases of a licensee are required for the ISA for performing its roles under this law and that the licensee must transfer such categories of data to the ISA.
(c) Any use of data found in a database according to subsection (b) is subject to a permit issued by the Head of the ISA after being convinced that the data are required for the ISA for performing its roles under this law; the permit will specify, inasmuch as possible, details concerning the data sought, the purpose for which they are sought, and the database in which they are found; the permit will be limited in duration for a period not greater than 6 months; except that the Head of the ISA may periodically extend this period.
(d) The Head of the ISA will report quarterly to the Prime Minister and the Attorney General, and annually to the parliamentary committee for ISA matters, about permits issued and data used under this section; reporting details will be set in rules.
(e) The Prime Minister will promulgate rules regarding the retention by a licensee of categories of data according to subsection (b) for a period that he determines and the transfer of categories of data to the ISA; the Prime Minister will determine in rules agreed upon by the Minister of Justice provisions regarding the storage and security of data transferred to the ISA under this section and deletion or destruction of data that are no longer necessary.
(f) Section 13(e) of the Telecommunications Act will apply to the performance of obligations under this section.[67]

The access powers under section 11 of the ISAA apply to data held by "licensees" under the Telecommunications Act. As discussed above, a licensee is defined broadly in the Telecommunications Act to include any fixed line or cellular operator, and ISPs, as well as broadcast licensees (cable and satellite operators).[68]

Section 11(b) grants the prime minister almost unfettered authority to promulgate rules setting forth categories of communications data that a licensee must transfer to the ISA. Such rules were in fact put in place by the prime minister, yet their content remains classified in accordance with Section 19(a)(1) of the ISA.[69] Under Section 11(c) of the ISAA, the Head of the ISA has broad powers to permit ISA access to or use of such categories of communications data that the prime minister set forth in his rules. Indeed, the only condition qualifying both

67. This is the author's translation and is non-binding.

68. Above note 30.

69. Section 19(a)(1) of the ISA provides that "rules, internal instructions, internal procedures and the identity of ISA operatives, in the past or present, as well as additional details concerning the ISA to be determined in regulations, are secret and their disclosure or publishing prohibited."

the prime minister's and Head of ISA's respective authority is that the communications data "are required for the ISA for performing its roles under this law." The communications data subject to the ISA authority include any data held by a licensee with the notable exception of communications contents.[70]

To counterbalance these broad powers, the ISAA sets forth certain transparency requirements. First, under Section 11(c) of the ISAA, the Head of ISA must specify in each permit details concerning the data sought, the purpose for which they are sought, and the database in which they are found. Yet this requirement is tempered by the modifier "inasmuch as possible," effectively allowing for much less detailed permits. In addition, each permit is limited in duration for a period no longer than six months; yet such a term may be extended time and again indefinitely. More significant, under Section 11(d) of the ISAA, the Head of ISA must report periodically to the prime minister and the attorney general (quarterly) and to the parliamentary committee for ISA matters (annually) about permits issued and data used under Section 11. These reporting requirements, although not public or subject to judicial oversight, are significant, as they are made to the highest official in the executive branch (the prime minister) and the legal service (the attorney general), as well as to the legislative branch (the parliamentary committee).

Although formally part of the executive branch, the attorney general enjoys a unique status in Israel's constitutional and administrative system. He is the only legal counsel to the government and the head of the general prosecution. His advice to the government is binding. He provides guidance to the government ministries' legal advisors, who are subject to the authority of the attorney general even where his position conflicts with that of their responsible minister.

Elyakim Rubinstein, a former attorney general and current Supreme Court justice, explains:

> A written directive by the Attorney General instructs the Government ministries to abide by legal opinions; the legal advisor's opinion binds the ministry; the Attorney General's advice binds the government subject, of course, to court decisions.[71]

In court, the government cannot be represented by outside counsel without the agreement of the attorney general, which is very rarely given. The attorney general is a non-political, professional appointment selected by a search committee chaired by a former Supreme Court justice. A candidate for attorney general must himself be eligible to become a Supreme Court justice.

To understand the attorney general's degree of autonomy and isolation from political influence, consider that as head of the prosecution, Israel's last attorney

70. See definition of "Data;" General Security Service Act, § 11(a), which stands in stark contrast to the highly detailed and nuanced definition of communications data in the Communications Data Act.

71. See Elyakim Rubinstein, "The Attorney General in Israel: A Delicate Balance of Powers and Responsibilities in a Jewish and Democratic State," 11:2 *Israel Affairs* 417, 422 (2005).

general Meni Mazzuz indicted an acting president (Moshe Katzav, convicted of rape and sentenced to eight years imprisonment), prime minister (Ehud Olmert, forced to resign, convicted of corruption and sentenced to 27 months imprisonment), minister of finance (Avraham Hirschzon, convicted of corruption and sentenced to 5.5 years imprisonment); and minister of justice (Haim Ramon, convicted of sexual misconduct and sentenced to community service).

By imposing strict reporting requirements on the attorney general, the ISAA strikes a balance between granting the ISA broad powers and imposing a degree of accountability. This balance may not be optimal—given the isolation of the process from public or judicial scrutiny. Yet this arrangement is not trivial as in some other Western democracies where the degree of engagement of the security services with the government legal service may not be as strong, and the government legal service itself not as independent.

The final provision of Section 11 of the ISAA provides immunity from civil or criminal liability to a licensee and its employees for complying with an obligation under the same section. A similar provision does not appear in the Communications Data Act, meaning that a telecom operator or its employee complying with an order under the Communications Data Act must rely on the exemptions in Sections 18(2)(b) or 19(a) of the PPA or Section 6 of the Torts Ordinance (New Version), which provides a blanket immunity from tort liability for non-negligent acts or omissions mandated by a legal obligation or based on a good faith belief in the existence of such an obligation.

Finally, it is important to note that access to communications data for national security purposes under the ISAA is restricted to the ISA; the regime does not apply to additional national security organizations such as the Mossad and Aman, particularly Unit 8200 responsible for SIGINT (signals intelligence).[72] There is no public information concerning these organizations' access to domestic communications data, if any.

3. Data Retention

Unlike the EU,[73] Israel does not have a general data retention statute. This means that the telecom operators could ostensibly delete communications data promptly after using them for their own purposes. Indeed, one interpretation of the purpose limitation provisions in the PPA[74] is that such deletion is *required* by privacy law. To this end, Section 11(e) of the ISAA authorizes the prime minister to promulgate rules "regarding the retention by a licensee of categories of data

72. See, for example, Gil Kerbs, "The Unit," *Forbes*, February 8, 2007, http://www.forbes.com/2007/02/07/israel-military-unit-ventures-biz-cx_gk_0208israel.html.

73. Directive 2006/24/EC of the European Parliament and of the Council of 15 Mar. 2006 on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/EC, 2006 O.J. (L 105) 54 (April 13, 2006).

74. Privacy Protection Act, §§ 2(9) and 8(b).

according to subsection (b), for a period that he determines." As discussed, such rules, if they have been put in place, remain secret. A similar provision is not found in the Communications Data Act, raising doubts whether telecom operators must retain data if not required to do so by the prime minister's national security rules.

The question of whether telecom providers are required (or, conversely, allowed) to retain communications data arose in the *Amir Liran v. Pelephone* case.[75] The plaintiff requested that his two cellular operators delete his communications data after he settled his bill. To assure the cellular operators he was not going to challenge the bills, he was willing to execute a waiver of claims. He argued that the retention of his communications data without a specific purpose infringes his privacy and violates the PPA. The attorney general, who has authority to intervene in litigation in order to represent the public interest, submitted an opinion in the case arguing that the Communications Data Act should be interpreted to permit the retention of communications data by telecom operators "for a reasonable period of time." The Tel Aviv District Court accepted the attorney general's argument, holding that absent a specific obligation to delete communications data, telecom operators were permitted to retain them. This decision was criticized by commentators, including the author of this chapter, who argued that the court misinterpreted the balance struck by the PPA between individual rights and legitimate business interests and failed to take account of the constitutional status of the right to privacy.[76]

4. The Mechanics of Data Transfers

What are the mechanics of data transfers from telecom operators to law enforcement and security services? Are transfers moderated by an employee of the telecom operator, or do data flow at the will of ISA operatives? Is the "switch" to the "pipe" in the hands of the telecom company or the security service? Who pays for retention and use of stored communications data? Although technical, these questions often determine the effective protection provided to subscribers' privacy rights. In practice, human rights are usually protected by detailed procedures and protocols and more easily compromised in their absence.

In *Movement for Freedom of Information v. Ministry of Communications*, the Israeli Movement for Freedom of Information (the Movement), an NGO, petitioned an administrative court under the Freedom of Information Act, 1998 (FOIA), to order the state to make public the "secret annexes" to the licenses of mobile operators and ISPs.[77] The Movement argued that when the government

75. Civ. 1994/06 *Amir Liran v. Pelephone* (Tel Aviv District Ct. November 30, 2010).

76. See Omer Tene, "Cellular Customers Have No Privacy," *The Marker*, January 11, 2011, http://www.themarker.com/law/1.596014; Dan Hay, *Communications Data in Israel* (Tel Aviv: Vital Publishing) 2011, 45–48.

77. Admin. App. 890/07 *Movement for Freedom of Information v. Ministry of Communications* (on file with the author).

awarded mobile operators and ISPs licenses, it annexed secret rules regulating the access of the ISA to the operators' databases. The Movement stated that even as Parliament debates the details of the draft Communications Data Act, the ISA enjoys unrestricted access to similar data without judicial oversight or public scrutiny. The Movement argued that although specific uses or data categories may warrant secrecy, there is no reason to conceal from the public the fact that government access *exists*. The government resisted the FOIA request and the petition, arguing that the annexes do not provide the ISA with any surveillance powers but rather set forth technical specifications for placing the "pipe" through which the data are channeled. Use of the "pipe" is only made in the presence of a statutory mandate, which is available for public review.[78] After having reviewed the "secret annexes" and heard the government's arguments ex parte in closed chambers, the court confirmed that the annexes contain strictly technical specifications as opposed to legal mandates and suggested that the Movement withdraw the appeal, which it did.[79]

An additional question concerns payment for retention and use of stored communications data. Section 10 of the Communications Data Act provides that "a licensee is entitled for reimbursement of expenses related to the transfer of communications data to the police or another investigating authority under Sections 3, 4, or 9, as well as for the transfer of a file under Section 6, in an amount determined by the Minister of Communications (. . .) The amount reimbursed shall be based on recovery of reasonable expenses." Some commentators believe that this provision was the motivating force for the enactment of the Communications Data Act, as before the legislation came into force the telecom operators charged the police high fees to perform similar services.[80] During the legislative hearings, one Member of Parliament suggested intentionally setting a high fee in order to temper the police's zeal to obtain data, thereby protecting individuals' privacy through a prohibitive cost structure.[81]

5. Cybersecurity

On August 7, 2011, the government of Israel approved the establishment of the Israel National Cyber Bureau (INCB) charged with leading the promotion of cyber-related matters in Israel, coordinating between the various bodies, enhancing the protection of national infrastructure from cyberattack, and encouraging the advancement of the subject in industry and academia (Decision

78. The use of the "pipe" metaphor appears in the government's response: Response of the Government of Israel to Admin. App. 890/07, at ¶ 35 (on file with the author).

79. Admin. App. 890/07, protocol and decision of November 5, 2007 (on file with the author).

80. See, for example, Hay, above note 76, at p. 206. In the government-sponsored bill leading to the enactment of the Communications Data Act, the government explained: "The police are required to pay very significant fees to the operators. The rates vary depending on the company, and there is no clear relation between the fee and the expenses incurred."

81. Hay, ibid., at p. 208.

3611). The INCB reports directly to the prime minister. On February 15, 2015, the government approved a comprehensive plan for national readiness in cyberspace, including the establishment of a National Cyber Defence Authority that will have overall national responsibility for cyber defense (Decision 2444).

The Authority, which will be established over a three-year period, will oversee cyber defense actions so as to provide a comprehensive response against cyberattacks including dealing with threats and events in real time. It will also operate an assistance center, a Cyber Event Readiness Team (CERT), for dealing with cyber threats. In connection with the establishment of the Authority, a group of Israeli privacy and data security experts, including the country's former privacy regulator Yoram Hacohen, wrote a letter to the attorney general expressing concern about lack of privacy protections and mechanisms for oversight in the arrangement.

Under Decision 2444, the Authority was required: (1) to conduct, operate, and implement, as needed, all the operational defensive efforts in cyberspace at the national level, including handling cyber threats and incidents in real time, formulating an ongoing situational awareness, consolidating and analyzing intelligence, and working with the defense community as detailed in a classified addendum; (2) to operate the national CERT, including working to improve cyber resilience, providing assistance in handling cyber threats and incidents, consolidating and sharing relevant information with all the organizations in the market, and serving as a central point of interface between the defense community and the organizations in the market; and (3) to build and strengthen the cyber resilience of the entire market through preparedness, training, and regulation.

At this point, it remains to be seen what if any voluntary or obligatory data sharing requirements will be imposed on businesses vis-à-vis the Authority or national CERT.

6. Additional Laws

In addition to the laws discussed above, which focus on communications data, Israel has launched various legislative initiatives involving collection of personal data by government, including a national biometric database (Law on Inclusion of Biometric Identifiers in Identification Documents and Database, 2009), a new credit reporting database (Credit Information Act, 2016), a connected cities initiative (City Without Violence), and a government decision to access to PNR and API (Advance Passenger Information) data of airlines flying to and from Israel (Government of Israel Decision 2258). These laws and initiatives demonstrate an ongoing erosion in privacy protections for individuals' data, particularly when faced with strong state interests.

V. CONCLUDING OBSERVATIONS

Israel regulates government access to communications data through four legislative instruments: the Wiretap Act, which deals with interception of communications contents; the Telecommunications Act, which deals with compatibility with

surveillance technologies; the ISAA, which deals with ISA access to communications data; and the Communications Data Act, which deals with such access by the police. In all cases, broad powers are conferred on the executive branch in the context of national security, reflecting Israel's unique challenges in this space. At the same time, mechanisms for accountability are put in place through periodic reporting requirements to Parliament and to the attorney general.

5

Systematic Government Access to Private-Sector Data in Italy

GIORGIO RESTA

I. ABSTRACT

Italian law contains a variety of different legal provisions relevant to data protection and access to private data by law enforcement.

The relevant sources of law can include interpretations of constitutional provisions by the Italian courts, implementation of EU law into Italian law, and statutory provisions, in particular the Italian "Data Protection Code"; general civil law is also relevant.

Special rules apply to data processing in specific sectors, in particular the judicial sector, law enforcement, and national security.

Several statutes make a broad reporting of private-sector data mandatory. This can include, for example, tax data, data relevant to anti-money-laundering obligations, data relating to mobile phone usage, data of hotel clients, and insurance data.

Legislation provides individuals with the opportunity to assert their rights either by filing a private lawsuit or by filing a complaint with the Italian Data Protection Authority.

II. NATIONAL LEGAL CONTEXT AND FUNDAMENTAL PRINCIPLES

The Italian Constitution does not explicitly protect the right to data privacy. This Constitution was adopted in 1947, when computers and electronic databanks were still unknown. It is not surprising, therefore, that no provision comparable to Article 13 of the Federal Constitution of the Swiss Confederation—according to which "[e]veryone has the right to be protected against the misuse of their personal data"—is to be found in Italy. However, Italy is committed to the rule

Bulk Collection. Fred H. Cate and James X. Dempsey.

of law and the safeguarding of fundamental rights,[1] and several articles of the Constitution provide for the protection of a range of interests that are strictly related to information privacy. One might mention, for instance, Article 14 (inviolability of the home) and Article 15 (privacy of communications). Such provisions have been frequently referred to—together with the general clauses on personal liberty and dignity[2]—as a constitutional basis for the right to privacy.[3]

More importantly, Articles 11 and 117 of the Constitution, recognizing the limitations of sovereignty necessary to achieve international cooperation, have opened the Italian legal system to the influence of European Law.[4] As a result, the right to data protection has acquired—although indirectly—constitutional status. Indeed, it should be recalled that, according to Article 8 of the European Charter of Fundamental Rights, "everyone has the right to the protection of personal data concerning him or her" (following the entry into force of the Lisbon Treaty, the Charter has the same legal status as the European Union Treaties). In a similar vein, the European Court of Justice and the European Court of Human Rights have repeatedly asserted that the right to data protection ranks among the fundamental rights guaranteed by European law.[5] One can conclude, therefore, that information privacy has constitutional (or at least para-constitutional) status in Italy, not through explicit guarantees, but as a result of the interaction between internal and European law.[6]

The influence of European law has proven extremely significant on a statutory level as well. Indeed, until 1996, Italy had no general regulation on data privacy. The only relevant sources were sparse and fragmentary provisions dealing, for instance, with the protection of workers' privacy, or privacy of communications. Italy signed the 1981 Strasbourg Convention for the protection of individuals with regard to automatic processing of personal data; however, this covenant has

1. Art. 2 *Italian Constitution*.

2. Arts. 2, 3, and 13 *Italian Constitution*.

3. See, for instance, the decisions of the Italian Constitutional Court 34/1973; 38/1973; 81/1993; 372/2006. On the protection of privacy under Italian constitutional law see G.M. Salerno, "La protezione della riservatezza e l'inviolabilità della corrispondenza," in R. Nania & P. Ridola, eds., *I diritti costituzionali*, vol. I (Torino: Giappichelli, 2001), 417.

4. See, in particular, art. 117, par. 1: "Legislative power belongs to the state and the regions in accordance with the constitution and within the limits set by European Union law and international obligations."

5. See, for example, ECJ, Case C-293/12, *Digital Rights Ireland Ltd. v. Minister for Communic's, Marine and Natural Res.*, 2014 E.C.R (2014); ECJ, Case C-362/14, *Maximilian Schrems v. Data Protection Commissioner [Ireland],* 2015; EuCtHR, *Roman Zacharov v. Russia*, App. No. 47143/06 (2015).

6. G. Resta, "Il diritto alla protezione dei dati personali," in F. Cardarelli, S. Sica & V. Zeno Zencovich, eds., *Il Codice dei dati personali: Temi e problemi* (Milano: Giuffre, 2004), 31–39; S. Niger, *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali* (Padova: CEDAM, 2006).

not been transposed into Italian law until recently. Only in 1996 did Italy pass a bill on the protection of individuals with regard to the processing of personal data, implementing the Directive 95/46/EC.[7]

In 2003 this act had been repealed and substituted by a "Data Protection Code" (hereinafter Data Protection Code) (d.lgs. 196/2003). This statute is conceived as a general law on information: it applies to the processing of personal data (defined as "any information relating to natural persons that are or can be identified, even indirectly, by reference to any other information including a personal identification number") with or without electronic means. Article 2, paragraph 1 states the purposes of the Data Protection Code as follows: "[t]his consolidated statute [. . .] shall ensure that personal data are processed by respecting data subjects' rights, fundamental freedoms and dignity, particularly with regard to confidentiality, personal identity and the right to personal data protection."

The linkage between the information privacy and the category of fundamental rights cannot be overlooked.[8] On a statutory level, this provision confirms the primary status of the right to data protection, conceived as an expression of dignity. Consistent with this approach, the second paragraph of Article 2 lays down the principle that "[t]he processing of personal data shall be regulated by affording a high level of protection for the rights and freedoms referred to in paragraph 1 [. . .]". The Italian Constitutional Court has indirectly confirmed the particular relevance of the right to data protection. In a 2005 ruling, for instance, the Court decided that, in the event of a conflict between the Data Protection Code and a regional law (Italy is not a federal state, but regions have the power to legislate in several fields), the former shall prevail, as information privacy is part of the general civil law framework (*ordinamento civile*) mentioned by Article 117 Const.[9] The institutional safeguards established by state law cannot therefore be infringed by contrasting provisions adopted by the regions.

III. STATUTORY AND REGULATORY OVERVIEW

The rules on information processing set out in the Data Protection Code are applicable both to the private and the public sector. Given the wide scope of application of the statute, the right to data protection must be constantly balanced against conflicting interests. Many of them have constitutional status as well. To name a few: freedom of expression (Article. 10 Const.), proper and fair operation of public affairs (Article 97 Const.), fair administration of justice (Article 111 Const.), and protection of health (Article 32 Const.). Striking a balance between

7. Law 675/1996, *Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali.*

8. S. Rodotà, "Tra diritti fondamentali ed elasticità della normativa: il nuovo Codice sulla *privacy*," in *Eur. Dir. Priv.* (2004), 2.

9. See Corte cost., 271/2005, in *Giur. cost.*, 2005, 2519, with a comment by A. Celotto, "Una additiva di principio 'inutile' o 'ridondante?'".

such values is never an easy task, and this is even more so in the public sector. Two factors play a major role. On the one hand, the greater expansion of the welfare state has enhanced the need for a capillary system of information retrieval and processing, not only with the purpose of making social services available, but also of preventing fraudulent behaviors. Several databanks have been established with this purpose in mind. Suffice it to mention, as a single example, the social security benefits database (*Casellario dell'assistenza*).[10]

On the other hand, the development of information and communication technologies and the increasing computerization of the public administration have made the setup and interconnection of data sets much easier, giving rise to more comprehensive and intrusive collections. It should also be added that the financial crisis has strengthened the pressure toward the adoption of measures aimed at curtailing tax evasion (Italy is among the top three ranking countries of the world for tax evasion)[11] and fraudulent behaviors in the field of social security benefits. As a result, "systematic" access to private data,[12] despite its strong impact on fundamental freedoms, is increasingly resorted to by the government.[13] However, the Data Protection Code laid down a detailed set of rules and principles aimed at striking an acceptable balance between private and public interests involved in the processing of personal data by public bodies.[14] I will stress here only three points.

(a) First, the whole regime is based on the principle of *use limitation*. The processing of personal data is not allowed for all purposes; public bodies are only permitted to process personal data "in order to discharge their institutional tasks" (Article 18, paragraph 2). Such a requirement is consistent with Article 7 of the Data Protection Directive, according to which personal data may be processed—among other conditions—if the "processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed."

10. This database has been set up on the basis of Art. 13, Decree-Law 78/2010 and Decree 206/2014.

11. See http://www.repubblica.it/economia/2012/10/03/news/corte_conti_evasione_italia_primissimi_posti-43782971/ (quoting the declaration of the head of the Italian Court of Auditors) (last visited April 30, 2017).

12. On this notion see Fred H. Cate, James X. Dempsey & Ira S. Rubinstein, "Systematic Government Access to Private-Sector Data," 2 *Int. Data Privacy L.* 195 (2012).

13. See *infra,* par. 4.

14. See A. de Tura, "Le regole ulteriori per i soggetti pubblici," in V. Cuffaro, R. D'Orazio & V. Ricciuto, eds., *Il codice del trattamento dei dati personali* (Torino: Giappichelli, 2007), 163–91.

(b) Second, *different standards* have been laid down in the Code, depending on the features of the data. (*i*) If the processing concerns sensitive data[15] and judicial data, it is allowed only if authorized by a law "specifying the categories of data that may be processed and the categories of operation that may be performed as well as the substantial public interest pursued" (Article 20). Lacking such a statutory basis, public bodies may request the Data Protection Authority (*Garante per la protezione dei dati personali,* hereinafter *Garante*) to determine the activities that pursue a substantial public interest among those they are required to discharge under the law. However, the Code makes clear that the processing of sensitive and judicial data by public bodies should be carried out only in exceptional situations; that is, it should be considered as *extrema ratio.* According to Article 22, paragraph 3, public bodies may process such sensitive and judicial data as are "indispensable for them to discharge institutional tasks that cannot be performed, on a case by case basis, by processing anonymous data or else personal data of a different nature" (this is frequently referred to as the principle of *necessity,* or *data minimisation*).[16] Also, particular technical measures should be adopted, in order to enhance the security of processing operations.[17] (*ii*) Data other than sensitive and judicial can be processed even in the absence of laws or regulations expressly providing for such processing. Particular rules apply to the communication[18] of such data to third parties, including public bodies. In this case, the communication is permitted only if it is envisaged by laws or regulations. Lacking such laws or regulations, the communication is allowed if two conditions are met: *a*) it is necessary in order to discharge institutional tasks; and *b*) the *Garante* has been notified of the intention to communicate the data and has not withheld its approval within 45 days.

(c) Last, one should note that, according to Article 18 of the Data Protection Code, *public bodies must abide by the rules, requirements, and limitations set out in the Code*. This means, in particular, that

15. Sensitive data are defined by the Code as "personal data allowing the disclosure of racial or ethnic origin, religious, philosophical or other beliefs, political opinions, membership of parties, trade unions, associations or organizations of a religious, philosophical, political or trade-unionist character, as well as personal data disclosing health and sex life."

16. R. D'Orazio, "Il principio di necessità nel trattamento dei dati personali," in V. Cuffaro, R. D'Orazio & V. Ricciuto, eds., *Il codice del trattamento dei dati personali*, above note 14, at 163–91.

17. Art. 22, par. 6 and 7, Data Protection Code.

18. As regards the distinction between the "communication" and the "dissemination" of personal data, see art. 4, Data Protection Code.

personal data undergoing processing must be "relevant, complete and not excessive in relation to the purposes for which they are collected or subsequently processed";[19] and that "[i]nformation systems and software shall be configured by minimizing the use of personal data and identification data."[20] Such principles are particularly relevant because they work as an indirect limitation of the government's power to indefinitely expand the size and number of databases containing personal data. Indeed, when called upon to issue recommendations on proposed bills and regulations pursuant to Article 154 Data Protection Code, the *Garante* has frequently referred to these principles.[21] In several cases, the government has been required by the *Garante* to adopt changes on proposed bills, on the ground that they did not conform to the principles of "necessity and data minimisation."[22] These principles can be regarded, therefore, as important parameters to assess the proportionality of statutes and regulations providing for the collection and systematic access to personal data.

IV. RULES APPLYING TO SPECIAL SECTORS

Different rules apply to the sectors of the administration of justice, law enforcement, and national security. They are generally characterized by a policy of weaker protections for data subjects and stronger support for the interests of data controllers. The relevant sources are to be found both in the Data Protection Code and in special statutes.

19. Art. 11 Data Protection Code.

20. Art. 3 Data Protection Code.

21. According to Art. 154, one of the main tasks of the *Garante* consists in "drawing the attention of Parliament and Government to the advisability of legislation as required by the need to protect the rights referred to in Section 2, also in the light of sectoral developments." Paragraph 3 of the same Article 154 provides also that "The Prime Minister and each Minister shall consult the Garante when drawing up regulations and administrative measures that are liable to produce effects on the matters regulated by this Code."

22. See, for instance, *Garante prot. Dati,* 7-7-2011, *Sistema informativo nazionale per la prevenzione nei luoghi di lavoro (SINP) e regole per il trattamento dei dati*, web doc. n. 1829704; *Garante prot. dati,* 21-3-2012, *Parere del Garante al Ministro della salute in ordine a uno schema di decreto recante "Modifiche al decreto del Ministro del lavoro, della salute e delle politiche sociali del 17 dicembre 2008, pubblicato nella Gazzetta Ufficiale n. 9 del 13 gennaio 2009, recante "Istituzione del sistema informativo per il monitoraggio delle prestazioni erogate nell'ambito dell'assistenza sanitaria in emergenza-urgenza"*, web doc. n. 1892560; *Garante prot. dati,* 17-4-2012, *Parere del Garante su uno schema di decreto del Ministro della salute concernente "Modifiche al decreto del Ministro del lavoro, della salute e delle politiche sociali recante "Istituzione della banca dati finalizzata alla rilevazione delle prestazioni residenziali e semiresidenziali"*, web doc. n. 1907937.

A. Processing of Personal Data in the Judicial Sector

The processing of personal data in the judicial sector is regulated by Articles 46–49. If personal data are collected, stored, or processed for "purposes of justice"—that is, if the processing "is directly related to the judicial handling of matters and litigations, [. . .] or if it is related to auditing activities carried out in respect of judicial offices"[23]—a series of rules set out in the Code will *not* apply.[24] Among them are the provisions concerning a data subject's right to access (Articles 9–10), the duty to inform (Article 13), termination of processing (Article 16), general principles concerning processing by public bodies (Articles 18–22), duty of notification to the *Garante* (Articles 37–38), trans-border data flows (Articles 42–45), and nonjudicial remedies before the *Garante* (Articles 145–151).

By contrast, the principles enshrined in Article 11 are applicable also to the judicial sector. Therefore, personal data undergoing processing shall be processed lawfully and fairly; collected and recorded for specific, explicit, and legitimate purposes, and used in further processing operations in a way that is not inconsistent with said purposes; accurate and, when necessary, kept up to date; relevant, complete, and not excessive in relation to the purposes for which they are collected or subsequently processed; and kept in a form that permits identification of the data subject for no longer than is necessary for the purposes for which the data were collected or subsequently processed.

These safeguards are particularly relevant in the judicial sector, as court databases—which may have a significant impact on an individual's rights and freedoms—need to be extremely accurate and always kept up to date. As regards the access by judicial authorities to data, information, and records from other public bodies,[25] Article 48 provides that such acquisition "may also take place electronically. To that end, judicial offices may avail themselves of the standard agreements made by the Minister of Justice with public bodies in order to facilitate interrogation by said offices of public registers, lists, filing systems and data banks via electronic communication networks, whereby compliance with the relevant provisions as well as with the principles laid down in Sections 3 and 11 of this Code shall have to be ensured."[26]

23. Art. 47, par. 2, Data Protection Code.

24. For a detailed analysis see G. Buonomo, "Il trattamento dei dati personali in ambito giudiziario," in V. Cuffaro, R. D'Orazio & V. Ricciuto, eds., *Il codice del trattamento dei dati personali*, above note 14, at 277.

25. See G. Buonomo, "Il trattamento dei dati personali in ambito giudiziario," above note 24, at 293.

26. The database relating to children suitable for adoption set up in February 2013 by the Ministry of Justice (and specifically provided for by Art. 40, law 149/2001) is just one example of the many databases established for "justice reasons" (see http://www.giustizia.it/giustizia/it/mg_2_5_8.wp).

B. Law Enforcement

The processing of personal data by police forces for purposes of law enforcement and public security is also subject to a special regime.[27] It does not differ too much from the one relating to the judicial sector. Indeed, according to Article 53, several provisions of the Code shall not apply "to the processing of personal data that is carried out either by the Data Processing Centre at the Public Security Department or by the police with regard to the data that are intended to be transferred to said centre under the law, or by other public bodies or public security entities for the purpose of protecting public order and security, or the prevention, detection or suppression of offences as expressly provided for by laws that specifically refer to such processing." As explained above in more detail, among the provisions exempted are Articles 9, 10, 12, 13, and 16; 18 to 22; 37, 38(1) to (5), and 39 to 45; and Articles. 145–151. As regards the conditions that have to be satisfied in order to gain the exemptions mentioned by Article 53, the processing has to be carried out: (1) by police authorities or equivalent public bodies; (2) for the purpose of protecting public order and security, or the prevention, detection, or suppression of crimes; and (3) pursuant to a statute (not simply a regulation) that specifically provides for such processing.

Particularly relevant for the issue of systematic access is Article 54. It provides that, in order to acquire data, records, and documents from other subjects (in accordance with the laws and regulations in force), public bodies "may avail themselves of agreements aimed at facilitating interrogation by said bodies or offices, via electronic communication networks, of public registers, lists, filing systems and data banks in pursuance of the relevant provisions as well as of the principles laid down in Sections 3 and 11." [28] It has to be emphasized that, upon a favorable opinion given by the *Garante,* the Minister for Home Affairs shall adopt such standard agreements.[29] This is an important institutional safeguard, aimed at ensuring that information privacy is adequately protected, and that access is limited only to the personal data necessary to the purposes mentioned by paragraph 1. The *Garante* has made use of its powers of advice and oversight on several occasions.[30] Also, prior communication shall be given to the *Garante* as regards the technical measures taken to safeguard data subjects, whenever they face higher risks of harm, "having regard, in particular, to genetic or biometric

27. I. Iai, "Il trattamento dei dati personali da parte delle forze di polizia e per la difesa e sicurezza dello Stato," in V. Cuffaro, R. D'Orazio & V. Ricciuto, eds., *Il codice del trattamento dei dati personali*, above note 14, at 303.

28. On this see ibid., at 313–16.

29. Art. 54, par. 1, Data Protection Code.

30. See, for instance, *Garante prot. dati,* 26-5-2011, *Convenzione fra il Ministero dell'interno-Dipartimento della pubblica sicurezza e l'Agenzia delle entrate per l'accesso da parte delle forze di polizia alla banca dati dell'Anagrafe tributaria attraverso l'applicativo denominato Puntofisco*, web doc. n. 1822278.

data banks, technology based on location data, data banks based on particular data processing techniques and the implementation of special technology."[31]

Furthermore, it is provided that the Data Processing Centre at the Public Security Department—which is one of the biggest and most important data-banks in this sector, and probably one of the biggest of all Italian databanks—"shall be responsible for ensuring that the personal data undergoing processing are regularly updated, relevant and not excessive, also by interrogating—as authorised—the register held by the Criminal Records Office and the register of pending criminal proceedings at the Ministry of Justice pursuant to Presidential Decree no. 313 of 14 November 2002 as well as other police data banks that are required for the purposes referred to in Section 53" (Article 54, paragraph 3).[32] Finally, according to Article 57, "a Presidential Decree issued following a resolution by the Council of Ministers, acting on a proposal put forward by the Minister for Home Affairs in agreement with the Minister of Justice, shall set out the provisions implementing the principles referred to in this Code with regard to data processing operations performed by the Data Processing Centre as well as by police bodies, offices and headquarters for the purposes mentioned in Section 53."

We should also mention the much-debated issue of a central DNA database.[33] Italy ratified in 2009 the Treaty of Prüm,[34] providing for the establishment of a national DNA database containing human biological materials and genetic profiles of persons convicted of serious crimes or under arrest. Judicial authorities and police forces shall only access such data for purposes of personal identification, or in order to accomplish tasks required by the cross-border collaboration between police forces.[35] Given the particular risks involved, the DNA database has been put under the oversight of the *Garante*, which has already issued several recommendations concerning safety measures and access to the database.[36] After a long discussion, the DNA database has been set up and made operative on the basis of the Decree 7-4-2016, n. 87.

31. Art. 55 Data Protection Code.

32. See Iai, "Il trattamento dei dati personali da parte delle forze di polizia e per la difesa e sicurezza dello Stato," above note 27, at 318–19.

33. See L. Scaffardi, "Le banche dati genetiche per fini giudiziari e i diritti della persona," in C. Casonato, C. Piciocchi & P. Veronesi, eds., *Forum BioDiritto 2008: Percorsi a confronto* (Padova: CEDAM, 2009), 453.

34. Law n. 85/2009, *Adesione della Repubblica italiana al Trattato concluso il 27 maggio 2005 tra il Regno del Belgio, la Repubblica federale di Germania, il Regno di Spagna, la Repubblica francese, il Granducato di Lussemburgo, il Regno dei Paesi Bassi e la Repubblica d'Austria, relativo all'approfondimento della cooperazione transfrontaliera, in particolare allo scopo di contrastare il terrorismo, la criminalità transfrontaliera e la migrazione illegale (Trattato di Prum).*

35. Art. 12 Law n. 85/2009.

36. *Garante prot. dati,* 15-10-2007, *Banca dati DNA,* web doc. n. 1448799.

Particularly relevant are the rules concerning the privacy aspects of the operations aimed at searching evidence of crimes: telephone and electronic traffic data retention, wiretapping, and interception of Internet communications.

1. Data Retention

The retention of telephonic traffic data for the purposes of detecting and countering criminal offenses is regulated by Article 132 Data Protection Code, as amended first by law n. 48/2008, implementing the Budapest Convention on cybercrime (2001), and then by legislative decree 48/2008, implementing the Directive 2006/24/EC.[37]

Article 132, in its original version, adopted different periods of data retention, depending on the seriousness of the offenses and the purposes of the investigation. The amended version has laid down a unitary regime. Traffic data shall be retained by the provider for 24 months; electronic communications traffic data shall be retained for 12. As regards the data relating to unsuccessful calls, they shall be stored for 30 days.[38] Within the 24 months, the public prosecutor (also at the request of private parties involved in the proceedings) may issue a motivated order, acquiring the data from the provider.[39]

It is worth noting that European Court of Justice annulled the EU Data Retention Directive in 2014;[40] nonetheless the Italian regulatory framework as of today remains unchanged.

2. Freezing

An important tool for investigations is represented by so-called "freezing" orders, that is, a nonjudicial proceeding consisting of the access by the police to electronic traffic data (and namely Internet communications data) held by IT and Internet service providers (also known as "preservation orders"). Article 132, paragraph 4-*ter* Data Protection Data, grants the Minister for Home Affairs or the heads of the central offices specializing in computer and/or IT matters from the police forces (*Polizia di Stato, Carabinieri* and *Guardia di Finanza*) the power to order IT and/or Internet service providers to retain and protect Internet traffic data ("*traffico telematico*") for no longer than 90 days, in order to carry out the pretrial investigations referred to by Article 226 *Norme di attuazione, coordinamento e transitorie del codice di procedura penale*, or else with a view to the detection and suppression of specific offenses. The term of 90 days may be

37. On this see A. Cappuccio, "*Privacy* e comunicazioni elettroniche," in G.F. Ferrari, ed., *La legge sulla privacy dieci anni dopo* (Milano: EGEA, 2008), 237–46; *Garante prot. dati,* 17-1-2008, *Sicurezza dei dati di traffico telefonico e telematico,* web doc. n. 1482111.

38. Art. 132, par. 1-*bis,* Data Protection Code.

39. Art. 132, par. 3, Data Protection Code.

40. See *e.g.* ECJ, Case C-293/12, *Digital Rights Ireland Ltd. v. Minister for Communic's, Marine and Natural Res.*, 2014 E.C.R (2014).

extended, on legitimate grounds, up to six months, while specific arrangements may be made for keeping the data under control as well as for ensuring that such data cannot be disposed of by the IT and/or Internet service providers and operators and/or third parties.

According to Article 132, paragraph 4-*quater*, any provider who receives such an order shall comply without delay and is required to keep the request confidential. The measures taken under paragraph 4-*ter* shall be notified in writing to the public prosecutor, who shall endorse them if the relevant preconditions are fulfilled. If the public prosecutor withholds its consent, the measures cease to be enforceable.[41]

3. Interceptions

Whereas Article 132 Data Protection Code deals with the traffic data, the main legal source relating to wiretapping and interception of private communications is the Criminal Procedure Code.[42] Telephone, electronic, and live ("environmental") interceptions are among the most important tools for investigations. Indeed, they are massively employed in Italy: according to the Minister of Justice, the total number of telephonic interceptions carried out in the year 2011 is 135,533. Out of them, 121,072 were wiretappings, 11,888 live ("environmental") interceptions, and 2,573 were interceptions of a different kind (in particular electronic interceptions).[43] However, they are also among the most intrusive tools, as they strongly interfere with the liberty and confidentiality of communications, protected by art. 15 Const., and with the inviolability of the home, protected by art. 14 Const. Personal communications may be intercepted only under the conditions set by Articles 266–269 Criminal Procedure Code. Interceptions have to be authorized by judicial authorities and can be carried out exclusively in investigations of serious offenses.[44]

C. National Security

A special regime also applies to the processing operations carried out by the Italian intelligence agencies (*AISI:* Internal Information and Security Agency; *AISE*: External Information and Security Agency), as well as for classified information.[45] In accomplishing their tasks, intelligence agencies have to abide

41. Art. 132, par. 4-*quinquies,* Data Protection Code.

42. For an overview see *Intercettazioni di conversazioni e comunicazioni: Un problema cruciale per la civiltà e l'efficienza del processo e per le garanzie dei diritti. Atti del Convegno: Milano, 5–7 ottobre 2007* (Milano: Giuffrè, 2009).

43. See *Relazione del Ministero sull'Amministrazione della Giustizia. Anno 2012* (Roma, 2012), 249, http://www.giustizia.it/giustizia/protected/812055/0/def/ref/NOL811573/.

44. Offenses with a maximum sentence of up to five years' imprisonment and other offenses specifically mentioned in Article 266.

45. See I. Iai, "Il trattamento dei dati personali da parte delle forze di polizia e per la difesa e sicurezza dello Stato," above note 27, at 320.

by the principles laid down by Articles 3 and 11 (data minimization, necessity, lawfulness, fairness, use limitation, accuracy) and by a series of further provisions, such as the ones concerning the prohibition of profiling (Article 14), the liability for damages (Article 15), the security measures (Articles 31 and 33), and the relationship with the *Garante* (Articles 154, 160, and 169). The solutions adopted by the Data Protection Code seem to be quite innovative and courageous, at least from a comparative law perspective.[46] Indeed, a sector traditionally characterized by the priority of public interests over individual rights and by the almost complete absence of external checks, consistently with the idea that *salus rei publicae suprema lex esto*, has now been subject to some of the most important rules and principles of the Data Protection Code.

V. LAWS REQUIRING BROAD REPORTING OF PERSONAL DATA

Several statutes make a broad reporting of private-sector data mandatory. What follows is an overview of some of the most important examples.

A. Tax Laws

A significant expansion of the hypotheses of systematic access to private-sector data can be observed in the fiscal sector. The need to fight against the extremely high level of tax fraud and tax evasion—magnified by the economic and financial crisis—is clearly the most important factor behind such policy. An emblematic example is represented by the new legal regime concerning personal information that can be accessed and obtained by the tax registry office. The so-called "Save-Italy" Decree, adopted by the emergency government led by Professor Monti in December 2011,[47] imposed on financial operators the obligation to periodically notify the tax registry office of activity in all the accounts held with them and any other information concerning such accounts needed to carry out tax controls.[48] Transactions of less than €1,500 carried out using a postal current account in-payment form are exempted from such notification duties.[49]

It should be stressed that the duty to communicate is automatic and independent from any charge or suspicion of tax evasion. Also, the General Manager of the Italian Revenue Agency can issue specific regulations, expanding the typology

46. See generally, G. Romeo, "Il diritto alla privacy e la lotta al terrorismo," in G.F. Ferrari, ed., *La legge sulla* privacy *dieci anni dopo*, above note 37, at 181–201; one of the best comparative analyses on this issue is F. Bignami, "European versus American Liberty: A Comparative Privacy Analysis of Anti-terrorism Data-Mining," 48 *Boston College Law Review* 609 (2007).

47. Decree-law n. 201/2011, *Disposizioni urgenti per la crescita, l'equità e il consolidamento dei conti pubblici*, converted into law by law n. 214/2011.

48. Art. 11, par. 2, Decree-law n. 201/2011.

49. Art. 7, par. 6, Presidential Decree n. 605/1973.

and the amount of information that has to be communicated. Furthermore, the Italian Revenue Agency and the *Guardia di Finanza* are to be notified by the National Institute of Social Security (*Istituto nazionale di previdenza sociale*) of the records of all beneficiaries of social benefits; such data shall then be matched with tax returns in order to prevent tax evasion.[50]

The *Garante* has played an important role in the regulatory process; following a communication by the General Manager of the Revenue Agency, it required a series of changes to the draft decrees relating to access to financial records, with the aim of increasing the safety of the system and reducing the risk of leaks in the information flow or abusive access to the data.[51]

Another example of mandatory communication of personal data is offered by the Decree-Law n. 78/2010, which makes it compulsory for financial operators to notify the Italian Revenue Agency of the purchases made by private individuals using credit cards and e-money for an amount of more than €3,600.[52]

B. Anti-money Laundering Legislation

Money laundering legislation also places obligations on a wide range of subjects (financial operators, non-financial enterprises, and various professionals, such as accountants, public notaries, lawyers, etc.) to make reports on suspicious transactions to the Financial Intelligence Unit.[53] Such a Unit was established at the Bank of Italy, pursuant to Art. 6 Legislative Decree 231/2007. It is charged with the task of carrying out financial analysis of the suspicious transactions and of examining any other fact that could be related to money laundering or terrorist financing. Once completed, the results of the analyses have to be transmitted to judicial and police authorities—also foreign authorities—for subsequent investigation.[54] The *Garante* has issued several recommendations concerning the data privacy aspects of such information exchanges.[55]

C. Hotel Clients

Italy differs from many Western countries in that it has long had an intrusive system of automatic reporting of the identity of hotel clients to police authorities.

50. Art. 11, par. 6, Decree-law n. 201/2011.

51. *Garante prot. dati,* 17-4-2012, *Comunicazione dei dati contabili all'anagrafe tributaria da parte di banche e operatori finanziari: parere all'Agenzia delle entrate sulle modalità di trasmissione e di conservazione dei dati*, web doc. n. 1886775; Garante prot. dati, 18-9-2008, *Anagrafe tributaria: sicurezza e accessi*, web doc. n. 1549548.

52. Art. 21, Decree-Law n. 78/2010, *Misure urgenti in materia di stabilizzazione finanziaria e di competitività economica*, converted into law by law n. 122/2010.

53. Arts. 10-35 Legislative Decree n. 231/2007, implementing Directive 2005/60/EC.

54. Art. 9 Legislative Decree n. 231/2007.

55. *Garante prot. dati,* 25-7-2007, *Nuova disciplina antiriciclaggio*, web doc. n. 1431012.

Originally provided for by Article 109 TULPS (*Testo unico leggi di pubblica sicurezza*), enacted in 1931 under the fascist dictatorship, the duty of hotelkeepers and similar subjects to identify their clients (Italians and foreigners), register their personal particulars, and notify the police without delay of such information was never eliminated during the Republican era and is still effective today. January 2013 the Minister of Internal Affairs, following a formal consultation with the *Garante,*[56] has issued a new decree, regulating the whole matter. It provides that the hotelkeepers shall report the personal particulars of their clients within 24 hours to police authorities.[57] Such data may be transmitted by electronic means and will be recorded in a central database established at the Ministry for Internal Affairs. The data shall be accessed only by judicial and police authorities for the purpose of protecting public order and security, or the prevention, detection, or suppression of offenses.[58] After five years, the data have to be erased.

D. Cell Phones

Another example of compulsory reporting of private-sector data, particularly relevant in practice, is offered by the Electronic Communications Code. According to Article 55, paragraph 7, telecommunications companies are required to identify at the time of the activation of the service all subscribers and buyers of prepaid cell phone cards, and notify (also by electronic means) the Ministry of the Internal Affairs of the list of these names. Judicial authorities may access these data "for justice purposes,"[59] that is for purposes "related to the judicial handling of matters and litigations."[60]

E. Insurance Frauds

Fraudulent behaviors with regard to compulsory insurance are unfortunately quite common. Therefore, art. 135 Private Insurance Code establishes a database on car accidents, with the aim of enhancing "prevention and combating of fraudulent behaviours in compulsory insurance for motor vehicles registered in Italy."[61] Pursuant to this provision, insurance companies are required to notify

56. *Garante prot. dati,* 18-10-2012, *Schema di decreto ministeriale sulla comunicazione alle autorità di P.S. dell'arrivo di persone alloggiate in strutture ricettive*, web doc. n. 2099252.

57. Art. 1 Minister of Internal Affairs Decree 7-1-2013, *Disposizioni concernenti la comunicazione alle autorita' di pubblica sicurezza dell'arrivo di persone alloggiate in strutture ricettive.*

58. Art. 4 Decree 7-1-2013.

59. Art. 55, par. 7, Leg. Decree n. 259/2003, *Codice delle comunicazioni elettroniche.*

60. Art. 47, par. 2, Data Protection Code.

61. Art. 135, Leg. Decree n. 209/2005, *Codice delle assicurazioni private*. For a detailed analysis see A. Longo, "*Privacy* e assicurazioni," in V. Cuffaro, R. D'Orazio & V. Ricciuto, eds., *Il codice del trattamento dei dati personali*, above note 14, 570–74.

the Institution for the supervision of private insurance (*ISVAP*, now *IVASS*) of the data about the accidents in which their policyholders are involved, on the basis of the procedures established by regulation adopted by the same Institution. This regulation was issued in 2009, following a consultation procedure with the *Garante*.[62] It is provided that such data shall be accessed by judicial authorities, public bodies in charge of detecting fraudulent behaviors in the sectors of compulsory insurance, insurance companies, and a series of other subjects, for the purpose of preventing and combating frauds. The nominative records will be stored for no longer than five years. Most of the principles laid down by the Data Protection Code shall apply to the processing operations.

VI. COURTS

According to Article 145 Data Protection Code, the data subject's rights may be enforced either by filing a lawsuit or by lodging a complaint with the *Garante*. Given the shorter time and the lesser costs involved in an action before the *Garante*, nonjudicial remedies have frequently been preferred over judicial ones. Therefore, the case law of the *Garante*—easily accessible on the Internet—is extremely important to grasp the state of the art in the field of information privacy.[63] However, the Italian courts have been called upon to decide important cases as well. The Italian Court of Cassation ruled that the debits and credits records of condo tenants and owners—although "personal data" according to the Data Protection Code—may be lawfully communicated by the condo manager to other members of the condominium.[64] In 2013 the Court of Naples reviewed the so-called *Redditometro* regulation (enabling the Revenue Agency to analyze household spending patterns and compare these with the household's earnings, with the aim of curtailing tax evasion),[65] and declared it void

62. ISVAP Regulation 1-6-2009, n. 31, *Regolamento recante la disciplina della banca dati sinistri di cui all'articolo 135 del decreto legislativo 7 settembre 2005*, n. 209—*Codice delle assicurazioni private; Garante,* 30-11-2005, *Parere sullo schema di regolamento per il trattamento dei dati sensibili e giudiziari dell'Istituto per la vigilanza sulle assicurazioni private e di interesse collettivo (Isvap)*, web doc. n. 1212464.

63. For an overview see G.F. Ferrari, ed., "La legge sulla privacy dieci anni dopo," above note 37.

64. Court of Cassation, n. 1593/2013. On this issue see also *Garante prot. dati, Data Protection and Management of Condos*, Provision of 18 May 2006, web doc. n. 1332463.

65. Minister of Finance Decree 24-12-2012, *Contenuto induttivo degli elementi indicativi di capacità contributiva sulla base dei quali può essere fondata la determinazione sintetica del reddito*. On this regulation see H. Burggraf, "Italians Protest as *Redditometro* Unveiled to Pursue Tax Cheats," *International Adviser* (January 21, 2013), http://www.international-adviser.com/news/tax-regulation/italians-protest-as-redditometro-unveiled. A. Johnston, "Italian Tax Dodgers Uncovered by the Redditometro," *BBC News* (January 21, 2013), http://www.bbc.co.uk/news/business-21064030.

as against the right to information privacy, protected by arts. 2 and 13 Const., and by arts. 1, 7 and 8 European Charter of Fundamental Rights.[66] This decision has been much debated and occasionally criticized,[67] but is a good example of the delicate problems arising from the systematic access by the public bodies to private-sector data.

66. Court of Naples, ord. 21-2-2013, http://www.lavorofisco.it/docs/redditometro-ordinanza-giudice-redditometro.pdf.

67. V. Onida, "Sbagliato giustificare l'evasione in nome del diritto alla privacy," *Corriere della sera* (February 26, 2013) 60; but see also, from a different perspective, P. Ostellino, "Il reddito-metro del Dottor Stranamore," *Corriere della sera* (January 6, 2013) 32.

The Americas

6

Systematic Government Access to Private-Sector Data in Brazil

BRUNO MAGRANI*

I. ABSTRACT

This chapter describes the ways through which the Brazilian government may have access to personal data in possession of private-sector organizations with a specific focus on identifying the possibility of systematic access. There is no comprehensive data protection legislation in Brazil. However, a law from 2014 together with specific statutes regulate governmental access for cases such as law enforcement access to data from the Internet and telecommunications companies, wiretapping, financial data, money laundering, and national intelligence. There have been many conflicting decisions in the judiciary about governmental access to personal data, particularly registration data. In an attempt to address this issue, a 2012 statute expanded the investigative powers of the police and the Public Prosecutor's Office, granting them access to registration data regardless of a court order. Later in 2014, the so called "Marco Civil da Internet" established new rules about government access to both registration data and the content of digital communications. An evaluation of several statutes revealed the existence of at least one potential case of systematic access granted by the law to the telecommunications regulatory agency.

* This chapter was first drafted around 2011 and at some point after 2014. During that period, Brazil was going through very intense legislative debates about data privacy regulation and Internet regulation. For this reason, I decided to take out most of the references to legislative proposals discussed by Congress and focus instead on the statutes and some of the recent decisions rendered by the high courts. Additionally, given the recent approval by Congress of the 2014 Internet Bill of Rights—also referred to here as "Marco Civil da Internet"—there was still no sufficiently stable or consolidated interpretation of this regulation by Brazilian courts. Finally, I would like to thank Marília Monteiro, Giovanna Carloni, Walter Britto, and Rebeca Garcia for their invaluable research assistance and comments on this chapter.

Bulk Collection. Fred H. Cate and James X. Dempsey.

II. NATIONAL LEGAL CONTEXT AND FUNDAMENTAL PRINCIPLES

Brazil is a federal republic founded on the rule of law. The Brazilian federal system comprises the Union (federal government), the states and the municipalities. Powers at the federal and the state level are divided among the executive, the legislative and the judiciary, whereas the municipalities have no judiciary.

Although states have general authority to legislate in all matters not assigned to the federal government, the Constitution has enumerated a substantial list of powers preserved for the latter. The federal government has exclusive authority to legislate over civil, commercial, criminal, and procedural law, in addition to telecommunications, broadcasting, and computer issues, among others. On issues such as finance and consumption, both the federal government and the state have concurrent lawmaking authority, but the former has the power to enact general rules, whereas the states can only enact supplementary legislation. If the federal government has not regulated the issues of this second group, the state has full authority until federal legislation is enacted. In short, the competence for virtually all relevant legislation about governmental access to private-sector data belongs to the federal government.

The Brazilian legal regime is based on the civil law tradition, and as such court decisions are not generally binding—unless decided by the Brazilian Supreme Federal Court ("Supremo Tribunal Federal"—STF) following a specific legal procedure. Legal precedent might influence future decisions, but judges are not bound by it. Therefore, cases involving issues not extensively regulated by the law are often subject to contradictory decision by different judges.

In very general terms, the STF has authority to decide on the constitutionality of laws using two main mechanisms: (1) an abstract judicial review—which considers the law in abstract without reference to any particular case; and (2) a concrete constitutional review—which reviews constitutionality for particular cases. Decisions made through the abstract review are binding and any legislation struck down this way is considered to be null for all purposes (*erga omnes*). In the second case, when the STF reviews constitutionality of laws for particular cases, decisions have effect only for the case under analysis and not for future cases. There is no *stare decisis* in Brazil. Despite this, a recent change allowed justices to decide whether to extend binding effect for decisions involving similar recurrent cases.

It is worth noting that the executive branch does not conduct public prosecution functions. Instead, they are carried out by an autonomous body, the Public Prosecutor's Office ("Ministério Público"), which operates at both the federal and state levels. Prosecutors must pass a rigorous public exam to gain admittance. Some constitutional specialists consider the body to be a fourth power in terms of separation of powers, given its independence.[1] The president

1. Alfredo Valladão, Haroldo Valladão, Mário Casasanta and Themístocles Brandão Cavalcanti, *O Ministério Público, Quarto Poder do Estado e Outros Estudos Jurídicos* (Rio de Janeiro: Livraria Freitas Bastos, 1973).

appoints the Prosecutor General and his or her nomination must be approved by the Senate. Both the federal and the state governments are not represented in courts by public prosecutors, but instead this responsibility belongs respectively to the Attorney General of the Union and the State Attorney General. Although public prosecutors are considered to represent and defend diffuse and collective interests of society in general—on cases of murder, for instance—the Attorney General of Union and the State Attorney General represent their respective federative member in courts in cases where that particular entity is involved.

The Brazilian Constitution[2] is quite prolific in enumerating rights and liberties.[3] As an example, article 5, which deals with most of the individual and fundamental rights, contains 78 items, including various more specific rights.[4]

A recent change to the Constitution gave human rights treaties the status of constitutional amendments once they are approved by Congress according to the same procedure governing constitutional amendments proposed in the standard manner. So far only one treaty has been incorporated into the Constitution as an amendment: the Convention on the Rights of Persons with Disabilities.[5]

Brazil has no broad data protection legislation. However, in 2014, Congress passed legislation—called "Marco Civil da Internet"—to regulate basic rights for citizens online, as well as access by law enforcement to data in possession of telecommunications and online providers; it also dealt with data retention, intermediary liability, network neutrality, open government, and other issues.

III. STATUTORY AND REGULATORY OVERVIEW

A. Laws (including Regulations or Other Authorities) Requiring, Explicitly Authorizing, or Restricting Governmental Access to Private-Sector Data and the Implications That Such Laws Have for the Question of Systematic Access

1. Constitutional Provisions

The Brazilian Constitution protects various aspects of privacy rights in several provisions located under the individual rights section of its article 5 as follows: (IV) "the expression of thought is free, and anonymity is forbidden"; (X) "the intimacy, private life, honor and image of persons are inviolable, and

2. http://bd.camara.gov.br/bd/bitstream/handle/bdcamara/1344/constituicao_ingles_3ed.pdf?sequence=7.

3. Marcos Nobre, "Indeterminação e estabilidade: Os 20 anos da Constituição Federal e as tarefas da pesquisa em direito," *Novos Estudos—CEBRAP* v. 82, p. 97–106 (2008).

4. Luiz Costa, *A Brief Analysis of Data Protection Law in Brazil* (June 2012). 28th Plenary meeting of the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data [ETS No. 108] (T-PD), Council of Europe, http://ssrn.com/abstract=2087726.

5. According to information available at http://www.planalto.gov.br/ccivil_03/constituicao/quadro_DEC.htm.

the right to compensation for property or moral damages resulting from their violation is ensured"; (XI) "the home is the inviolable refuge of the individual, and no one may enter therein without the consent of the dweller, except in the event of *flagrante delicto* or disaster, or to give help, or, during the day, by court order"; (XII) "the secrecy of correspondence and of telegraphic, data, and telephone communications is inviolable, except, in the latter case, by court order, in the cases and in the manner prescribed by law for the purposes of criminal investigation or criminal procedural finding of facts"; (LXXII) "habeas data shall be granted: (a) to ensure the knowledge of information related to the person of the petitioner, contained in records or databanks of government agencies or of agencies of a public character; (b) for the correction of data, when the petitioner does not prefer to do so through a confidential process, either judicial or administrative."[6]

Of these items, three are of special interest to understanding governmental access to private-sector data in Brazil: the prohibition of anonymous speech (article 5, item IV), the right to the secrecy of communications (article 5, item XII), and a generic protection to privacy, private life, honor, and image (article 5, item X).

Article 5, item X provides for a general privacy right. According to some decisions from the STF, rights such as the secrecy of financial data, professional secrecy, and several others have been derived from this general privacy clause.[7] The article is often used as a general privacy umbrella when other more specific articles do not provide enough protection.

Unlike in other jurisdictions, anonymous speech is forbidden in Brazil.[8] One of the main consequences of this provision is that courts have ruled that judicial authorization is not required for the police or the Public Prosecutor's Office to have access to subscriber identifying data from companies. This understanding, however, is far from being unanimous and a recent decision at a Federal Court decided exactly in the opposite direction, stating that the privacy provisions of article 5, items X through XII protect a subscriber's identifying information.[9] In a slightly different case, the STF decided that an email provider had to give access to subscriber identifying data when the party requesting that information was part of the communication process.[10] The court found that there was

6. Brazil, *Constitution of the Federative Republic of Brazil*, http://bd.camara.gov.br/bd/handle/bdcamara/1344.

7. Supreme Federal Court. HC 87.654. See also AI 655.298-AgR.

8. In the United States, for instance, the First Amendment protects anonymous speech.

9. Federal Regional Court 4. Embargos Infringentes n. 0033295-12.2006.404.7100/RS, http://www.trf4.jus.br/trf4/processos/visualizar_documento_gedpro.php?local=trf4&documento=4852744&hash=ada05adcfc6834d2f9e5b5d10f66309f.

10. See Brazilian Federal Supreme Court. AI 763133/SP. Justice Cármen Lúcia. March 5, 2012.

no privacy violation in this case, because the communication had been directed at the recipient and therefore he not only already had access to the content of the message, but the prohibition of anonymous speech in the Constitution allowed that party to know the identity of the sender. Given the high level of controversy over this issue in the courts, lobby groups have managed to pass language in what was supposed to be a minor change to the money laundering law that now allows for the police and the Public Prosecutor's Office to have uncontroversial access to a subscriber's identifying information in possession of the electoral courts, Internet service providers, telecommunications companies, financial institutions and credit card companies. This will be covered in more detail below.

Article 5, item XII (see above), on the other hand, protects the secrecy of communications. There are four types of communications listed in the article: correspondence, telegraphy, data, and telephone communications. Although the clause protects them from access by others, there is an exception that allows for communications to be intercepted for the purposes of criminal investigation or criminal procedural findings of fact as long as authorized by the courts. The controversy involving this article lies in whether the expression "except, in the latter case" would refer only to telephone communications, or if it would also apply to data. The doctrine and the courts also diverge as to whether the expression includes the content of the data or only the transmission of such data.[11] The issue was partly resolved by case RE 418.416-8/SC with Justice Sepulveda Pertence writing the majority opinion. The case involved the seizure of computers containing data about fraud on import taxes committed by a company. The computers were seized according to a court order, but the defendant argued that the data was inviolable according to the provision of article 5, item XII. In the opinion, Justice Pertence established a difference between the content of the data and the transmission of data, stating that although the latter was protected the former was not. To be clear, according to this opinion courts can authorize seizure of computers and access the data stored in them. Although his opinion resolved the matter of access to the content of static data stored in computers, it also affirmed that the transmission of data was inviolable, which raised questions as to whether the monitoring of real-time digital communications—even when authorized by the judiciary—would be constitutional. We will come back to this issue when discussing some of the pending issues in item IV.

11. See Tercio Sampaio Ferraz Jr., "Sigilo de dados: o Direito à privacidade e os limites à função fiscalizadora do Estado," *Cadernos de Direito Tributário e Finanças Públicas*, nº 1, RT (São Paulo: 1992), pp. 141–54, http://www.terciosampaioferrazjr.com.br/?q=/publicacoes-cientificas/28. See also Fábio Alceu Mertens, "O sigilo de dados no direito constitucional brasileiro" for an overview of the major doctrinal and judicial positions about the issue. Available at http://jus.com.br/revista/texto/10748/o-sigilo-de-dados-no-direito-constitucional-brasileiro.

2. Statutory Law

a. The Brazilian Civil Code

Brazil does not have a data protection law, so general statutory privacy protections can only be found in the Civil Code—although more detailed protection is provided for specific types of data. The general protections are included in the broader section of personality rights and provide little specification in addition to the constitutional provisions. In this sense, one article is relevant to our analysis: article 21 provides that "the private life of the natural person is inviolable, and the judge, attending the applicant's request, may take the necessary measures to prevent or terminate action contrary to this standard." The article establishes some basic general privacy protections, however, its broad and abstract wording provides little guidance in determining the limits to systematic governmental access to personal data in the private-sector. This is especially true when an individual agreed to terms that allow such practices to take place.

B. Separate Laws That Might Exist for Law Enforcement Access, Regulatory Access, and/or National Security Access (including Distinctions, If Any, between Domestic Intelligence and Foreign Intelligence) and, If Applicable, How These Laws Address Systematic Access

1. Law Enforcement Access

In 2014, Brazil passed legislation to regulate the use of the Internet.[12] The statute known as *Marco Civil da Internet*—from the Portuguese expression to describe an Internet regulatory framework—created rules addressing access by law enforcement to personal data, the content of communications, subscriber identifying information (IP address), and registration data from telecommunications and online providers.

As a general rule, the Marco Civil da Internet requires a court order before law enforcement can get access to personal data, to the content of communications, and to basic subscriber identification data such as IP addresses. When it comes to registration data related to personal qualification, affiliation and address (Art. 10, §3°), the statute simply recognizes that other legislative bodies may grant access to such information without a court order. As we will discuss in Section B(5) below, the Money Laundering Act grants law enforcement with access to this kind of data regardless of court orders.

The law establishes two groups of actors that must retain and make basic information available in order to identify Internet users: (1) "Internet connection providers" and (b) "Internet application providers." The first (1) refer to organizations that offer connection services or access to telecommunication infrastructure. In order to simplify understanding of the regulations we will refer to them as telecommunication providers. The second category (2) refers to organizations

12. See Federal Act 12,965 / 2014.

that offer online services or applications on top of the telecommunication infrastructure; they will be referred to as online providers.

The Marco Civil statute requires both providers to retain certain basic subscriber information that allow for the identification of users. Telecommunication providers must retain for one year records that inform "date and time of the start and end of an Internet connection session, its duration and the IP address used by the [computer] terminal to send and receive data packets." Online providers must retain for six months "information related to the date and time that a certain application was used from a given IP address."

In order to identify a user, first law enforcement is required to request the online provider to inform law enforcement of the IP address used by that individual to access the service on a certain date and time. Once in possession of this information, authorities can go to the telecommunication providers and request them to identify which of their users was assigned to that IP address on that particular date and time.

Law enforcement may request telecommunication and online providers to preserve data for a longer period of time. However, law enforcement will have 60 days to file an application for a judicial order of access to data—if no application is filed during this period, the request becomes ineffective (Art. 13, §§ 2, 3, and 4).

Telecommunication providers are prohibited from storing records of access to applications (Art. 14). According to the legislative debate the intent was to prohibit telecommunication providers from keeping a sort of browsing history obtained from their users. Online providers are prohibited from storing access data regarding other Internet applications, unless previously authorized by the user (Art. 16). Finally the statute also forbids the storage of personal data considered excessive in relation to the purpose that governed the consent originally given (Art. 16). These restrictions combined with the requirement of a court order before the government can have access to personal data help prevent systematic access to private-sector data.

Marco Civil's implementing regulations (Decree 8,771/2016) established further requirements for law enforcement to have access to registration data without court orders. Accordingly, law enforcement is required to inform the specific legal authority that grants access to the registration data, alongside with the motivation for the request (Art. 11). This request must also be specific about the individuals whose data are requested—collective requests that are generic or unspecific are forbidden (Art. 11, §3).

The definition of registration data under the request comprises: affiliation, address, and personal qualification—user's name, marital status, and profession (Art. 11, §2). It also requires law enforcement—or any other authority that may have access to registration data—to publish annual transparency reports including data about the number of requests for registration data (Art. 12).

It is worth noting, though, that when the article on which this chapter is based was finished, both Marco Civil and its regulations had been enacted very recently, so not many parts of the law had been tested by higher courts.

2. Access for Telecommunications Regulatory Enforcement

Since 2010, the Brazilian Communications Agency (ANATEL) has been at the epicenter of what is probably one of the main examples of governmental systematic access to private-sector data in the country. During that year, a major newspaper revealed that the Agency planned to build technical infrastructure and enact regulation to allow it to connect directly into telecom companies' systems[13] and obtain information related to customer's usage of services, such as numbers dialed, time, date, amount paid, and duration of all phone calls made.[14] To be sure, this technical and legal structure would allow ANATEL's officials to have direct and unmediated online access to telecom carriers' system with the alleged purpose of assessing whether companies are providing services with the level of quality that is determined by the Agency.

According to the Agency's general enforcement manager, such access would be necessary to validate information that is provided by telecom companies without any sort of filtering or meddling with the data. Moreover, it would allow the Agency to assess in real time the capacity of the network infrastructure and order its expansion before the situation reaches a critical level. The system has also been justified by the need to modernize the Agency and the limited availability of technicians to inspect all companies.[15]

ANATEL has given assurances that the system will not be used for surveillance. According to the new rules issued by ANATEL, "the data and information accessed and obtained by the Agency pursuant to this Regulation are those directly related to the obligations of the company under supervision and essential to the effective exercise of the supervisory function of ANATEL, making sure that the content of communications between users remains secret."[16] The rule also mandates ANATEL to keep user's personal data secret and establishes both civil and criminal liability for official misconduct.

3. Wiretapping Act

The Wiretapping Act[17] dates back from 1996 and regulates wiretapping of both telephone and digital communications. The statute authorizes eavesdropping

13. See "Anatel terá acesso total a dado sigiloso de telefones," *Folha de São Paulo* (January 19, 2011), http://www1.folha.uol.com.br/mercado/862698-anatel-tera-acesso-total-a-dado-sigiloso-de-telefones.shtml (last visited October 5, 2011).

14. See Ronaldo Lemos, "Brazilian Communications Agency Moves towards Surveillance Superpowers," *Freedom to Tinker* (January 31, 2011). Available at https://freedom-to-tinker.com/blog/rlemos/brazilian-communications-agency-moves-towards-surveillance-superpowers/ (last visited February 4, 2012).

15. "Agência diz que não haverá quebra de sigilo," *Folha de São Paulo* (January 19, 2011), http://www1.folha.uol.com.br/fsp/mercado/me1901201104.htm (last accessed June 22, 2011).

16. See ANATEL, Regulation 596/2012, article 36, http://legislacao.anatel.gov.br/resolucoes/34-2012/308-resolucao-596 (last visited June 23, 2014).

17. Brazilian Federal Act 9296/1996.

on communications only for the purpose of producing evidence to be used in criminal investigations (article 1) and requires that the Court order the procedure. Additionally, wiretapping is not allowed if: (1) there is no reasonable suspicion that the crime has been committed by the person who will be investigated, (2) evidence can be produced through other means available, or (3) if the crime is punishable with "detention"—a less rigorous type of imprisonment.

Interception may be ordered ex officio by the judge or can be requested by either the Public Prosecutor's Office or the police (articles 3 and 4). The statute also requires the request to include a clear description of the purpose of the investigation indicating the subjects who will be placed under surveillance—unless such indication is not feasible—and the means through which the interception will be performed. Eavesdropping may last for 15 days, but the term may be renewed. Courts have allowed for the extension of such term but have not established a maximum time limit for the procedure, as long as the judge supervising it deems it relevant to the investigation.[18]

Wiretapping practices of the Federal Police and the Brazilian Intelligence Agency were the focus of a recent scandal when an agent intercepted calls of a justice from the Brazilian Supreme Federal Court. The scandal led to public scrutiny over current wiretapping procedures and revealed that there was a clear abuse of the practice. The public outcry for more control over wiretapping practices led to the promulgation of a resolution by the National Counsel of Justice in 2008 establishing specific procedures to enhance the secrecy of the interception process and judicial control over them.[19] According to the most recent data made available (related to the entire year of 2016), the judiciary authorized the monitoring of 11,066 email accounts, 18,298 lines using voice over IP, and more than 255,000 telephone lines.[20] Although the rationale behind the judicial authorization is that the courts will protect citizens from abuse, such a high number of interceptions may suggest that when this control is not sufficiently exercised by judges, practical results may be very similar to those of systematic access.

The statute allows for the police to request that telephone companies provide the necessary technical services and personnel to perform the wiretapping. Illegal wiretapping is punishable with imprisonment of two to five years and a fine.

18. See Superior Court of Justice (STJ) HC 110644/RJ. April 16, 2009.

19. The National Counsel of Justice is a body formed by members of the judiciary, the Public Prosecutor's Office, lawyers, and members of civil society tasked with overviewing judicial malpractices and improving the management of the judiciary. For information about the control of wiretapping by the Counsel, see Conselho Nacional de Justiça (CNJ). Resolution 59/2008, as amended by Resolution 217/2016.

20. See Conselho Nacional de Justiça (CNJ), http://www.cnj.jus.br/interceptacoes_tel/relatorio_quantitativos.php (last visited April 15, 2017).

4. Secrecy of Financial Data Act

The secrecy of financial data is protected both by the general privacy provision of article 5, item X of the Constitution (above) and by the Secrecy of Financial Data Act.[21] The statute applies to financial institutions such as banks, credit card companies, securities companies, stock exchanges, credit unions, and many others. The general rule is that financial data can only be obtained with a warrant, when necessary to the investigation of illicit activities. The statute however allows for the Brazilian Revenue Service (BRS) to request and obtain financial information directly from financial institutions regardless of judicial authorization. Although the Act has authorized such access to take place since 2001, it faces increasing opposition in the public opinion and the judiciary. For instance, an article in a major Brazilian newspaper criticized the system, revealing that since the law was enacted, the BRS had requested financial data to be disclosed over eighty thousand times.[22] Despite the critics, recently the STF, judging five actions that called into question provisions of the Secrecy of Financial Data Act, decided that the BRS may request and obtain financial information directly from financial institutions with no need for a judicial order.[23]

Violating the secrecy of financial data is punishable with up to four years in prison and a fine.

5. Amendments to the Money Laundering Act

In 2012, the Money Laundering Act was amended to broaden investigative powers of both the police and the Public Prosecutor's Office. A new article 17-B was included to allow both of them to have access, without a warrant, to a suspect's identifying data in possession of the Electoral Courts, telephone companies, financial institutions, Internet service providers, and credit card companies.[24] Access to subscriber identifying information has been a long-standing demand of the police and the Public Prosecutor's Office.

Members of the Public Prosecutor's Office have been arguing that despite the fact that the provision was included in the Money Laundering Act its effects are not limited to the scope of the statute, but rather apply to all criminal

21. Brazilian Federal Supplementary Act 105/2001.

22. Danilo Fariello, "Leão que Devora Sigilo," *O Globo Economia*, p. 15 (September 4, 2012), http://oglobo.globo.com/economia/leao-que-devora-sigilo-6177901.

23. http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=310670 (last visited March 10, 2016).

24. Brazilian Federal Law 9.613/1998: "Article 17-B. Police authorities and public prosecutors shall have access, exclusively, to registration data of the suspect that disclose personal qualification, father and mother names and address, independently of judicial approval, kept by the Electoral Justice, by phone companies, by financial institutions, by Internet providers and by credit card companies," http://www.planalto.gov.br/ccivil_03/leis/l9613.htm and https://www.eff.org/pages/mapping-laws-government-access-citizens-data-brazil.

investigations.[25] The inclusion of such an overreaching provision in a statute dealing with a subject that is not commonly monitored by digital rights activists suggests that it was part of a strategy meant not to draw attention until the Act had been approved. In the beginning of 2013, the constitutionality of access provision was challenged, but it is yet to be decided whether the STF will hear the case.

6. Intelligence

The Brazilian Intelligence System is a collegiate body responsible for planning and executing intelligence activities in Brazil. It is coordinated by a central agency, the Brazilian Intelligence Agency (ABIN), and composed of governmental institutions such as the Central Bank, the Federal Police, the Revenue Service, and the Ministries of Defence, Foreign Relations, Justice, Environment, and Finance. The Agency reports to the Office of Institutional Security, which in turn reports directly to the president.

The ABIN does not have investigative or surveillance powers, which are reserved to the police.[26] Additionally, the Constitution only authorizes interception of communications for the purpose of investigating crimes, a provision that severely restricts the possibility of these practices being used in intelligence activities. These limitations to the Agency powers can probably be explained by recent history. During the military regime from the 1960s to the 1980s, the National Information Service was responsible for intelligence activities, and as such conducted wiretapping and investigation of several political dissidents and leaders of social movements. The Agency's activities during the military regime still resonate in the public opinion and create substantial political barriers whenever a proposal to expand its powers appears.

In 2008, a scandal revealed the involvement of ABIN's agents in the wiretapping of telephone calls made by a Supreme Court justice.[27] After the scandal, a Presidential Decree expanded even further the possibilities of cooperation between the ABIN and other bodies of the Brazilian Intelligence System—such as the Federal Police—as a way to fix the alleged illegality.[28] Instead of responding to public criticism with stricter rules, the executive did the opposite. The Decree created a Department for the Integration of activities developed by the Brazilian Intelligence System (DIBIS), which was tasked with the coordination and articulation of data flows relevant to intelligence activities. This has

25. Vladimir Aras, "Requisição de dados cadastrais: o segredo de polichinelo," *Blog do Vlad* (July 26, 2012), https://blogdovladimir.wordpress.com/2012/07/26/requisicao-de-dados-cadastrais-o-segredo-de-polichinelo/ (last visited September 8, 2012).

26. Brazil, *Constitution of the Federative Republic of Brazil*. Article 144.

27. See High Court of Justice (STJ). Habeas Corpus n.149.250—SP.

28. See Presidential Decree 6540/2008, which modified Presidential Decree 4376/2002, https://www.planalto.gov.br/ccivil_03/decreto/2002/d4376.htm.

significantly expanded the exchange of information between governmental bodies and created unprecedented integration of the police and the ABIN's databases.[29] When reviewing the case many years later, the High Court of Justice ruled that the participation of intelligence agents in the wiretapping was illegal. However, it is not clear if the decision would be the same in light of the new rules introduced by the aforementioned Presidential Decree.

In short, given (1) that the Brazilian Intelligence Agency does not have investigative powers, (2) that only the police and the Public Prosecutor's Office can investigate and request wiretap of communications, and (3) that such requests have to be authorized by the courts, in principle, intelligence activities do not seem to be a fruitful field for the Brazilian government to gain systematic access to private-sector data.

C. Laws Requiring Broad Reporting of Personal Data (Passenger Records, Financial Data) by Private-Sector Entities, Especially in the National Security and Law Enforcement Contexts and, if Applicable, How These Laws Address Systematic Access

Broad reporting of data in Brazil is usual in the context of financial data. The Secrecy of Financial Information Act creates obligations for financial institutions to report financial transactions exceeding a certain amount (R$5,000 per month for natural persons or approximately $2,500 in 2012 dollars) to the Revenue Service.[30] Data reported must include only the name of the customer and the total amount of the money transacted in a given month. It is forbidden to report information related to the origin or the nature of each individual transaction, but such additional information can be obtained with a warrant.[31]

The Money Laundering Act mandates several organizations—such as banks, stock markets, insurance companies, credit card companies, jewelers, public registries, accountants, and others—to report activities that might indicate the existence of money laundering and related crimes. The information must be reported to the Counsel for the Control of Financial Activities (COAF), a department of the Ministry of Finance responsible for monitoring money-laundering activities in the country.

In November 2012, the Brazilian National Civil Aviation Agency (ANAC) enacted resolution 255/2012 mandating the report of passenger data—comprising Advance Passenger Information[32] and Passenger Name Record—to

29. Ibid. Art. 6-A, § 4.

30. Brazil. Federal Supplementary Act n. 105/2001. Article 5. See also Presidential Decree n. 4489/2002. Article 4.

31. Ibid. Article 5, §2.

32. Advance Passenger Information (API) include information such as: travel document number and type, passenger full name, nationality, date of birth, gender, visa number, seat, residential address, destination, etc. Passenger Name Record (PNR) information comprise

border control authorities.[33] The rules create an electronic system through which air companies will send passenger records to law enforcement authorities before the departure or arrival of flights. The types of data requested and the process of automatic communication to law enforcement appears to have been heavily inspired by regulations in place in the United States. The Brazilian Aviation Agency has defended the new rules on the grounds that law enforcement would be better prepared to act against illicit activities related to drug trafficking and terrorism, and that Brazilian regulations needed to be harmonized with international standards.

D. Laws Permitting or Restricting Private-Sector Entities from Providing Government Officials with Voluntary Broad Access to Data, Whether Pursuant to a Formal Order or as a Result of More Informal and Cooperative Arrangements

There are no specific laws other than the ones aforementioned dealing with the specific issue of voluntary disclosure of data from companies to governmental agencies and law enforcement authorities. To be clear, there is specific legislation determining the secrecy of financial information and communications, but there are exceptions for law enforcement access as long as judicial authorization is granted. Nevertheless, as many companies include in their terms of services provisions allowing the disclosure of information to law enforcement officials without a warrant, voluntary systematic access would be possible.[34]

Since the early 2000s, public prosecutors have been pressing companies to disclose increasingly more information. In this sense, at least two examples are worth noting. First, after the police unveiled a series of cases of child pornography in Orkut—Google's first social network, which became extremely popular in Brazil—Google was forced to sign an agreement giving authorities a direct communication channel with the company allowing officials to request data retention, removal of content, and identification of users. Access in this case does not seem to be direct or even unmediated.

Second, in a recent Federal Court decision, it became clear that the Public Prosecutor's Office had been trying to compel telecom companies to make subscriber identifying data available to law enforcement authorities through

information such as: full name, telefone number, API information, frequente flyer number, reservation number, flight dates, payment type, seat, etc.

33. See Resolution 255/2012 from Agência Nacional de Aviação Civil, http://www.anac.gov.br/assuntos/legislacao/legislacao-1/resolucoes/resolucoes-2012/resolucao-no-255-de-13-11-2012/@@display-file/arquivo_norma/RA2012-0255%20consolidado%20at%C3%A9%20RA2014-328.pdf. For background and discussion about the Resolution see also http://www2.anac.gov.br/transparencia/audiencia/aud22_2012/justificativa.pdf.

34. In this sense, and as an example, see the terms of services of: (1) Mercado Livre, available at http://www.mercadolivre.com.br/seguro_privacidad.html; (2) Terra, http://www.terra.com.br/avisolegal/.

an online electronic system that would give them unmediated access to such information. Despite this attempt, the Federal Court has decided that subscriber identifying information is protected under article 5, items X through XII of the Constitution, and therefore, can only be accessed with a warrant.[35]

E. For Major Categories of Data (Communications Content, Communications Metadata, Subscriber Identifying Data, and Non-communications Transactional or Business Records), the Role of the Courts (When Is Judicial Authorization Required and When Can Data Be Compelled upon Executive or Administrative Authority?)

The following Table 6.1 summarizes the role of the courts in authorizing access to different sorts of data. To avoid repeating what has been addressed on previous sections, please refer to them for more detailed information.

Table 6.1. Type of Authorization Required to Access Different Sorts of Data

Type of Data/Type of authorization needed to have access to it.	**Judicial authorization is required**	**Police or the Public Prosecutor's Office request is sufficient**	**A Regulatory Agency can access the data with the strict purpose of supervising the regulated activity**
Communications content	Yes	No	No
Communications metadata	Yes	No	No
Registration data	No	Yes	Yes
Non-communications Transactional or business records	Yes	Unclear	Yes

F. Standards for Use (e.g., Once the Government Acquires Data, What Rules Govern Its Use and Sharing?), Access, Retention, and/or Destruction

Rules dealing with standards for use, access, retention, and destruction of data by the government are rather scarce and vague. Brazil's Internet bill of rights[36] established rules to govern access of the data by the government, but did not

35. Federal Regional Court 4. Embargos Infringentes n. 0033295-12.2006.404.7100/RS, http://www.trf4.jus.br/trf4/processos/visualizar_documento_gedpro.php?local=trf4&documento=4852744&hash=ada05adcfc6834d2f9e5b5d10f66309f.

36. See Brazil Federal Act 12.965/2014.

establish specific rules concerning how the government should handle such data. As there is no general legislation addressing the issue, only the Wiretapping Act and the Constitution provide some guidance to the courts. In the case of wiretapping, existing provisions related to these standards refer to the physical cautions necessary to handle recordings and transcripts. In this sense: (1) files must be kept secret in a separate court record; (2) recordings that are not used as evidence for the case must be destroyed, and (3) blank envelopes should be used to transport and communicate files.[37] Despite the fact that the Wiretapping Act allows for the interception of digital communications, there are no further provisions regulating how the data should be treated.

The absence of substantial standards for using intercepted communications was a key factor that influenced the International Human Rights Court to rule against Brazil in the case *Aso Escher v. Brasil*.[38] It dealt with illegal wiretapping of the phones of an organization connected to the landless movement in the State of Paraná—the country was condemned for disrespecting due process guarantees (8.1) and for failing to adopt internal measures to give effect to human rights protections, as put forth by the American Convention on Human Rights.

Finally, intelligence statutes allow for information to be shared between the members of the Brazilian Intelligence System, such as from the Central Bank to the Federal Police, the Revenue Service, and several Ministries of State.

G. Cross-Border and Multi-jurisdictional Issues (e.g., under What Circumstances Does the Government Assert Jurisdiction over Data Stored outside Its Borders?)

The Internet bill of rights from 2014 included provisions[39] to try and address the long-debated issue of Internet jurisdiction.[40] The law and these particular provisions were crafted as a strong response to the leaks claiming that the Brazilian president at the time, Dilma Rousseff, had been the target of surveillance by the United States government. Accordingly, article 11 states that "in any operation of collection, storage, retention or processing of personal data or communications conducted by [telecommunication] or [online providers] in which at least one of the aforementioned acts occur in national territory, Brazilian law shall be observed along with the protection of personal data and the secrecy of private records and communications." The statute goes on to apply the provision above to "activities carried out by a legal person established overseas, as long it provides

37. See Wiretapping Act, Federal Act n.9296/1996. See also National Counsel of Justice (CNJ). Resolution 59/2008.

38. *Escher v. Brazil*, Judgement (IACtHR, 20 Nov. 2009), http://www.corteidh.or.cr/docs/casos/articulos/seriec_200_por.pdf.

39. See articles 10 through 12 from Law 12.965 / 2014.

40. See comments in Section B(1) above.

services to Brazilian audiences or at least one member of the same economic group has an establishment in Brazil."

In an attempt to fix a complex jurisdiction issue, the Marco Civil statute caused additional confusion by potentially creating contradictory obligations for global or multinational online providers offering service worldwide and with offices in multiple countries. Even though there is no precedent at the Supreme Court level testing Marco Civil's jurisdiction provision, lower courts have issued diverging decisions.[41] The main issue at stake in these cases involve the interpretation of Marco Civil's jurisdiction clause in accordance with an existing mutual legal assistance treaty (MLAT) in criminal matters between Brazil and the United States.[42] In other words, given that the data controller entities of many multinational online providers are based in the United States, should Brazilian law enforcement rely on the legal process established by international cooperation treaties to request data from online providers, or can they request this data directly from the Brazilian entity that is part of the same economic group? The answer to this question has two practical consequences: (1) the amount of time necessary for law enforcement to have access to the data, and (2) the determination of the law applicable to the case.

Although there is no definitive answer from Brazilian high courts, there are diverging court decisions across the country both interpreting Marco Civil so as to recognize the need to use existing legal assistance treaties, and dismissing such treaties to apply solely the Marco Civil jurisdiction clause. This lack of definition by courts has generated confusion for online providers and has increased the uncertainty of operating in Brazil.

IV. RECENT CONTROVERSIES AND/OR PENDING UNRESOLVED ISSUES CONCERNING SYSTEMATIC GOVERNMENT ACCESS TO PRIVATE-SECTOR DATA

There is still much controversy in the judiciary with regard to the limits of governmental access to private-sector data.

41. Just by means of illustration, the lower court of the state of Rio Grande do Sul has recently decided that the Federal Prosecutor's Office should use the MLAT to request access to private messages exchanged via Facebook—the information would be allegedly included in an investigation on corruption and extortion (see https://jota.info/justica/mpf-deve-obter-por-tratado-dados-de-rede-social-diz-juiz-02122016, last visited May 7, 2017). On the other hand, also as an illustration, the 4th Circuit Federal Court has considered that the MLAT was unnecessary if the company at hand was regularly established in Brazil, having a foreign shareholder (TRF, 8th Panel, Appeal No. 0000310-03.2013.404.0000, June 12, 2013).

42. For more information on the treaty between Brazil and the United States on mutual legal assistance in criminal matters please see https://www.state.gov/documents/organization/106962.pdf.

One of the key issues relates to whether public prosecutors and the police may have access to subscriber identifying data without a warrant.[43] For instance, although a couple of decisions at the Superior Court of Justice[44] (STJ) have found that ISPs can only provide information about its subscribers when authorized by the judiciary,[45] the STF has indicated that such information should not be protected under the prohibition of anonymous speech.[46] As higher courts' decisions do not bind those of lower courts, there are many conflicting interpretations, which makes it hard to establish a uniform position. Should the courts understand that judicial authorization is required, then systematic access such as the one mentioned in Section III(D) above—direct unmediated online access by the public prosecutor's office and the police to identifying data—is likely to be considered illegal.

Wiretapping is also far from being uncontroversial, and the law has been challenged twice before the STF.[47] In one of the cases, the provision allowing for the interception of digital communications was brought to the attention of the court, but it has yet to be decided.[48] There is a clear tension between Justice Pertence's interpretation of the secrecy of communications' constitutional clause and the provision that allows for the interception of digital communications. As mentioned above when we discussed the constitutional protections to data, the Supreme Federal Court has already decided that although data stored on a computer might be obtained with a warrant, Justice Pertence's opinion also affirmed that the *flow of data* was protected under article 5, item XII even against judicially authorized wiretapping.

V. CONCLUDING OBSERVATIONS

There is at least one clear example of systematic governmental access to private-sector data in Brazil: the one established for the purpose of regulatory supervision of telecommunication companies.

43. See note 31.

44. The Superior Court of Justice is a high instance of the Brazilian judiciary responsible for deciding cases involving divergence of interpretation of federal legislation. For more information see http://www.stj.gov.br.

45. See Superior Court of Justice (STJ) AI 1.203.054/SP. See also Superior Court of Justice (STJ) REsp 1.068.904/RS.

46. See Section III(A)1. above and note 9.

47. See ADI 4112, http://www.stf.jus.br/portal/processo/verProcessoAndamento.asp?incidente=2630565.

48. See Brazilian Supreme Federal Court (STF) ADI 1488.

The approval of the Marco Civil da Internet in 2004 made it harder for the government to have access to private-sector data without court orders or in systematic form. Although the statute still left many unresolved issues to be interpreted by the courts, there are clear improvements when it comes to the protection of citizens from government access to their data or that of private organizations. These very interpretative gaps left to the courts may prove, however, to create uncertainty and increase costs for organizations to operate in Brazil.

7

Systematic Government Access to Private-Sector Data in Canada

JANE BAILEY AND SARA SHAYAN

I. INTRODUCTION

In Canada, information privacy is implicitly constitutionally protected by the Charter of Rights and Freedoms (Charter), as well as by provincial, territorial, and federal privacy statutes that regulate the collection, use, retention, and disclosure of personal information.[1] The Privacy Act regulates federal government institutions' relationship with personal information,[2] whereas private sector organizations' relationship with personal information is regulated by the federal Personal Information and Protection of Electronic Documents Act (PIPEDA) or by any substantially similar legislation promulgated in the province in which the private entity operates.[3] These protections, however, are subject to numerous exceptions that allow, and even encourage, information sharing between government entities and between private-sector and state entities.

Statutes enabling law enforcement access to personal information generally require prior authorization, subject to numerous exceptions. Domestic law enforcement agencies obtain prior authorization under the Criminal Code (Code),[4] whereas Canada's primary national security intelligence gathering agencies—the Communications Security Establishment (CSE)[5] and the Canadian Security Intelligence Service (CSIS)—are subject to more relaxed provisions in their respective enabling statutes. National security concerns in relation to

1. Canadian Charter of Rights and Freedoms, being Part I of the Constitution Act 1982.

2. Privacy Act, RSC 1985, c. P-21.

3. Personal Information and Protection of Electronics Documents Act, SC 2000, c. 5.

4. Criminal Code of Canada, RSC 1985, c. C-46, as amended.

5. The Communications Security Establishment (CSE) is sometimes also referred to as the Communications Security Establishment of Canada (CSEC).

Bulk Collection. Fred H. Cate and James X. Dempsey.

large financial transactions and air travel have also led to laws requiring certain private-sector entities to gather and disclose personal information about their clients to government agencies. Canadian law enforcement agents' access to data outside of the jurisdiction generally arises from formal and informal networks, and from requests for assistance from partners under Mutual Legal Assistance Treaties (MLATs).

Although the CSE's capacity to intentionally surveil communications in Canada without ministerial authorization is limited, the agency continuously surveils foreign signals intelligence in cooperation with other signatories to the UK-USA Security Agreement (popularly known as the "Five Eyes"). The Snowden disclosures revealed substantial cooperation between the CSE and its international intelligence partners, with leaked documents showing that the CSE tracked travelers using wi-fi in a Canadian airport, participated in extensive surveillance operations in Brazil and Mexico, surveilled millions of Internet downloads, and helped to set up numerous international spy posts for the United States' National Security Agency.[6]

The Privacy Commissioner of Canada (PCC) and his or her provincial and territorial counterparts play an active role in informing Canadians about information privacy issues, including transborder flows of Canadians' personal information. All privacy commissioners have taken an active role in public debate relating to law enforcement demands for greater access to data and greater secrecy in investigation. The recently-passed Protecting Canadians from Online Crime Act (Bill C-13), Protection of Canada from Terrorists Act (Bill C-44), and Anti-Terrorism Act, 2015 (Bill C-51) have made it easier for state actors to obtain and share information about Canadians domestically and abroad, resulting in what the current PCC has called "a sea change for privacy rights in Canada."[7]

6. Greg Weston, Glenn Greenwald, and Ryan Gallagher, "CSEC Used Airport Wi-Fi to Track Canadian Travellers: Edward Snowden Documents," *CBC News* (January 30, 2014), http://www.cbc.ca/news/politics/csec-used-airport-wi-fi-to-track-canadian-travellers-edward-snowden-documents-1.2517881; Greg Weston, Glenn Greenwald, and Ryan Gallagher, "Snowden Document Shows Canada Set Up Spy Posts for NSA," *CBC News* (December 9, 2013), http://www.cbc.ca/news/politics/snowden-document-shows-canada-set-up-spy-posts-for-nsa-1.2456886; The Associated Press, "Canadian Spies Targeted Brazil's Mines Ministry: Report" (October 7, 2013), http://www.cbc.ca/news/canadian-spies-targeted-brazil-s-mines-ministry-report-1.1927975; Amber Hildebrandt, "CSE Spying in Mexico: Espionage Aimed at Friends 'Never Looks Good,'" *CBC News* (March 25, 2015), http://www.cbc.ca/news/canada/cse-spying-in-mexico-espionage-aimed-at-friends-never-looks-good-1.3005887; Amber Hildebrandt, Michael Pereira, and Dave Seglins, "CSE Tracks Millions of Downloads Daily: Snowden Documents," *CBC News* (January 27, 2015), http://www.cbc.ca/news/canada/cse-tracks-millions-of-downloads-daily-snowden-documents-1.2930120.

7. Privacy Commissioner of Canada, *2014–2015 Privacy Act Annual Report to Parliament: Protecting Personal Information and Public Trust* (December 2015) at 15, https://www.priv.gc.ca/information/ar/201415/201415_pa_e.asp; see Protecting Canadians from Online Crime

Public debate surrounding the Snowden disclosures and controversial national security legislation enacted in subsequent years has highlighted the need for improved oversight and accountability mechanisms. The National Security and Intelligence Committee of Parliamentarians Act (Bill C-22) would, if enacted, address some of these concerns by creating a new committee of parliamentarians with the authority to review national security and intelligence issues across federal departments, subject to some exceptions.[8]

II. NATIONAL LEGAL CONTEXT AND FUNDAMENTAL PRINCIPLES

Canada is a parliamentary democracy founded on the rule of law. Canada's Constitution Act specifies the heads of power of the federal and provincial/territorial governments, whereas the Charter guarantees enumerated rights and freedoms applicable against all levels of government.[9] Any law inconsistent with the Constitution is of no force or effect. Information privacy has constitutional status in Canada, not through explicit Charter guarantees, but as a result of the interpretation of guarantees relating to the right against unreasonable search and seizure (s. 8) and, to a lesser extent, to life, liberty, and security of the person (s. 7).[10]

Provincial/territorial and federal privacy commissioners also play a role in the protection of personal information and data privacy, with oversight powers relating in some cases both to private sector and government operations. Although they tend to have only limited direct enforcement powers, privacy commissioners play an important role in raising public awareness about privacy rights and data security. The limited enforcement powers of the PCC is one issue that, at the time of writing, is under consideration by The House of Commons' Standing Committee on Access to Information, Privacy and Ethics as it conducts a review of PIPEDA.

Act, SC 2014, c. 31; Protection of Canada from Terrorists Act, SC 2015, c. 9; Anti-terrorism Act, 2015, SC 2015, c. 20.

8. Bill C-22, *An Act to establish the National Security and Intelligence Committee of Parliamentarians and to make consequential amendments to certain Acts,* 1st Sess, 42nd Parl, 2016 (passed by the House of Commons, April 4, 2017 and passed second reading and referred to committee by Senate on May 30, 2017).

9. The Constitution Act, 1982, being Sched. B. to the Canada Act 1982 (UK), c. 11.

10. Notable exceptions in which privacy has been examined outside the § 8 criminal context include § 7 challenges mounted against provincial laws relating to the confidentiality of sperm donor and adoption records: *Pratten v. BC (AG)* 2011 BCSC 656; *Cheskes v. Ontario (Attorney General)*, 2007 CanLII 38387 (ON SC).

III. CONSTITUTIONAL, STATUTORY, AND REGULATORY OVERVIEW

A. Constitutional Law

The Canadian Charter of Rights and Freedoms protects "reasonable" expectations of privacy, with reasonableness determined on a "normative rather than descriptive" standard.[11] As a result, the growth and prevalence of surveillance technologies should not *per se* diminish the objective reasonableness of an expectation of privacy.

Section 8 rights are only triggered in relation to information if an individual subjectively expected his or her information to be kept private, and if that subjective expectation was reasonable. The reasonableness of an expectation of privacy depends upon an analysis of the "totality of the circumstances" in which an alleged search or seizure takes place.[12] "Core biographical information" that reveals "intimate details" about a person's lifestyle and individual choices is one kind of information that definitely attracts a reasonable expectation of privacy.[13] Where a reasonable expectation of privacy is found to exist in relation to information, authorities generally cannot obtain that information without prior authorization. The Supreme Court of Canada (SCC) has recognized a reasonable expectation of privacy in, inter alia, personal computers; work-issued computers; cellular phones, regardless of whether they are password-protected; and Internet Service Provider (ISP) subscriber data, but no reasonable expectation of privacy in patterns of heat emanating from a home, or patterns of electricity use measured by a digital recording ammeter.[14] In 2016, a provincial court affirmed a reasonable expectation of privacy in cell phone records, and held that a "tower dump" production order implicating more than 30,000 mobile phone users was overly broad and clearly violated section 8.[15]

As emerging surveillance technologies increasingly permit collection of new types of information or bits of data that were previously inaccessible, Canadian courts have struggled with the question of whether the bits themselves must constitute "core biographical information" in order to trigger section 8 protection, or whether section 8 can be triggered where these bits may combine with other information to facilitate an inference about intimate lifestyle choices. Despite differences of opinion in lower courts, the SCC held in 2014 that Canadians have

11. *R. v. Tessling*, [2004] 3 SCR 432, at 42.

12. *R. v. M. (M.R.)*, [1998] 3 S.C.R. 393, at 286.

13. *R. v. Gomboc,* 2010 SCC, at 28.

14. *R. v. Morelli,* 2010 SCC 8, at 2–3 (personal computers); *R. v. Cole*, 2012 SCC 53, at 59 (work-related computers); *R. v. Fearon*, 2014 SCC 77, at 53 (cell phones); *R. v. Spencer*, 2014 SCC 43, at 66 (ISP subscriber data); *Tessling*, above note 11, at 63 (heat patterns); *Gomboc*, above note 13, at 1 (electricity usage).

15. *R. v. Rogers Communications*, 2016 ONSC 70.

a reasonable expectation of privacy in ISP subscriber information. Section 8 accordingly protects the "link between [an] identified individual and personal information provided anonymously," and extends to overlapping understandings of privacy as secrecy, control, and anonymity.[16]

Information held by a third party with no obligation to maintain confidentiality in relation to it may not be subject to a reasonable expectation of privacy. The SCC has concluded that, although not determinative, contractual waivers of confidentiality may be a factor in assessing the reasonableness of any claimed expectation of privacy in relation to data disclosed by private-sector entities to police.[17]

Searches and seizures without prior authorization may pass constitutional muster if a reasonable law permitted the search and the authorities conducted themselves reasonably.[18] For example, a cell phone search incident to a lawful arrest will not violate section 8 if the search is sufficiently tailored, and if police take detailed notes of what they searched and why.[19] Statutory provisions allowing for voluntary compliance with police requests for disclosure of particular data (such as the one in PIPEDA, discussed below) or mandatory reporting to state agencies (such as those relating to financing of terrorist organizations discussed below in Section III(D)) may also be constitutionally permissible without prior authorization, so long as they are properly tailored to minimize intrusions on privacy (e.g., to apply only in exigent circumstances and/or in circumstances where there are reasonable and probable grounds to believe an offense is being committed in the place to be searched). Bill C-13, which came into force in March 2015, amended the Criminal Code such that any person who voluntarily provides requested information to a public official without a warrant or production order will not incur any civil or criminal liability for doing so (s. 487.0195(2)).

Canadian courts tend to strain against indiscriminate surveillance premised on a "generalized suspicion" even in relation to public spaces and communications facilities (with notable exceptions in relation to airports, border crossings, and intelligence gathering for national security purposes).[20] Even in the context of terrorism investigations, courts have sought to protect the privacy interests

16. *Spencer*, above note 14, at 42, 38.

17. *Gomboc*, above note 13.

18. *R. v. Collins*, [1987] 1 SCR 265.

19. *Fearon*, above note 14.

20. *R. v. Thompson*, [1990] 2 SCR 1111 (public spaces and communications facilities); *R. v. AM,* [2008] 1 SCR 569 (border crossings); Ian Kerr, "Searching for the Right Balance", (May 1, 2008), *Ian Kerr* (blog) (border crossings), http://iankerr.ca/content/2008/05/05/searching-for-the-right-balance/; Re Canadian Security Intelligence Service Act, 2008 FC 301 (CanLII) (national security intelligence); *Re X*, [2010] 1 FCR 460 (national security intelligence).

of unrelated third parties by including minimization provisions in intercept authorization orders.[21]

B. Statutory Law

The privacy of personal information is also protected in federal and provincial/territorial legislation. Government collection, use, retention, and disclosure of personal information is regulated by applicable legislation in each province and territory, and through the Privacy Act at the federal level. For private sector organizations involved in commercial activity, the collection, use, retention, and disclosure of personal information is regulated by the federal PIPEDA, unless the organization is statutorily exempted or the organization operates in a province or territory with legislation declared substantially similar to the federal legislation.[22] In the latter case, the organization's information practices would be governed by the relevant, substantially similar provincial or territorial legislation.[23]

Both the Privacy Act and PIPEDA have been recognized as fundamental laws of Canada and therefore enjoy quasi-constitutional status on the basis that protection of privacy is an essential component of a democracy.[24] For similar reasons, although most privacy commissioners' authority is limited by comparison with their European counterparts, their reports and submissions play an important role in developments relating to the Canadian information privacy framework.

1. The *Privacy Act*—Regulation of Federal Government Institutions

The purposes of the Privacy Act, which came into effect in 1983, are twofold: (1) to protect personal information[25] held by federal government institutions,

21. *R. v. Ansari,* 2010 ONSC 1316, at 31–32.

22. Whether PIPEDA is ultra vires Parliament's powers under § 91 of the Constitution Act has been challenged, but not determined. *State Farm Mutual Automobile Insurance Company v. Privacy Commissioner of Canada*, 2010 FC 736 (CanLII).

23. In this regard, British Columbia, Alberta, and Quebec have laws recognized as substantially similar to PIPEDA, and Ontario has enacted laws relating to health information that are also recognized as substantially similar. Canada has 10 provinces and 3 territories. Given space constraints and the fact that PIPEDA or statutes substantially similar to PIPEDA regulate privacy protection in private-sector entities, this chapter focuses on the federal legislation.

24. *Eastmond v. Canadian Pacific Railway*, 2004 FC 852; *Lavigne v. Canada (Office of the Commissioner of Official Languages),* 2002 SCC 53 (CanLII).

25. Personal information includes inter alia information relating to race, age, religion, marital status, education, address, and fingerprints relating to an individual; views or opinions of another about an individual; and the individual's name where it appears with other personal information relating to that individual: Privacy Act, § 3.

including the Royal Canadian Mounted Police (RCMP), CSIS, and CSE; and (2) to provide individuals with a right of access to their information (s. 2). The Privacy Act regulates federal government institutions' collection, use, retention, and disclosure of personal information as follows:

- *collection*—of personal information only if it "relates directly to an operating programme or activity of the institution" (s. 4) and generally is to be collected from the individual directly (s. 5(1));
- *retention*—for a period of time (that may be prescribed by regulation or set out in institutional policies) that would ensure the individual to whom it relates "has a reasonable opportunity to obtain access" to it (s. 6(1));
- *disposal*—in accordance with regulations, directives, or guidelines of the minister designated in relation to that federal institution (s. 6(3)), with "federal institutions [being] required to develop retention and disposal schedules to manage their records"[26] (although they do not always do so[27]);
- *use*—limited to the original purpose for obtaining the information, or a use consistent with that purpose, or a purpose for which the information was disclosed to the institution by another institution (s. 7); and
- *disclosure*—from one federal institution to another is prohibited, except for a long list of exceptions including disclosure to designated investigative bodies for purposes of enforcing Canadian or provincial laws or pursuant to arrangements or agreements with other institutions, governments of foreign states, etc. for purposes of administering or enforcing laws or carrying out investigations (s. 8(2)).

The PCC is appointed under the Privacy Act and is empowered to investigate complaints and make recommendations (ss. 34–35) as well as to periodically audit government handling of personal information (s. 37).

2. PIPEDA—Regulation of Private Sector Organizations

PIPEDA was enacted in 2000 for the stated purpose of promoting "electronic commerce by protecting personal information[28] that is collected, used or

26. Privacy Commissioner of Canada, *Privacy and Aviation Security: An Examination of the Air Transport Security Authority, Final Report* (2011), http://www.priv.gc.ca/information/pub/ar-vr/ar-vr_catsa_2011_e.pdf.

27. Privacy Commissioner of Canada, *Audit of Selected RCMP Operational Databases Final Report* (2011), http://www.priv.gc.ca/information/pub/ar-vr/ar-vr_rcmp_2011_e.cfm. [hereinafter PCC *RCMP*].

28. Personal information "means information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization." PIPEDA, § 2.

disclosed in certain circumstances by providing for the use of electronic means to communicate or record information or transactions" (s. 3). PIPEDA applies to every organization in relation to personal information that it "collects, uses or discloses in the course of commercial activities" or is about an employee of a federal work, undertaking, or business. It expressly does not apply to any government institution governed by the Privacy Act (s. 4(2)). All organizations governed by PIPEDA must comply with a list of obligations set out in Schedule 1 of the Act, which sets out the Model Code for the Protection of Personal Information. The Model Code requires compliance with 10 fair information practices relating to accountability, identifying purposes, consent, limiting collection, limiting use, disclosure and retention, accuracy, safeguards, openness, and individual access (Schedule 1). As noted above, at the time of writing, the House of Commons Standing Committee on Access to Information, Privacy and Ethics was holding hearings as part of its review of the data protection provisions of PIPEDA, which s. 29 of the Act requires to be conducted every five years. Eventually, this review could yield future amendments to the Act.

Generally, under PIPEDA, private sector organizations that handle personal information must obtain consent from individuals before collecting, using, or disclosing personal information, and must limit collection, use, and disclosure to predefined purposes. Personal information can only be retained as long as necessary to fulfill the purpose for which it was originally collected. However, these restrictions are subject to numerous exceptions. For example, consent to collection, use, and disclosure is not required where "inappropriate" because, inter alia, the information is being collected for law enforcement purposes and seeking consent might defeat the purposes of that investigation. Likewise, personal information may be used or disclosed for purposes other than its original purposes if required by law. Further, an individual's right to access information about the existence, use, and disclosure of personal information may be limited for legal or security reasons. These exceptions to the general fair information practice rules outlined in the Model Code are reflected in certain exceptions within the body of PIPEDA itself.

PIPEDA section 7 allows private sector organizations to collect, use, and disclose personal information about an individual without his or her knowledge or consent in a variety of circumstances (s. 7(1), 7(2), 7(3)), including for purposes relating to law enforcement. Although the frequency with which these exceptions are used is not consistently publicly reported, the most prominent provision publicly discussed is section 7(3), which allows private organizations to, inter alia, disclose personal information without knowledge or consent where disclosure is made to a government institution that has requested the information, identified its lawful authority to obtain the information, and indicated that it suspects the information relates to national security; enforcement of a Canadian, provincial, or foreign law; or is requested for purposes of administering a Canadian or provincial law. Private-sector organizations may also voluntarily collect personal information without notice or consent for similar kinds of purposes. Individuals' general rights relating to disclosure of how private

organizations are dealing with their personal information under PIPEDA are also subject to exceptions, including with respect to disclosures made under section 7(3). In these situations, the government must be notified of the request and may effectively veto disclosure to the individual of even the fact that the individual's personal information was disclosed to government (ss. 8 and 9).

The PCC is empowered to investigate individual complaints lodged under PIPEDA and to issue reports and recommendations for corrective action in relation to them (ss. 12 and 13). Although the recommendations themselves are not legally enforceable, courts can be called upon to review the PCC's decisions and to issue orders. The PCC may also conduct audits and promote the purposes of the *Act* through information programs and public research, and is empowered to share information with other commissioners (s. 24).[29]

C. Specific Laws for Law Enforcement Access, Regulatory Access, and/or National Security Access

1. Basic Organizational Concepts and the Antiterrorism File

In 2003, the federal government created a department focused on issues relating to national security, which since 2006 has been called Public Safety Canada (PSC). PSC reports to the Minister of Public Safety (MPS) and was created to "ensure coordination across all federal departments and agencies responsible for national security and the safety of Canadians."[30] In February 2012, the MPS unveiled Canada's first comprehensive counterterrorism strategy, setting as its first priority to "counter domestic and international terrorism in order to protect Canada, Canadians, and Canadian interests."[31] One component of the strategy is to detect terrorists, terrorist organizations, and their supporters through investigation, intelligence operations, and analysis, which the PSC notes will require "extensive collaboration and information sharing with domestic and international partners."[32]

The strategy identifies three primary federal government intelligence collection organizations: CSIS, the CSE, and the RCMP. Other federal agencies, including the Department of National Defence (DND), the Department of Foreign Affairs and International Trade, the Canada Border Services Agency (CBSA), Transport Canada, and the Financial Transactions and Reports Analysis Centre (FINTRAC) are also to be involved in information collection "in support of

29. Provincial and territorial privacy commissioners also have investigatory, audit, and educative functions in relation to violations of their respective pieces of legislation. Virtually all, however, have noted that a lack of resources undermines their capacity in these areas.

30. Public Safety Canada, *About Public Safety Canada* (November 27, 2015), http://www.publicsafety.gc.ca/cnt/bt/index-eng.aspx.

31. Public Safety Canada, *Building Resilience against Terrorism: Canada's Counter-Terrorism Strategy* (2011), http://www.publicsafety.gc.ca/prg/ns/_fl/2012-cts-eng.pdf.

32. Ibid.

their primary responsibilities," which assist with developing "a broader counter-terrorism intelligence picture."[33] A key priority of the strategy appears to be ensuring information exchange between and amongst these domestic players, as well as with similar agencies acting for international partners. Since the 2015 enactment of Bill C-51, over a hundred government departments are authorized to share information for national security purposes, facilitating investigation into "activities that undermine the security of Canada."[34]

2. Domestic Law Enforcement and the General Requirement for Prior Authorization

Canada has federal, provincial, and municipal law enforcement agencies. The RCMP is the federal law enforcement agency, and is also intimately involved in the terrorism file. Domestic law enforcement agencies' search and seizure powers are generally constrained by the need for prior judicial authorization, subject to exceptions such as those outlined below.

Under Code section 184, willful interception of "private communication"[35] is a crime, except in specific circumstances. For example, the general prohibition on interception does not apply to, inter alia, interceptions with prior judicial authorization (s. 184(2)), or non-pre-authorized interceptions made by a peace officer in certain urgent situations involving imminent unlawful acts that there are reasonable grounds to believe "would cause serious harm to any person or property" (s. 184.4). Generally, prior authorization is only to be granted where a number of criteria are met, including that alternative methods of investigation have been tried and failed, or are unlikely to succeed, or are impractical because of urgency (s. 185). However, the alternative methods criteria is not required to be satisfied for offenses involving a criminal organization or terrorism (s. 185(1.1)). Judicial authorizations must be specific with regard to the type of private communication intercepted, and must include any other terms necessary to protect the public interest (s. 186(4)). Targets of interception must generally be notified within 90 days of the order, although there are provisions that allow for extensions of this time period, particularly in relation to terrorism offenses.

Following passage of Bill C-13, a judge issuing an interception order can also issue "a search warrant, a general warrant, make a general production order, make a specific production order to obtain certain information (such as computer data

33. Ibid.

34. Security of Canada Information Sharing Act, SC 2015, c. 20, § 2, § 5(1).

35. A "private communication" is "any oral communication, or any telecommunication, that is made by an originator who is in Canada or is intended by the originator to be received by a person who is in Canada and that is made under circumstances in which it is reasonable for the originator to expect that it will not be intercepted by any person other than the person intended by the originator to receive it, and includes any radio-based telephone communication that is treated electronically or otherwise for the purpose of preventing intelligible reception by any person other than the person intended by the originator to receive it." Code, § 183.

or financial information), make an assistance order or issue a warrant to use a tracking device or a 'transmission data recorder.'"[36] As a result, law enforcement agencies are now authorized to make a demand or obtain a court order to preserve electronic evidence if they have reasonable grounds to *suspect*, among other things, that an offense under Canadian or foreign law has been committed (s. 487.012) and courts can make ex parte preservation and production orders to trace a specified communication, to obtain transmission data, to obtain tracking data, and to obtain financial data when requested on similar grounds (s. 487.013; 487.015; 487.016; 487.017; 487.018). Judges issuing these kinds of preservation and production orders are also authorized to issue orders prohibiting disclosure of their existence or content in certain circumstances (s. 487.0191). Judges may also issue warrants to obtain transmission data in real time and to permit remote activation of tracking devices in certain types of technologies (s. 492.1; 492.2).[37] Finally, although C-13 amendments state that preservation demands, preservation orders, and production orders are not necessary in order for law enforcement officers to ask a person to preserve or produce a document (s. 487.0195), this provision must be read in light of the *Spencer* decision, which requires prior authorization.

One area that had been controversial is whether certain forms of digital communications ought to be treated as "private communication" and therefore subject to the prior authorization regime for interception rather than the regular warrant provisions relating to searches of persons, places, or things. The regular warrant provisions are arguably easier to satisfy than the intercept authorization provisions, as the former do not require the issuing justice to be satisfied that there are no reasonable alternative investigative methods (s. 487).[38] In 2013, the SCC held that law enforcement officials must obtain prior authorization under the interception regime before accessing text messages held by telecommunications providers, noting that text messages are private communications, and that "[t]echnical differences inherent in new technology should not determine the scope of protection afforded to private communications."[39] The SCC also recently held that law enforcement officials must obtain a separate warrant before searching the contents of a computer (although officers may, under the general warrant regime, seize a computer and take measures to preserve its data until a separate search warrant is issued).[40]

36. Julia Nicol & Dominique Valiquet, *Legislative Summary of Bill C-13: An Act to amend the Criminal Code, the Canada Evidence Act, the Competition Act and the Mutual Legal Assistance in Criminal Matters Act* (Dec. 11, 2013), http://www.lop.parl.gc.ca/About/Parliament/LegislativeSummaries/bills_ls.asp?ls=C13&Parl=41&Ses=2#a27.

37. Ibid.

38. Craig Forcese, *National Security Law: Canadian Practice in International Perspective* (2008), at 451.

39. *R. v. Telus Communications,* 2013 SCC 16, at 5.

40. *R. v. Vu*, 2013 SCC 60.

Under section 195 of the *Code*, the MPS must produce an annual report on electronic surveillance in Canada, describing, inter alia, the number of pre-authorization applications made and granted, the average time for which authorizations are issued, the types of offenses investigated using electronic surveillance, and the general methods of interception used. In 2015, PSC reported 67 applications for authorization (44 pursuant to ss. 185, 22 pursuant to section 487.01, and 1 renewal pursuant to s. 186), all of which were granted.[41]

3. Intelligence Agencies

Under PSC's counterterrorism strategy, three agencies are primarily tasked with intelligence gathering functions relating to national security: CSE, CSIS, and the RCMP.

CSE is housed under the DND, which is responsible for Canadian military operations. Under provisions added to the National Defence Act (NDA) with the passage of the Anti-terrorism Act in 2001, CSE is authorized to: (1) collect foreign signals intelligence, (2) assist with protection of Canada's information infrastructures, and (3) provide technical and operational assistance to federal law enforcement and security agencies.[42] However, section 273.64(2)(a) of the NDA limits CSE's mandates under (1) and (2) by prohibiting it from directing its activities at Canadian citizens, permanent residents, or corporations wherever they are, or at anyone in Canada regardless of nationality. Where one-end Canadian communications are unintentionally intercepted, CSE is only permitted to retain them if it is "essential to either international affairs, defence or security, or to identify, isolate or prevent harm to Government computer systems or networks."[43]

However, the Minister of National Defence (MND) may authorize CSE to intercept private communications if satisfied that certain criteria are met (e.g., where interception is necessary to CSE's foreign intelligence mandate) (s. 273.65 *NDA*). As a result, unlike domestic law enforcement agencies, CSE need not seek prior *judicial* authorization to intercept private communication of Canadians, and the ministerial authorizations it obtains last longer than intercept authorizations under the Code and need never be disclosed to those whose communications were intercepted. Although a former CSE Commissioner opined that the ministerial authorization process is Charter compliant, others argue that judicial oversight is necessary (while recognizing that this weaker form of authorization may be found justifiable under the Charter on the basis of "national security").[44]

41. Public Safety Canada, *2015 Annual Report on the Use of Electronic Surveillance*, at 5 (2015), https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/lctrnc-srvllnc-2015/lctrnc-srvllnc-2015-en.pdf.

42. Communications Security Establishment Commissioner, *Annual Report 2010–2011*, at 3, https://www.ocsec-bccst.gc.ca/s21/s46/s16/eng/2010-2011-annual-report.

43. Ibid., at 4.

44. Forcese, above note 38, at 456–58.

In performing its mandate (3), CSE's powers are limited in the same ways as those of the agencies it is assisting.[45] CSE's operations are subject to review by the CSE Commissioner.

CSE gathers foreign intelligence through its participation in the SIGINT network operated by Australia, Canada, New Zealand, the UK, and the United States as signatories to the UK-USA Security Agreement. The network, which is popularly referred to as Echelon or "Five Eyes," is reportedly capable of intercepting, inter alia, phone calls and data traffic globally (including emails) through various networks, including the telephone network.[46] Documents leaked by Edward Snowden confirm and expand upon these reports, describing CSE metadata collection programs and extensive assistance afforded to Five Eyes partners.[47]

CSIS, which lies within the authority of the MPS, was created with passage of the *CSIS Act* in 1984 and is mandated to aid in the protection of national security. In pursuit of its mandate, CSIS collects, analyzes, and retains intelligence relating to activities it has reasonable grounds to suspect threaten the security of Canada, and reports and advises the Canadian government with respect to that intelligence. Its powers are limited to collecting only that which is "strictly necessary" to its mandate, and it must only undertake investigations with "demonstrable grounds for suspicion" of a threat to national security.[48] CSIS's operations are subject to review by the Security Intelligence Review Committee (SIRC).

CSIS has its own warrant provisions under the CSIS Act, which allow it to obtain prior judicial authorization for searches relating to threats to the security of Canada or to permit it to assist the MND or Minister of Foreign Affairs to gather intelligence relating to the capability, intention, or activity of foreign actors. These authorization provisions (which have withstood constitutional scrutiny)[49] allow for orders entitling CSIS to search or seize a variety of materials and places and to "install, maintain or remove any thing" (in relation to interception activities). They may last up to 60 days and never require notification of the target after the search has been completed. Bill C-44, the Protection of Canada from Terrorists Act, amended the CSIS Act in 2015 to explicitly authorize CSIS to perform its duties within or outside Canada (CSIS Act §§ 12(2), 15(2)).

45. CSEC, *Annual Report 2010–2011*, above note 42, at 8.

46. Gerhard Schmid, *Report on the Existence of a Global System for the Interception of Private and Commercial Communications (ECHELON interception system)* (European Parliament: Temporary Committee on the ECHELON Interception System, July 11, 2001), http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A5-2001-0264+0+DOC+PDF+V0//EN&language=EN.

47. Michael Geist, "Why Watching the Watchers Isn't Enough: Canadian Surveillance Law in the Post-Snowden Era" in Michael Geist, ed, *Law, Privacy and Surveillance in Canada in the Post-Snowden Era* (2014) 225–55.

48. Forcese, above note 38, at 84, 457–58.

49. Ibid., at 452.

Further, the Federal Court is now authorized to issue warrants allowing CSIS to conduct activities both within and outside of Canada in order to investigate threats to national security regardless of "any other law, including that of a foreign state" (CSIS Act § 21(3.1)).

The RCMP, in addition to its role as Canada's national police force, is specifically vested with exclusive authority to police national-security related crimes. As a result, despite the creation of CSIS in 1984, the RCMP continues to be involved in intelligence collection relating to crimes involving a "threat to the security of Canada" (which is defined in the CSIS Act).[50]

As intelligence gathering is increasingly centralized through Integrated Security Units (ISUs) for particular events such as the Olympics and G8 meetings, the national security functions of the RCMP and other Canadian police forces have become increasingly intermeshed with those of CSIS. The centralization of antiterror and national security intelligence functions in Canada through ISUs and the Integrated Threat Assessment Centre formed by CSIS in 2007 has been compared to US fusion centers.[51] Others have suggested a need to formally increase the integration of CSE, the RCMP, and FINTRAC in order to better protect critical infrastructure against terrorist attack.[52]

Review of Canada-wide RCMP activities (ranging from "officer rudeness to allegations of the use of unnecessary force") is conducted by the Civilian Review and Complaints Commission for the RCMP.[53] Although the RCMP's national security investigations and investigatory powers have expanded in recent years, there has not been a commensurate increase in resources granted to the Commission. Furthermore, despite strict secrecy legislation, the Commission may be denied access to secret information where the RCMP cites a need to protect operational information and foreign intelligence sources.[54]

4. Regulatory Agencies

Numerous regulatory agencies at the federal and provincial/territorial level are empowered to require disclosure from private sector entities in relation to their mandates. This chapter addresses only the two federal agencies that seem most pertinent: the Canadian Radio-television and Telecommunications Commission (CRTC) and the Competition Bureau.

50. Ibid. at 88.

51. Jeffrey Monaghan & Kevin Walby, "Making up 'Terror Identities': Security Intelligence, Canada's Integrated Threat Assessment Centre and Social Movement Suppression" (2011) *Policing and Society* 1, 3–4.

52. Kosta Rimsa, "Eavesdroppers" in Dwight Hamilton, ed, *Inside Canadian Intelligence*, at 141–42 (2011).

53. Craig Forcese & Kent Roach, *False Security: The Radicalization of Canadian Anti-terrorism*, at 434 (Irwin Law, 2015).

54. Ibid., at 434–35.

The CRTC regulates broadcasting[55] and telecommunications[56] in Canada pursuant to, respectively, the Broadcasting Act (BA) and the Telecommunications Act (TA).[57] The CRTC has largely chosen to forebear from regulating retail mobile and Internet services (including billing, rates, service quality, or ISP business practices) because it has concluded there is sufficient competition in these areas.[58] It has also largely exempted from regulating new media broadcasting undertakings (NMBU) that deliver broadcasting[59] services over the Internet and via P2P technology received over mobile devices.[60] NMBUs are, however, subject to an undue preference prohibition.[61] However, the CRTC does regulate certain aspects of wholesale Internet services, and handles complaints about Internet traffic management practices at both the retail and wholesale level.[62] Complaints about other ISP practices are directed to the Commissioner for Complaints for Telecom Services,[63] whereas complaints regarding Internet content are directed to the Canadian Association of Internet Service Providers for examination under its Code of Conduct or to the appropriate law enforcement agency where illegal content is in issue.[64] The CRTC does, however, monitor and report on broadcasting, telecommunications, and Internet-related developments annually, using survey data obtained

55. "'[B]roadcasting' means any transmission of programmes, whether or not encrypted, by radio waves or other means of telecommunication for reception by the public by means of broadcasting receiving apparatus, but does not include any such transmission of programmes that is made solely for performance or display in a public place." BA, § 2(1).

56. "'[T]elecommunications' means the emission, transmission or reception of intelligence by any wire, cable, radio, optical or other electromagnetic system, or by any similar technical system." *TA*, § 2(1).

57. Broadcasting Act, SC 1991, c. 11, as amended; Telecommunications Act, SC 1993, c. 38, as amended.

58. CRTC, *Internet—Our Role* (June 28, 2016), http://www.crtc.gc.ca/eng/internet/role.htm.

59. Conflicting opinions around whether ISPs qualify as broadcasters under the *BA* and concerns around the ways in which convergence is rendering obsolete distinctions such as telecom and broadcasting have led, respectively, to a CRTC commitment to refer the broadcaster question to the Federal Court and a CRTC call for development of a national digital strategy. CRTC, *Broadcasting Regulatory Policy, CRTC 2009-329* (June 4, 2009)

60. CRTC, *Public Notice CRTC 1999-197* (December 17, 1999), http://www.crtc.gc.ca/eng/archive/1999/pb99-197.htm; CRTC, *Broadcasting Regulatory Policy, CRTC 2009-329* (June 4, 2009).

61. CRTC, *Broadcasting Regulatory Policy*, above note 60.

62. CRTC, *Internet—Our Role*, above note 58.

63. CRTC, *How to Make a Complaint about Your Internet Service* (May 27, 2015), http://www.crtc.gc.ca/eng/internet/plaint.htm.

64. CRTC, *TV and Music Online* (April 2, 2014), http://crtc.gc.ca/eng/internet/musi.htm#internet.

from industry providers.[65] The Telecommunications Act and Broadcasting Act empower the CRTC to issue policies, implement licensing regimes, compel licensees to submit information relating to their operations, and (in relation to hearings it is empowered to hold) compel production and inspection of documents and entry and inspection of property (Broadcasting Act, ss. 9, 10, 16; Telecommunications Act, ss. 55, 58, 67).

In recent years, the CRTC has begun exercising its authority to issue search warrants, in some cases carrying out investigations "in close collaboration with its partners, including the Federal Bureau of Investigation, Europol, Interpol, Microsoft Inc., the Royal Canadian Mounted Police (RCMP), Public Safety Canada and the Canadian Cyber Incident Response Centre."[66] The CRTC successfully carried out a warrant to enter a building associated with an antivirus telemarketing scam in November 2015,[67] and used powers conferred under Canadian anti-spam legislation to take down a command and control server hosting malware one month later.[68]

The Competition Bureau (Bureau) is an independent law enforcement agency responsible for administering and enforcing, inter alia, the Competition Act, including in relation to telecommunications undertakings.[69] It has a variety of powers to compel disclosure of information and its own statutory process to obtain warrants to authorize searches and seizures connected with its mandate domestically. It can also obtain warrants to assist international agencies involved in competition-related matters in respect of which the Mutual Legal Assistance in Criminal Matters Act (MLACMA) applies.[70] The Bureau has also worked closely with domestic law enforcement agencies, such as the RCMP, in relation to mass marketing fraud (including online), as well as identity theft.

D. Laws Requiring Broad Reporting of Personal Data by Private Sector Entities

1. National-Security Related Provisions

A number of federal laws require private-sector entities to report personal data to governmental agencies or statutorily created regulatory bodies, often in relation

65. CRTC, *CRTC Communications Monitoring Report* (2011), http://www.crtc.gc.ca/eng/publications/reports/PolicyMonitoring/2011/cmr2.htm#n0.

66. CRTC, "CRTC Serves Its First-Ever Warrant under CASL in Botnet Takedown" (December 3, 2015), http://news.gc.ca/web/article-en.do?nid=1023419.

67. CRTC, "CRTC Executes First Inspection Warrant as Part of Telemarketing Investigation" (November 27, 2015), http://news.gc.ca/web/article-en.do?nid=1022319.

68. CRTC, "CRTC Serves Its First-Ever Warrant under CASL in Botnet Takedown," above note 66.

69. Competition Act, RSC 1985, c. C-34.

70. Mutual Legal Assistance in Criminal Matters Act, RSC 1985, c. 30 (4th supp.).

to matters of public or national security. Since 2000, in what the PCC characterized as "precedent setting" legislation, certain private-sector entities have been mandated to collect and disclose information to a government agency, without prior authorization for or demonstration of reasonable grounds to compel these acts.[71] The Proceeds of Crime (Money Laundering) and Terrorist Financing Act requires a wide variety of government agencies, individuals, and business entities engaged in what might broadly be described as financial services (e.g., banks, loan and trust companies, casinos, foreign exchange services) to keep and retain records relating to prescribed transactions (e.g., "large cash" transactions in excess of $10,000) and to report these transactions within a specified time period to FINTRAC.[72]

The reports include a variety of personal information, including the name, address, telephone number, and personal identifier of an individual who has conducted a large cash transaction.[73] All of these entities are also required to report to FINTRAC "every financial transaction that occurs or that is attempted in the course of their activities" where there are reasonable grounds to suspect that the transaction related to commission or attempted commission of a money laundering or "terrorist activity financing offence."[74]

Although FINTRAC is at arm's length from law enforcement agencies, it may disclose information it has received to law enforcement officials where it has "reasonable grounds to suspect" the information would be relevant to investigating or prosecuting money laundering or terrorism offenses or a threat to Canadian security.[75] Similarly, financial institutions are required to determine on a continuing basis whether they are "in possession or control of property owned or controlled by or on behalf of" an entity listed in the Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism and to report to

71. Privacy Commissioner of Canada, *Submission to the Standing Committee on Banking, Trade and Commerce re: Bill C-25, An Act to amend the Proceeds of Crime (Money Laundering) and Terrorist Financing Act and the Income Tax Act and to make a consequential amendment to another Act* (December 31, 2006), http://www.priv.gc.ca/parl/2006/sub_061213_e.cfm.

72. Proceeds of Crime (Money Laundering) and Terrorist Financing Act, § 2000, c. 17.

73. FINTRAC, *Guideline 7A: Submitting Large Cash Transaction Reports to FINTRAC Electronically* (December 2016), http://www.fintrac-canafe.gc.ca/publications/guide/guide7A/lctr-eng.asp.

74. "Terrorist activity financing offences" include providing or collecting property for terrorist activities (including offenses implementing various international conventions related to acts such as hostage taking, unlawful acts of violence in airports, terrorist bombings), providing or making available property or services for terrorist purposes, and using or possessing property for terrorist purposes. Code, §§ 83.01, 83.02, 83.03, 83.04.

75. Senate Canada, *Security Freedom and the Complex Terrorist Threat: Positive Steps Ahead, Interim Report of the Special Senate Committee on Anti-terrorism*, at 36 (March 2011), http://www.parl.gc.ca/Content/SEN/Committee/403/anti/rep/rep03mar11-e.pdf.

their respective regulators monthly either that they are or are not in possession or control of such property (*Code* § 83.11).

Concerns relating to terrorism and threats to national security have also led to compelled disclosure of passenger and travel data from commercial carriers under the Passenger Protect Program (which was expanded after the Secure Air Travel Act came into effect following passage of Bill C-51). CBSA operates an advance passenger information (API) and passenger name record (PNR) program pursuant to which it requires commercial airlines to provide it with basic data relating to travelers' names, dates of birth, gender, citizenship, travel document, type of ticket, travel date, and related flight information prior to their arrival in Canada.[76] The CBSA also collects a "limited set" of the PNR data collected by air carriers or their agents relating to all passengers seeking entry into Canada, which includes "basic identity data," contact, payment, and billing information about their booking agent, as well as the traveler's check-in status, seating, and baggage information.[77] CBSA can use PNR to "to identify persons who have or may have committed a terrorism offence or a serious transnational crime [e.g. narcotics smuggling, human trafficking]" or to develop trend analysis or risk indicators for identifying people who have or may commit such offenses or crimes.[78] CBSA maintains API and PNR data in an access-restricted database (PAXIS) for a maximum of six years after receipt (CBSA, Guidelines). CBSA is authorized to disclose PNR to domestic authorities including CSIS, as well as to federal, provincial, and municipal police forces on a case-by-case basis subject to certain conditions. It can also disclose PNR to a foreign government authority on a case-by-case basis, so long as there is an international agreement in place to provide for that disclosure (CBSA, Guidelines). Records of disclosure must be kept and individuals have rights to request access to, request correction of, and to complain to the PCC about the PNR the CBSA holds about them (CBSA, Guidelines).

The MPS maintains a list of people he or she has reasonable grounds to believe will, among other things, threaten transportation security or use air travel to commit a terrorism offense—commonly referred to as the no-fly list.[79] The MPS can direct an air carrier, among other things, not to allow persons on the list to travel by air or require them to screen listed persons.[80] The Ministers of Transport and of Citizenship, the RCMP, CSIS, CBSA, and other persons authorized by regulation can assist the MPS in collecting and disclosing information

76. Canada Border Services Agency, *Guidelines for the Access to, Use, and Disclosure of Advance Passenger Information (API) and Passenger Name Record (PNR) Data, Memorandum D-1-16-3* (May 31, 2016), http://www.cbsa-asfc.gc.ca/publications/dm-md/d1/d1-16-3-eng.html; Secure Air Travel Act, SC 2015, c. 20, § 11, § 5(2).

77. CBSA *Guidelines*, above note 76.

78. Ibid.

79. Secure Air Travel Act, above note 76, § 8(1)

80. Ibid., § 9(1).

and the MPS can also enter into agreements with foreign states to disclose all or part of the list to them.[81] Individuals whose names appear on the list and have been denied travel can apply to the MPS to have their names removed, however, notwithstanding a report in November 2016 that a federal system of redress was under consideration, as of the date of writing no such system was as yet available.[82] Various prohibitions in the Secure Air Travel Act limit the bodies that have access to the list from disclosing it for purposes other than those provided for in the Act.[83]

The Immigration and Refugee Protection Act also authorizes certain officials to request disclosure of passenger information from commercial carriers.[84]

2. Other Kinds of Provisions

A variety of provincial legislation also compels disclosure of personal information, including with respect to public health. For example, the Ontario Health Protection and Promotion Act requires health care practitioners to report to the local public health authority the name, address, date of birth, health card number, gender and telephone number of any person infected or suspected of being infected with a listed communicable disease.[85]

E. Laws Permitting or Restricting Private Sector Entities from Providing Government Officials with Voluntary Broad Access to Data

Privacy laws in various provinces and territories[86] (as well as certain other kinds of legislation[87]) allow private-sector entities to share personal information with government officials in certain situations. Of these, the PIPEDA section 7

81. Ibid., §§ 10, 12.

82. Ibid., § 15(1); Michelle Zilio, "Ottawa Tight-Lipped on Delay to Improving No-Fly List" (April 10, 2017) *The Globe and Mail* http://www.theglobeandmail.com/news/politics/ottawa-tight-lipped-on-delay-to-improving-seriously-deficient-no-fly-list-database/article34662667/.

83. Ibid., §§ 20–21.

84. Forcese, above note 38, at 472.

85. Health Protection and Promotion Act, RSO 1990, c. H.7, § 25.

86. The kinds of situations in which provincial and territorial privacy statutes permit private-sector entities to provide information to public officials includes those where disclosure is required or permitted by law, to minimize imminent health or safety risks, for research or statistical purposes, or "in the public interest." M. Lacroix et al., *The Reporting and Management of Personal Information and Personal Health Information to Control and Combat Infectious Disease: An Analysis of the Canadian Statutory and Regulatory Framework* (March 2004), http://www.phac-aspc.gc.ca/php- psp/pdf/privacy_analysis.pdf.

87. See, for example, § 10(3) of the Code of Conduct Regulation (Alta Reg 160/2003) enacted pursuant to Alberta's Electric Utilities Act, SA 2003, c. E-5.1, which explicitly permits hydro

provisions (discussed above in Section III(B)2) that allow for collection, use, and disclosure for purposes relating to law enforcement have tended to be the most prominent. Media reports, case law, and transparency reports produced by Canadian telecommunications providers suggest that many section 7(3) requests for disclosure seek subscriber information in relation to online child sexual exploitation investigations. Since the *Spencer* ruling in 2014, these requests must be made pursuant to a production order. Examples drawn from case law in which police have relied upon "PIPEDA requests" in order to access subscriber identity indicate that a standard form letter is used, in which the officer identifies that the officer is acting in his or her capacity as a law enforcement officer investigating a child sexual exploitation offense, requests disclosure of the last known customer name and address of the account associated with a specified IP address being used at a specified date and time, and identifies the legislative source from which the officer's authority to make the request derives (typically the constating act and/or regulations for the police force to which that particular officer belongs).

In its 2015 Transparency Report, Rogers Communications indicated that it complied with 83,871 requests for disclosure by law enforcement agencies, or 97 percent of requests made that year.[88] Telus Communications similarly received 57,167 requests in 2015,[89] while Canada's largest telecommunications provider, Bell, has yet to release any transparency reports.[90] Prior to the SCC's *Spencer* ruling in 2014, state access to ISP subscriber data required only five minutes of paperwork, with documents released through access to information requests suggesting that some telecommunications providers may have created law enforcement databases to make subscriber data readily accessible to state officials.[91]

providers to disclose personal information about their customers to a peace officer for the purpose of investigating an offense, unless disclosure is contrary to an express request by the customer. In *Gomboc*, a majority of the SCC concluded that the defendant's failure to specify that he wished his information to be kept confidential when granted the option to do so, made it possible for the hydro authority to voluntarily disclose that information to the police. However, the Court left to another day the question of whether the regulation itself was constitutional. Similar kinds of provisions may well be buried in any number of legislative or regulatory instruments at the federal, provincial, and territorial level.

88. Rogers Communications, *2015 Rogers Transparency Report* (May 2016), http://about.rogers.com/about/helping-our-customers/transparency-report.

89. Telus Communications, *Sustainability Report 2015, "Business Operations: Transparency*," https://sustainability.telus.com/en/business-operations/transparency-report/.

90. Michael Geist, "Why Telecom Transparency Reporting in Canada Still Falls Short," *Michael Geist* (blog) (May 30, 2016), http://www.michaelgeist.ca/2016/05/why-telecom-transparency-reporting-in-canada-still-falls-short/.

91. Jim Bronskill, "RCMP Drops Some Internet-Related Probes Following Supreme Court Ruling," *CBC News* (November 21, 2014), http://www.cbc.ca/news/politics/rcmp-drops-some-internet-related-probes-following-supreme-court-ruling-1.2844390; Michael Geist, "The Spencer Effect: No More Warrantless Access to Subscriber Info with Five Minutes of

Apart from PIPEDA requests, it is clear that law enforcement and intelligence agencies interact with and rely upon private sources of information in a variety of ways, including through data mining techniques that scan publicly available information online,[92] as well as through purchasing information from private-sector data brokers.[93] However, the exact nature, extent, and prevalence of these practices remains unclear.

F. Role of the Courts

The courts play a central role in delineating the parameters within which the government may gain access to personal information in various capacities discussed above, including: articulating the constitutional parameters surrounding access, reviewing and (where applicable) enforcing decisions by privacy commissioners, and hearing and deciding applications for warrants and prior judicial authorizations for interceptions. In 2013, Federal Court Justice Richard Mosley held that that CSIS breached its duty of candor when it solicited help from Five Eyes partners while executing a surveillance warrant.[94] Furthermore, as noted above, the 2014 SCC ruling on voluntary disclosure of subscriber data in *Spencer* has had significant impact on Canadian private-sector disclosure norms, requiring that law enforcement seek pre-authorization before requesting subscriber data from ISPs.

G. Standards for Use, Access, Retention, and/or Destruction by Government

Standards for government use, access to, retention, and/or destruction of information about individuals are set first and foremost by the Privacy Act for federal institutions and by various provincial and territorial privacy acts for their respective jurisdictions. The key provisions in the federal legislation are set out in detail in Section III(B)1 above. The sharing of information among the CSE, CSIS, and the RCMP through memorandums of understanding technically permitted under the Privacy Act have been the subject of some controversy.

Police Work," *Michael Geist* (blog) (November 21, 2014), http://www.michaelgeist.ca/2014/11/spencer-effect-warrantless-access-subscriber-info-five-minutes-police-work/; Geist, Why Watching the Watchers, above note 47, at 243.

92. Security Intelligence Review Committee, *Checks and Balances: Viewing Security Intelligence Through the Lens of Accountability, Annual Report 2010–2011*, http://www.sirc-csars.gc.ca/pdfs/ar_2010-2011-eng.pdf.

93. Canadian Internet Policy and Public Interest Clinic, *On the Data Trail: How Detailed Information about You Gets into the Hands of Organizations with Whom You Have No Relationship, A Report on the Canadian Data Brokerage Industry* (April 2006), http://www.cippic.ca/sites/default/files/May1-06/DatabrokerReport.pdf.

94. *Re X*, 2013 FC 1275.

Of particular concern has been the possibility that the more onerous warrant provisions applicable to the RCMP might be circumvented through cooperation with CSIS and/or CSE, each of which has access to its own specific authorization provisions discussed above.[95] The more general issue of information sharing between law enforcement and intelligence agencies, and between Canadian agencies and foreign counterparts (particularly those who engage in torture) has also been canvassed in several prominent public inquiries.[96] Despite cautions against increased information sharing, Bill C-51 introduced provisions authorizing federal agencies and departments to share information pursuant to national security investigations, as discussed in more detail above.

H. Cross-Border and Multi-jurisdictional Issues

Participation in numerous information sharing arrangements and networks[97] to some degree facilitates law enforcement agencies' access to general information outside of Canadian borders through counterparts in other jurisdictions. More formal requests for access to such data can also be made from law enforcement officials in other countries under the numerous mutual legal assistance treaties to which Canada is a signatory.[98] Canada also cooperates with its co-signatories to the UK-USA Security Agreement, as noted above in Section III(C)3. Further, as discussed above, passage of Bill C-51 brought with it explicit authorization for sharing of certain kinds of information (such as no-fly lists) with foreign states.

Protecting the privacy of Canadians' data has certainly involved cross-border issues, particularly in relation to that data's accessibility to US authorities under the *PATRIOT Act*. For example, Canadian entities' outsourcing of data-related services to US entities generated recommendations from the British Columbia

95. CSEC, *Annual Report 2010–2011*, above note 42; Forcese, above note 38, at 501–02.

96. Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *Report of the Events Relating to Maher Arar: Analysis and Recommendations* (2006), http://epe.lac-bac.gc.ca/100/206/301/pco-bcp/commissions/maher_arar/07-09-13/www.ararcommission.ca/eng/AR_English.pdf; Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182, *Air India Flight 182: A Canadian Tragedy* (2010), http://publications.gc.ca/collections/collection_2010/bcp-pco/CP32-89-4-2010-eng.pdf; Frank Iacobucci, *Internal Inquiry into the Actions of Canadian Officials in Relation to Abdullah Almaki, Ahmad Abou-Elmaati and Muayyed Nureddin Final Report* (2008).

97. See, for example: the Virtual Global Taskforce Combatting Online Child Sexual Abuse, involving organizations from Canada, the United States, Australia, Europe and elsewhere: RCMP, *Virtual Global Taskforce: International Law Enforcement Working Together to Protect Children*, http://www.rcmp-grc.gc.ca/ncecc-cncee/vgt-eng.htm.

98. Included amongst the countries with whom Canada has signed such treaties are Australia, China, France, India, the United States, and numerous others. Information Exchange Network for Mutual Assistance in Criminal Matters and Extradition, *Principles Providing a Framework for Mutual Legal Assistance and Extradition and More Information: Canada 2004*, http://www.oas.org/juridico/mla/en/can/en_can-mla-gen-g8iag.html.

Privacy Commissioner in 2004 for, inter alia, legislation making it an offense to outsource the handling of a British Columbian's personal information outside of Canada.[99] A complaint to the PCC relating to the transborder flow of Canadians' personal information to a US data broker resulted in a judicial decision declaring that the PCC had jurisdiction to investigate the complaint, even though PIPEDA did not have extraterritorial effect.[100] Given that the PCC may assert jurisdiction in cases involving extraterritorial elements, so long as there is a real and substantial connection to Canada, the PCC has issued recommendations relating to Canadian companies' outsourcing of data-related services to firms in foreign countries, reminding Canadian entities of their PIPEDA obligations relating to notice and consent.[101] More recently, the PCC issued a publication identifying the privacy implications relating to cloud computing and reiterating the jurisdictional constraints and capacities of the Office of the Privacy Commissioner of Canada in relation to it.[102]

IV. RECENT CONTROVERSIES

The last five years have seen significant changes to Canadian national security and lawful access regimes, as well as dramatic revelations of bulk, indiscriminate, and pervasive international surveillance affecting and involving Canadians. Systematic domestic and international access to Canadian private-sector data remains a complex issue, governed by a patchwork of laws that feature many moving parts. As Lisa Austin notes, increased information sharing and the increasingly blurred investigatory roles of law enforcement, border control, and intelligence agencies have made "gaining a clear public understanding of proposed changes to lawful access laws or the full significance of legal cases before the courts [. . .] extremely difficult."[103] Although an extended discussion of the systemic effects of recent Canadian legislative changes lies beyond the scope of this chapter, we highlight some pertinent events, concerns, and controversies below.

In 2013, following the high-profile suicides of two Canadian teens, the Canadian government passed legislation prohibiting the non-consensual

99. Office of the Information and Privacy Commissioner for British Columbia, *Privacy and the USA Patriot Act: Implications for British Columbia Public Sector Outsourcing* (October 2004), https://www.oipc.bc.ca/special-reports/1271.

100. *Lawson v. Accusearch Inc*., 2007 FC 125.

101. *Outsourcing of Canada.com Email Services to US-Based Firms Raises Questions for Subscribers,* 2008 CanLII 58164 (PC).

102. Privacy Commissioner of Canada, *Reaching for the Cloud(s): Privacy Issues Related to Cloud Computing* (2010), http://www.priv.gc.ca/information/pub/cc_201003_e.cfm.

103. Lisa M. Austin, "Lawful Illegality: What Snowden Has Taught Us about the Legal Infrastructure of the Surveillance State," in Michael Geist, ed., *Law, Privacy, and Surveillance in Canada in the Post-Snowden Era* (2014) 103, 106.

distribution of intimate images, which also contained lawful access provisions long sought by Canada's previous federal government. Bill C-13 established new warrants and production orders for transmission, tracking, and financial data held by private-sector organizations, available to public officers who have reasonable grounds to suspect that an offense has been or will be committed under domestic law or under a law of a foreign state. As the current PCC notes, Bill C-13 leaves the definition of "public officers" broad, potentially offering "not just police, but anyone from a township reeve to a fisheries officer to a mayor with lawful access to personal information under reduced thresholds."[104] The new law also includes an immunity provision that "increases the likelihood of voluntary disclosures at the very time that Canadians are increasingly concerned with such activity,"[105] and imposes no good faith or reasonableness requirement on organizations that voluntarily disclose information to authorities. Others have further argued that the reasonable suspicion standard for metadata warrants in Bill C-13 seems at odds with the values underpinning the SCC's *Spencer* decision, which recognized a significant privacy interest in subscriber data held by ISPs.[106]

These changes take on new significance when considered alongside Bill C-51, a piece of controversial antiterror legislation passed in 2015. In addition to authorizing information sharing across federal departments for national security purposes, Bill C-51 makes changes to the no-fly list regime, and introduces provisions that criminalize knowingly advocating or promoting the commission of terrorism offenses in general. The new speech crime provisions in C-51 expand the range of situations where Bill C-13's metadata warrants may be issued, and raise the troubling possibility that "to detect the wrong type of speech, police may need to monitor all sorts of other speech during which the bad things might be said."[107] Furthermore, Bill C-51's permissive information sharing provisions may afford CSIS and other agencies indirect access to metadata that has been collected by police under the relaxed reasonable suspicion standard established in Bill C-13.[108]

Metadata collection in particular has become a matter of heightened public concern and debate in Canada in light of the 2013 Snowden revelations. The legal basis for CSE's metadata collection programs is the subject of an ongoing constitutional challenge by the British Columbia Civil Liberties Association and related "Stop Illegal Spying" public outreach campaign.[109] Furthermore, in

104. PCC, *2014–2015 Privacy Act Annual Report*, above note 7, at 14.

105. Michael Geist, *Testimony before the Justice and Human Rights Committee* (May 29, 2014), https://openparliament.ca/committees/justice/41-2/27/dr-michael-geist-1/only/.

106. John Geddes, "Cyberbulling, the Supreme Court and the Future of Bill C-13," *Maclean's* (June 21, 2014), http://www.macleans.ca/news/canada/suspicion-may-not-cut-it/.

107. Forcese & Roach, above note 53, at 127.

108. Ibid., at 128.

109. British Columbia Civil Liberties Association, "Stop Illegal Spying" (last visited April 26, 2017), https://bccla.org/stop-illegal-spying/.

light of recent insights into the extent of international spying, some have called for efforts to build more Canadian Internet exchange points, promote greater Canadian network sovereignty, and take measures to prevent data flow to countries with questionable privacy and surveillance practices.[110]

Despite having review bodies that can separately evaluate RCMP, CSE, and CSIS conduct, Canada currently lacks a body that can review cross-departmental national security activities. As Roach and Forcese write, "accountability bodies [in Canada] are restricted in the extent to which they can carefully scrutinise security service operations—each review body is 'siloed' to its own agency and cannot share confidential information."[111] Furthermore, as four former Canadian prime ministers noted in an open letter published during the debates surrounding Bill C-51, "the lack of a robust and integrated accountability regime for Canada's national security agencies makes it difficult to meaningfully assess the efficacy and legality of Canada's national security activities."[112]

In April 2017, the House of Commons approved Bill C-22, the National Security and Intelligence Committee of Parliamentarians Act and on May 30, 2017 the Senate referred the Act to Committee. If enacted, this bill would create a committee of parliamentarians with the power to review any matter or activity relating to national security or intelligence. Although public response to Bill C-22 has been largely positive to date,[113] some doubts remain as to whether the body will be able to act free of executive interference, and whether enhanced review can be effective without further substantive changes to the complex legal framework governing lawful access, information sharing, and national security investigations in Canada.[114]

110. Andrew Clement & Johnathan A. Ober, "Canadian Internet 'Boomerang' Traffic and Mass NSA Surveillance: Responding to Privacy and Network Sovereignty Challenges" in Michael Geist, ed, *Law, Privacy and Surveillance in Canada in the Post-Snowden Era* (2014) 13, 35.

111. Forcese & Roach, above note 53, at 145.

112. Jean Chrétien, Joe Clark, Paul Martin & John Turner, "A Close Eye on Security Makes Canadians Safer," *The Globe and Mail* (February 19, 2015), http://www.theglobeandmail.com/opinion/a-close-eye-on-security-makes-canadians-safer/article23069152/; Forcese & Roach, above note 53, at 400.

113. Ian McLeod, "Liberal Plan for New National Security Watchdog Gets Thumbs Up from Experts, Despite 'Inevitable Flaws,'" *National Post* (June 19, 2016), http://news.nationalpost.com/news/canada/canadian-politics/liberal-plan-for-new-national-security-watchdog-gets-thumbs-up-from-experts-despite-inevitable-flaws; Canadian Civil Liberties Association, "Bill C-22: A Step towards Real Accountability" (June 20, 2016), https://ccla.org/bill-c-22-a-step-towards-real-accountability.

114. Geist, Watching, above note 47, at 226; Austin, above note 103, at 104.

V. CONCLUDING OBSERVATIONS

Canada is at something of a crossroads in terms of expanded systematic state access to data held by the private sector. Constitutional and statutory norms protecting reasonable expectations of privacy from state intrusion generally underline the importance of prior judicial authorization and investigations focused by reasonable grounds relating to identifiable offenses. However, these norms have already been challenged by provisions that empower CSE to surveil Canadians' data with ministerial approval, compel private-sector organizations to collect and disclose personal information to authorities, and facilitate easier access to intercept authorization, if not warrantless access to data. Exceptions in the *Privacy Act* and PIPEDA that permit sharing of personal information between government institutions as well as recent provisions authorizing voluntary personal information disclosure by the private sector to law enforcement agencies further erode the standard of prior judicial authorization (subject to the SCC's findings in *Spencer*). Recent legislation authorizing information sharing among law enforcement, security agencies, other government officials, and, in some cases, foreign states, raises further cause for concern and presents challenges for meaningful and robust public accountability and oversight. Whether a newly proposed oversight committee would adequately address those challenges remains the subject of some controversy.

8

Systematic Government Access to Private-Sector Data in the United States I

STEPHANIE K. PELL*

I. ABSTRACT

After the September 11 (9/11) attacks, law enforcement's mission expanded to include, at times even prioritize, the general "prevention, deterrence and disruption" of terrorist attacks, which presumed a new emphasis upon threat detection and identification by analyzing patterns in larger, less specific bodies of information.

Moreover, after 9/11, law enforcement was integrated into a much larger intelligence gathering operation directed at "connecting the dots" proactively, in order to avert the *next* terrorist attack. This new focus, spread across a broad range of federal and state agencies, has created a voracious appetite for information—data found most often in the possession of industry, given consumer use of new technologies to facilitate personal, social, business, and economic transactions.

Indeed, the unprecedented level of "third-party" possession of information inevitably makes the private sector the most reliable and comprehensive source of information available to law enforcement and intelligence agencies alike. Notwithstanding the impacts on business costs or innovation—whether for a criminal or intelligence terrorism matter or more traditional crimes where perpetrators leave electronic fingerprints with a host of third parties—there is an expectation by law enforcement, intelligence agencies, and even legislators that industry third parties will facilitate real-time government access to data when needed, and that these data will be in possession of the relevant private entities if and when a government agency realizes their potential investigative value.

This chapter will explore the potential applications of systematic government access to data held by third-party private-sector intermediaries that would not be

* The views expressed here are those of the author and do not represent the position of the United States Military Academy at West Point, the Army, or the United States government.

Bulk Collection. Fred H. Cate and James X. Dempsey.

considered public information sources but, rather, data generated based on the role these intermediaries play in facilitating economic and business transactions (including personal business, such as buying groceries or staying at a hotel on vacation).

II. INTRODUCTION AND OVERVIEW

Following the September 11th attacks, the mission of police and prosecutors expanded dramatically. Before that date, most law enforcement resources were allocated for the post-facto investigation or prospective prevention of specific crimes (such as organized crime and drug trafficking investigations), with far fewer devoted to intelligence collection and threat detection to prevent an attack upon the homeland. After September 11th, however, law enforcement's mission expanded to include, at times even prioritize, the general "prevention, deterrence and disruption" of terrorist attacks, which presumed a new emphasis upon threat detection and identification by analyzing patterns in larger, less specific bodies of information. Moreover, after 9/11, law enforcement was integrated into a much larger intelligence gathering operation directed at "connecting the dots" proactively, in order to avert the *next* terrorist attack.

This new focus, spread across a broad range of federal and state agencies, has created a voracious appetite for information—data found most often in the possession of industry, given consumer use of new technologies to facilitate personal, social, business, and economic transactions. Indeed, the unprecedented level of data in the possession of third parties inevitably makes the private sector the most reliable and comprehensive source of information available to law enforcement and intelligence agencies alike. Moreover, although many sources and forms of information are already available to law enforcement, the widespread adoption of Internet of Things (IoT) technology will generate additional forms of metadata, potentially revealing sensitive information that would have been difficult for the government to obtain in the past.

Notwithstanding the impacts on business costs, business reputation, or innovation—whether for a criminal or intelligence terrorism matter or more traditional crimes where perpetrators leave electronic fingerprints with a host of third parties—there is an expectation by law enforcement, intelligence agencies, and even legislators that industry third parties will facilitate real-time government access to data when needed, and that these data will be in possession of the relevant private entities if and when a government agency realizes their potential investigative value.

Perhaps the earliest, most visible post-September 11th expression of the government's appetite for information came in the form of a data mining project led by the Defense Advanced Research Projects Agency (DARPA), originally named "Total Information Awareness" (TIA), but later, significantly, renamed "Terrorism Information Awareness."[1] The new name might have suggested a new

1. Fred H. Cate, "Government Data Mining: The Need for a Legal Framework," 43 *Harv. C.R.-C.L. L. Rev.* 445, 449 (2008).

and limiting precision in the scope of the project, but this change should not be read to signal any change, either in practice or in the program's ultimate goal. In 2002, John Poindexter, retired admiral and director of DARPA's Information Awareness Office, identified the "transaction space" as one of the "significant new data sources that need to be mined to discover and track terrorists."[2] This "transaction space" included data encompassing communications, financial, education, travel, medical, veterinary, country entry, place/event entry, transportation, housing, critical resources, and government records. As part of the TIA program, DARPA "Red Teams" would develop model attack scenarios and then determine the types of transactions that would be necessary to carry out such attacks in reality.[3] These transactions could form patterns that would be discernable in databases to which the government would have lawful access. Having developed targetable patterns of attack precursor behavior, the government, it was proposed, could then search across databases to detect the presence of those patterns.

Although the funding for this kind of "total information awareness" program was ultimately terminated by Congress in 2003, following protests about the privacy impact of such an operation, the kind of threat forecasting through data mining represented by the TIA concept was an early indicator of the role powerful automated suspicion algorithms may increasingly play in law enforcement and intelligence operations. Moreover, the Snowden disclosures, beginning in the summer of 2013, revealed other kinds of collection programs aimed at facilitating certain kinds of comprehensive information awareness by the government, for specific purposes.[4]

This chapter will explore the potential applications of systematic US government access to data held by third-party private-sector intermediaries that would not be considered public information sources[5] but, rather, data generated based on the role these intermediaries play in facilitating economic, business, and personal transactions. For the most part, US laws and regulations do not directly

2. John Poindexter, Director, Info. Awareness Office, Overview of the Info. Awareness Office, Prepared Remarks for Delivery at DARPATech 2002 Conference (August 2, 2002), at 1, http://www.fas.org/irp/agency/dod/poindexter.html.

3. Info. Awareness Office, US Dep't of Def., *Report to Congress Regarding the Terrorism Information Awareness Program* (2003) 15, https://epic.org/privacy/profiling/tia/may03_report.pdf.

4. Although numerous classified documents have been made public since the initial Snowden disclosures in summer of 2013, this chapter will only make reference to declassified or unclassified information pertaining to these disclosures. There may be additional examples relevant to this discussion that are in the public realm but, nevertheless, remain classified.

5. With government access to the full Twitter Firehose, a service that pushes public tweets to end users in near real time that match customers' criteria, the government could collect voluminous and possibly indiscriminate amounts of information on an ongoing basis. Although such activity raises significant privacy concerns, this chapter focuses on data in the possession of third parties that is not otherwise in the public realm.

authorize ongoing, indiscriminate government access to data held by third-party intermediaries.[6] For purposes of this chapter, the term *systematic* denotes one or more of the following practices, each of which permits the government to obtain information without *any* process or using processes to facilitate either ongoing and indiscriminate collection or discrete but significant over-collection of information by: (1) exploiting[7] gaps in existing statutes regulating government access to certain types of data held by specifically enumerated types of third parties; (2) pushing, even breaking, the boundaries of statutory language to permit the bulk collection of data; (3) using presidential authorizations; (4) creating informal partnerships with private entities; or (5) exploiting the lack of constitutional or statutory impediments to government access to certain types of data held by specific third parties. The ways in which systematic government access may operate are rarely transparent, often presenting themselves only when a controversy surfaces in the press, as was the case of the Terrorist Surveillance Program, an NSA program discussed below involving the warrantless interception of phone conversations when at least one party was located in the United States, or, more recently, the NSA's broad, indiscriminate collection and storage of US domestic telephone records, also discussed below.

This chapter examines the primary US constitutional and statutory authorities governing law enforcement and intelligence agency access to private-sector data. As these various authorities are discussed, relevant examples of systematic government access to private-sector data—whether by voluntary disclosure or compelled legal process—are raised and integrated into the analysis.[8]

6. US law mandates some ongoing third-party disclosures of various types of information involving, for example, cargo and passengers coming into the United States from abroad or financial data that might assist the government in identifying money laundering or terrorist financing. These data are divulged to the government pursuant to various regulatory requirements.

7. The term "exploiting" as used in this paragraph is not meant to convey a sinister motive. Rather, if the government is not prohibited from collecting data by the Constitution or by statute, then it can lawfully collect that data consistent with internal agency guidelines and authorized investigative activities, with very limited, if any, barriers.

8. This chapter is written as an overview of the subject matter and is not meant to be a comprehensive treatment of systematic access to private-sector data in the United States. Of note, this chapter does not address the application of Executive Order (E.O.) 12333, issued by President Reagan in 1981 and modified several times since, which, among other things, regulates the collection of information about foreigners outside the United States for foreign intelligence purposes. E.O. 12333 governs activities that are "not covered by statute and do not [otherwise] require a court order." Timothy Edgar, "Surveillance Reform: Privacy Board Turns to E.O. 12,333," *Lawfare* (May 3, 2015), https://www.lawfareblog.com/surveillance-reform-privacy-board-turns-eo-12333. The Privacy and Civil Liberties Oversight Board (PCLOB), an independent, bipartisan executive branch agency authorized by Congress to ensure that "liberty concerns are appropriately considered in the development and implementation of laws, regulations, and policies related to efforts to protect the Nation against terrorism" (42 U.S.C. § 2000(c)(2) (2012)), has held public hearings about E.O. 12333 and also plans to issue a public report.

III. US CONSTITUTIONAL LIMITS

The primary constitutional limit on the government's ability to obtain private or personal information is the Fourth Amendment, which prohibits unreasonable searches and seizures. Supreme Court Fourth Amendment case law has prescribed certain tests to determine whether a search has occurred, which is the preliminary question to be answered before turning to whether any particular search is unreasonable. Justice Harlan's famous concurrence in *Katz v. United States,*[9] now commonly referred to as the *Katz* test, guides courts in determining what constitutes a search under the Fourth Amendment: courts must determine whether the government conduct in question violates a subjective expectation of privacy and an objectively reasonable expectation of privacy. More recently, in *United States v. Jones,*[10] a case involving the government's warrantless attachment and use of a GPS device to track the movements of Jones's car for 28 days, Justice Scalia wrote a majority opinion articulating a property-based rationale for determining what constitutes a Fourth Amendment search. This trespass-based test is satisfied when: (1) a "trespass" occurs, (2) the trespass is to a target enumerated in the Fourth Amendment ("persons, houses, papers, or effects"), and (3) it occurs with the intent "to find something or to obtain information."[11] Of note, the application of this trespass, property-based rationale allowed the majority to avoid ruling in a way that would have had implications for other types of tracking technologies that solely employ the transmission of radio or other electronic signals not enabled by a direct physical trespass, such as tracking a target's cell phone through compelled disclosure of location information possessed by a third party. Indeed, the law is still in flux with respect to whether the Fourth Amendment protects location information in the possession of a third-party carrier.

Generally speaking, the Fourth Amendment provides little to no protection for non-content information stored by third parties. Specifically, the infamous *third party doctrine,* a long-standing constitutional principle suggests, when taken in its strongest expression, that once data is disclosed to a third party, it no longer receives Fourth Amendment protection.[12] The seminal cases establishing the third-party doctrine are *United States v. Miller,*[13] a case concerning

9. *Katz v. United States*, 389 U.S. 347, 361 (1967).

10. 132 S. Ct. 945 (2012).

11. See Orin Kerr, "The New Doctrine of What Is a Fourth Amendment Search," *Volokh Conspiracy Blog* (January 23, 2012), http://volokh.com/2012/01/23/the-new-doctrine-of-what-is-a-fourth-amendment-search/.

12. For a detailed discussion about the difficulty of applying the third-party doctrine in an IP-based communications environment, see Steven M. Bellovin, Matt Blaze, Susan Landau, and Stephanie K. Pell, "It's Too Complicated: How the Internet Upends *Katz, Smith*, and Electronic Surveillance Law," 30 *Harvard Tech. L.J.* 1 (2017).

13. 425 U.S. 435 (1976).

cancelled checks where the Supreme Court reasoned that the respondent "can assert neither ownership or possession" in documents "voluntarily conveyed to banks and exposed to their employees in the ordinary course of business,"[14] and *Smith v. Maryland*,[15] where the Court held that the Fourth Amendment does not apply to transactional information associated with making phone calls (for example, time/date/length of call and numbers dialed) because that information is voluntarily conveyed to third parties to connect the call, and phone companies record the information for a variety of legitimate business purposes.

The privacy protections that do exist for third-party records are primarily found in statutes enacted by Congress specifically in response to Supreme Court opinions limiting Fourth Amendment protections. Additional privacy protections may be found in agency guidelines and privacy policies, some of which exist because Congress has mandated their creation by statute. Although it is beyond the scope of this chapter to conduct an analysis of the full scope of such policies (some of which may be classified) and their impact on the government's systematic access to third-party records, policy that is managed by political leadership of an agency is always subject to change, for better or worse.

IV. STATUTORY OVERVIEW AND ANALYSIS

For purposes of exploring potential systematic government access to third-party private-sector data, it is often useful to think about statutory privacy protections in terms of (1) what kind of third-party private-sector entities they regulate, and (2) what type of information they regulate. Sometimes, a statute will regulate the disclosure of a specific type of information to the government, but only by a specific type of third party. Thus, the disclosure of the same type of information by a third party not covered by the statute could lawfully occur without any legal process. In the service of exploring the potential for systematic government access, this section will analyze the primary statutes regulating third-party disclosure of information to the government, the Electronic Communications Privacy Act (ECPA),[16] the Foreign Intelligence Surveillance Act (FISA),[17] the statutes authorizing National Security Letters (NSLs),[18] and the Right to Financial Privacy Act (RFPA).[19] These statutes, although certainly not the only authorities

14. Ibid. at 442–43.

15. 442 U.S. 735 (1979).

16. 18 U.S.C. §§ 2511–2520 (2012); 18 U.S.C. §§ 2701–2712 (2012); 18 U.S.C. §§ 3121–3127 (2012).

17. 50 U.S.C. §§ 1801–1862 (2012 & Supp. 2014).

18. There are five provisions of law that authorize the FBI to issue five types of NSLs: 12 U.S.C. § 3414(a)(5)(A) (2012); 18 U.S.C. § 2709 (2012); 15 U.S.C. § 1681u (2012 & Supp. 2015); 15 U.S.C. § 1681v (2012 & Supp. 2015); 50 U.S.C. § 436, recodified as 50 U.S.C. 3162 (Supp. 2014)].

19. 12 U.S.C. §§ 3401–3422 (2012).

affecting government access to and retention of third-party private-sector data, provide the richest opportunity for discussion of systematic government access to these data. As these key statutes govern various aspects of government access to (1) electronic communications, (2) financial data, and (3) other records in the possession of third parties for both criminal and national security investigations, the discussion below will group these authorities as they relate to these three major categories of information.

A. Electronic Communications Data: ECPA, FISA, and NSLs

1. "Real-Time" Communications Content

The Wiretap Act (Title I of ECPA) governs law enforcement access to real-time wire, oral, and electronic communications in criminal investigations. To collect these communications, the government must establish, in a written application to a judge of competent jurisdiction, that there is probable cause to believe: (1) an individual is committing, has committed, or is about to commit a particular offense enumerated in the Wiretap Act; and (2) particular communications concerning that offense will be obtained through the requested interception.[20] In addition to this probable cause showing, the government must also demonstrate that other normal investigative procedures have been tried and have failed, or reasonably appear unlikely to succeed if tried, or would be too dangerous to execute.[21] The Wiretap Act also limits this intrusive surveillance tool to specific crimes listed in the statute. This list is extensive and includes a broad range of terrorism-related statutes.

In the case of terrorism national security investigations, however, the federal government's ability to intercept real-time communications is not limited to authorities provided in the Wiretap Act. Such investigations—involving the collection of foreign intelligence about "foreign powers" or "agents of foreign powers" in addition to or even in the absence of pursuing activity that may violate criminal statutes—are often more readily and appropriately pursued under FISA authorities. Accordingly, FISA authorizes interception of real-time wire, oral, and electronic communications when, by written application to the FISA Court, the government demonstrates that there is probable cause to believe that (1) the target of the electronic surveillance is a foreign power or agent of a foreign power, and (2) each of the facilities or places at which electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power, which includes a so-called "lone wolf" (i.e., an unaffiliated foreign individual posing a threat).[22]

Warrants granted pursuant to the Wiretap Act are often called "super warrants" and considered by some to be the gold standard with respect to limiting unconstitutional and/or over-collection of communications content. The "high

20. 18 U.S.C. §§ 2518(3)(a),(b) (2012).

21. 18 U.S.C. § 2518(c) (2012).

22. 50 U.S.C. § 1805 (2012 & 2014 Supp.).

comfort" with the statute derives from several factors, including, but not limited to the fact that the probable cause showing is predicated upon the discovery of evidence of a specific crime, that non-relevant communications must be minimized, and that all federal wiretap applications must go through a special review process at the DOJ in Washington DC (Main Justice). Although a comprehensive comparison between the Wiretap Act and FISA is beyond the scope of this chapter, FISA also contains minimization and oversight provisions, including its own specialized review process at Main Justice and a certification by a high-level official that such information cannot be obtained by normal investigative techniques. FISA's probable cause standard, however, is premised on the collection of foreign intelligence relating to foreign powers or agents of foreign powers rather than the collection of evidence a crime, arguably permitting a broader, more flexible exercise of government surveillance powers.

Notwithstanding the lower threshold of FISA surveillance standards, in 2005 the *New York Times* reported that the Bush administration, via classified presidential authorizations, had granted the NSA authority for *warrantless* monitoring of international telephone calls and electronic communications (such as email), even when one party was a US person located on US soil.[23] This so called Terrorist Surveillance Program (TSP), which circumvented FISA, was evidently developed through a public-private partnership where NSA informally arranged with top telecommunications company officials to gain access to switches carrying America's communications without warrants or court orders.[24] After the TSP was exposed, industry members sought and received retroactive immunity for their participation, which had been at least partially contingent upon guarantees that they would not suffer adverse consequences stemming from their uncompelled informal cooperation.[25] The TSP illustrates a problematic example of systematic access to private-sector data: the executive branch, through a classified presidential order, circumvented existing provisions of the FISA statute and bypassed congressional oversight by, among other things, enlisting the assistance of third-party telecommunications providers in its legally questionably operation.[26]

23. James Risen and Eric Lichtblau, "Bush Lets U.S. Spy on Callers without Courts," *N.Y. Times* (Dec. 16, 2005); see also Jon D. Michaels, "All the President's Spies: Private-Public Intelligence Partnerships in the War on Terror," 96 *Cal. L. Rev.* 901, 910 (2008).

24. Michaels above note 23 at 910.

25. On December 29, 2011, the Ninth Circuit, in *Hepting v. AT&T Corp.*, 671 F.3d 881 (9th Cir. 2011) upheld the constitutionality of § 802 of the FAA of 2008, which gave telecom companies a path to retroactive immunity from charges of misconduct, including privacy violations, for cooperating with the Bush administration's warrantless wiretapping efforts.

26. For further discussion of the TSP, how it violated FISA, and how it was brought under court supervision via the FAA, see Stephanie Cooper Blum, "What Really Is at Stake with the FISA Amendments Act of 2008 and Ideas for Future Surveillance Reform," 18 *Boston Univ. Public Interest L.J.* 269 (2009).

Ultimately, Congress brought the TSP under the umbrella of FISA and some degree of FISC oversight by enacting the Protect America Act of 2007 (PAA)[27] and the FISA Amendments Act of 2008 (FAA).[28] When compared with traditional FISA processes, however, the FAA, via Section 702,[29] "impose[s] significantly fewer limits on the government when it targets foreigners located abroad, permitting greater flexibility and a dramatic increase in the number of people who can realistically be targeted."[30] Specifically, Section 702 authorizes the attorney general and the Director of National Intelligence jointly to authorize surveillance, and to compel third-party assistance for such surveillance, which targets people who are not US persons and who are reasonably believed to be outside the United States, so long as the surveillance is conducted to acquire foreign intelligence information. Notably, there is no requirement that the government make an individualized showing to the FISC that there is probable cause to believe a particular target is a foreign power or an agent of a foreign power. Instead, the attorney general and the director of national intelligence make annual certifications authorizing the targeting to acquire foreign intelligence information and develop targeting and minimization procedures that must meet certain criteria. The FISC reviews and approves the annual certifications and accompanying procedures, evaluating whether they satisfy the identified criteria.

When examining the government's use of Section 702, the Privacy and Civil Liberties Oversight Board (PCLOB) found general government "compliance with the text of Section 702 [and that] the text of 702 provides the public with transparency into the legal framework for collection."[31] One significant public criticism of Section 702, however, concerns what some call "backdoor searches."[32] Although US persons cannot be targeted pursuant to Section 702 (with the understanding that some US person information will be collected incidentally), it appears that some US person identifiers have been used to query information collected under Section 702, and that Section 702 may not explicitly prohibit such searches.[33] In response, lawmakers attempted to amend the Defense Appropriations Act of 2017 with a provision preventing the NSA from using funds for such queries.[34]

27. Protect America Act of 2007, Pub. L. No. 110-55, 121 Stat. 552. The PAA was limited to six months, expiring in February 2008.

28. FISA Amendments Act of 2008, Pub. L. No. 110-261, § 403, 122 Stat. 2463, 2473 (2008).

29. The second story published about the Snowden disclosures in June 2013 involved Section 702 and the PRISIM program. See PCLOB, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* (July 2, 2014) at 1–8.

30. Ibid. at 10.

31. Ibid. at 8.

32. See Ashley Nicole Baker, "Congress Must Shut the Backdoor on Section 702 Surveillance," *FreedomWorks*, blog post (June 15, 2016).

33. Ibid.

34. See Amendment to H.R. 5293, offered by Rep. Thomas Massie of Kentucky.

Section 702 is set to expire in 2017. When Congress considers the statute for reauthorization, the unresolved issue of whether and how to amend Section 702 in response to backdoor searches will likely arise once again.

2. Stored Communications Content

Title II of ECPA, the Stored Communications Act (SCA),[35] governs law enforcement access to the content of communications when in the possession of a third-party providing an "electronic communications service" (ECS)[36] or a "remote computing service" (RCS)[37] to the public. These definitions reflect the state of the Internet and corresponding Internet-based services that existed in 1986, the year the SCA was enacted by Congress. Although the definition of RCS certainly reflects Congress's understanding that there could and would be third-party storage of content ("computer storage or processing services"), Congress could not have foreseen the extent to which various types of third-party storage used by consumers and businesses alike would become a booming business model due to an explosion in cloud-based services. Recall that in 1986, third-party storage was prohibitively expensive, causing most people and businesses using computers to store electronic content locally on a hard drive or floppy disk.

Consistent with Fourth Amendment doctrine, law enforcement must normally get a warrant in order to search and seize a laptop, desktop, or thumb drive. Congress extended the warrant protection via statute to communications content stored in an ECS (such as unopened email).[38] Today, however, a large amount of data stored in the cloud (including opened emails) is arguably in RCS storage. In 1986, Congress did not extend full warrant protections to communications content in RCS storage.[39] Rather, under the SCA, the government can compel third-party providers to disclose communications content in RCS storage with an 18 USC § 2703 (d) Order (a court order under which the government must show, with "specific and articulable facts," that there are reasonable grounds to believe that the information sought is "relevant and material" to an ongoing criminal investigation), or even with a subpoena.[40] This disparity in the level of privacy protections given to information stored "in the cloud" versus content

35. 18 U.S.C. §§ 2701–2712 (2012).

36. An electronic communication service (ECS) is "any service which provides to users thereof the ability to send or receive wire or electronic communications." Examples include telephone or email services. 18 U.S.C. § 2510(15) (2012).

37. A "remote computing service" (RCS) is a "provision to the public of computer storage or processing services by means of an electronic communications system." 18 U.S.C. § 2711(2) (2012). Roughly speaking, a remote computing service is provided by an off-site computer that stores or processes data for a user. Examples include data stored "in the cloud," such as online backup services.

38. See 18 U.S.C. § 2703(a) (2012).

39. See 18 U.S.C. § 2703(b) (2012).

40. 18 U.S.C. §§ 2703(b), (d) (2012).

stored on a laptop, combined with the sheer amount of content now in third-party storage, has given the government much greater access to private-sector communications content. In response to this disparity, since 2010, Congress has held several hearings followed by the introduction of several bills that, among other things, would provide the same warrant protections to content stored in the cloud (or other forms of RCS storage). Although no legislation has passed as of April 2017, courts have begun to address this disparity. Specifically, in the 2010 *Warshak* opinion, the Sixth Circuit held that "if government agents compel an ISP to surrender the contents of a subscriber's emails, those agents have thereby conducted a Fourth Amendment search, which necessitates compliance with the warrant requirement absent some exception."[41] Moreover, the Court held that "to the extent that the SCA purports to permit the government to obtain such emails warrantlessly, the SCA is unconstitutional."[42] Although not a Supreme Court opinion or an amendment to ECPA, *Warshak* is a strong step toward the protection of content "in the cloud."

3. Stored Non-content Communications Data

A strong potential for systematic government access to *non-content* communications data comes from gaps in existing statutes and government practices. The SCA governs law enforcement access to stored non-content communications data when it is in possession of a third party providing an ECS or RCS service to the public. The SCA, however, only regulates non-content data (for example, transactional or other records pertaining to subscriber and customer names, addresses, length and type of service, temporarily assigned network address, means and source of payment) with respect to entities providing ECS and RCS services. If this non-content data is in the possession of a third party that is not acting as a public ECS or RCS, then the SCA does not provide any level of protection for the data. Without any statutory protection, third parties can, if they choose, voluntarily disclose data without any process. For example, when security researchers discovered that Apple and Google phones were collecting and transmitting back to the companies information about a device's nearby wi-fi access points and geolocation data,[43] the transmission of the location data was arguably not a function of an ECS or RCS service and thus would not receive the SCA protections otherwise afforded to historical location data. The government could, therefore, compel the disclosure of that location data with a subpoena (when the SCA would otherwise require a court order) or it could be disclosed to the government voluntarily by a third-party entity, in the absence of any emergency and without any process.

41. *United States v. Warshak*, 631 F.3d 266, 286 (6th Cir. 2010).

42. Ibid. at 288.

43. See Julia Angwin and Jennifer Valentino-Devries, "Apple, Google Collect User Data," *Wall Street Journal* (April 21, 2011), http://online.wsj.com/article/SB10001424052748703983704576277101723453610.html.

Moreover, the SCA does not prohibit the entities that provide public ECS and RCS services from disclosing non-content data to other nongovernmental entities. Once in the possession of these fourth-party entities (such as data brokers), which are not providing public ECS and RCS services, the data can be sold or otherwise disclosed to the government without process. These fourth-party commercial data brokers collect information from a range of third parties (not just those regulated by the SCA) and can provide "one stop shopping" for law enforcement and intelligence agencies alike.[44]

The SCA also contains one of the five National Security Letter (NSL)[45] authorities, a series of foreign intelligence statutory authorities, similar to subpoenas, allowing the government to compel certain types of non-content data principally from communications providers, financial institutions (defined very broadly), and credit agencies. The FBI and other designated intelligence agencies can issue NSLs without court authorization, much like subpoenas. Unlike subpoenas, however, NSLs need not even be reviewed by a prosecutor. The NSL authority found in the SCA permits the government to obtain subscriber or customer identifying records and, the government argues, other types of transactional records[46] in the possession of ECS and RCS providers (for example, non-content data pertaining to telephone and email communications).

Three different DOJ Inspector General (IG) Reports released between 2007 and 2010 document a series of abuses concerning the FBI's use of NSL authorities. Although these reports identify several types of abuses, two key problems are particularly relevant to the examination of when and how the government can get unmediated access to third-party data. First, the FBI, in violation of ECPA and various internal guidelines, used "exigent letters" (ad hoc instruments with implied legal authority where none existed) to acquire information from communication providers with the promise that actual process (NSLs or subpoenas) would follow.[47] Going forward, this kind of subterfuge with promises that "process is on its way" should raise red flags for all public-private relationships. Second, from April 2003 through January 2008, employees of certain communications providers were located in FBI's Communications Assistance Unit (CAU), which included being provided with FBI email accounts and access

44. See Michaels, above note 23 at 918.

45. 18 U.S.C. § 2709 (2012).

46. See 18 U.S.C. § 2709 (2012). The *Washington Post* reported that the government was seeking from Congress what it characterized as a "technical clarification" to § 2709 to facilitate the collection of transactional records. Others characterized the government's request as an expansion of collection authority under § 2709. See Ellen Nakashima, "White House Proposal Would Ease FBI Access to Records of Internet Activity," *Washington Post* (July 29, 2010), http://www.washingtonpost.com/wp-dyn/content/article/2010/07/28/AR2010072806141_pf.html.

47. See Oversight Review Division, Office of the Inspector General, *A Review of the Federal Bureau of Investigation's Use of Exigent Letters and Other Informal Requests for Telephone Records* (Jan. 2010).

to the CAU computer share drive.[48] These on-site providers' employees regularly attended CAU unit meetings and were treated by CAU personnel as "team members." Although the IG recognized that the collegial relationship between the co-located personnel fostered a productive working relationship, the 2010 report also notes that the "proximity of the on-site providers' employees to the CAU personnel, combined with the lack of guidance, supervision, and oversight of their interactions with FBI employees . . . contributed to some of the most serious abuses identified in this review."[49] Indeed, in this instance, there appeared to be a merger of the "public" and "private" roles.[50]

In 2014, the DOJ IG issued a fourth report reviewing the FBI's use of NSLs. This report clarifies an issue the *Washington Post* had flagged four years earlier[51] concerning the types of records the FBI could collect under ECPA's NSL provision. Although the FBI has historically interpreted Section 2709 of ECPA as granting the authority to compel "electronic communication transactional records,"[52] which have been defined in the media as "email metadata and header information, URL browsing data and more,"[53] beginning in 2009, certain third-party companies refused to provide such records in response to NSLs on the grounds that NSLs do not, in fact, authorize the FBI to compel the production of these records.[54] This dispute is premised on a discrepancy in the statute: although "electronic communication transactional records" appear in one part of the statute (18 U.S.C. § 2709(a)), they don't appear in the part of the statute that specifically lists the kinds of records available to the FBI under ECPA's NSL authority (18 U.S.C. § 2709(b)). The companies take the position that the list found in Section 2709(b) is exhaustive and, accordingly, the statute does not authorize the FBI to compel electronic communication transactional records.[55]

48. Ibid. at 24.

49. Ibid. at 25.

50. Another public-private interface involved Sprint Nextel developing a web interface to give law enforcement direct access to its subscribers' location data in order to cope with the high volume of government demands the company was receiving for disclosure of these data. *United States v. Pineda-Moreno*, 617 F.3d 1120, 1126 (9th Cir. 2010) (Kozinski, J. dissenting from denial of rehearing en banc).

51. See above note 46.

52. Office of the Inspector General, Oversight and Review Division, *A Review of the Federal Bureau of Investigation's Use of National Security Letters: Assessment of Progress in Implementing Recommendations and Examination of Use in 2007 through 2009* [hereinafter "2014 IG NSL Report"] (August 2014) at 70.

53. See Jenna McLaughlin, "Tech Companies Fight Back after Years of Being Deluged with Secret FBI Requests," *The Intercept: Unofficial Sources* (June 21, 2016), https://theintercept.com/2016/06/21/tech-companies-fight-back-after-years-of-being-deluged-with-secret-fbi-requests/.

54. 2014 IG NSL Report, above note 52 at 70–71.

55. Ibid. at 71–72.

The FBI disagrees with this position but has adapted by using a different authority found in FISA—Section 215 of the PATRIOT Act—to compel the production of electronic communication transactional records.[56] The FBI reported to the IG that the use of Section 215, which requires more internal review and approval by the FISA Court (FISC), has slowed down national security investigations.[57] The IG has consequently recommended that DOJ continue to pursue legislative clarification, consistent with DOJ's prior efforts to seek a legislative fix.[58]

Whether one agrees with the FBI's interpretation of ECPA's NSL authority or believes that electronic communication transactional records should be obtainable under NSL authority, this example illustrates that third-party companies play an important role in controlling systematic access to private-sector data. Specifically, in this case, third-party companies challenged the FBI's interpretation of the NSL authority, and it appears that Congress will affirmatively have to determine whether the government *should* have access to these kinds of records under the NSL authority's low relevance threshold.

Although Section 215 of the PATRIOT Act (Section 501 of FISA) has added greater oversight to government collection of electronic communication transactional records, the government has also used Section 215 to obtain systematic access to domestic telephone records. Section 215 permits the government to compel "tangible things" from third parties that are "relevant" to an "authorized investigation" in order: (1) "to obtain foreign intelligence information not concerning a United States person," or (2) to "protect against international terrorism or clandestine intelligence activities."[59] The very first published story about the Snowden disclosures in June 2013 involved the government's use of Section 215 to collect domestic call detail records and other domestic telephony metadata in *bulk*. Specifically, the FISC had issued questionable orders under Section 215, renewed approximately every 90 days, "authorize[ing] the NSA to collect nearly all call detail records generated by certain telephone companies in the United States, and specifie[d] detailed rules for the use and retention of these records."[60] These records, stored in a centralized NSA database, included the date and time of a call, its duration, and the participating telephone numbers. The records did not, however, include the content of any telephone conversation. The program was "intended to enable the government to identify communications among known and unknown terrorism suspects, particularly those located inside the

56. Ibid. at 72–74.

57. Ibid. at 73–74.

58. Ibid. at 74.

59. 50 U.S.C. § 1861(a)(1) (2012 & Supp. 2014).

60. Privacy and Civil Liberties Oversight Board (PCLOB), *Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court* (2014) at 8, http://www.pclob.gov/SiteAssets/Pages/default/PCLOB-Report-on-the-Telephone-Records-Programme.pdf.

United States."[61] If the government identified a phone number associated with a terrorist, for example, it could run that seed number against all the domestic telephone numbers stored in the database to assist in determining whether a known terrorist had contact with anyone in the United States.

One major criticism of this domestic surveillance program is that the "common sense" reading of the statutory text of Section 215 does not, on its face, appear to permit collection on this scale. More specifically, critics argue, an entire massive database of records—in this case the records of nearly every domestic telephone call—cannot be deemed relevant in its totality simply because *some* of the records in that database are actually relevant to an investigation. Indeed, if everything is relevant, then nothing is relevant and the limiting concept of *relevance* itself, as found in the statute, is rendered *irrelevant*. However well intentioned this collection program may have been, it is a problematic example of government systematic access to private-sector data. Although the government can rarely disclose the specific details of classified collection programs, it is important for the public to be able to gain a general understanding of the terrain and scope of the legal authorities permitting government surveillance. When reviewing the Section 215 bulk collection program, the PCLOB concluded that "Section 215 does not provide an adequate legal basis to support the program."[62] Moreover, prior to the program's disclosure in the summer of 2013, Senator Wyden warned his colleagues that "when the American people find out how their government has secretly interpreted the PATRIOT Act, they will be stunned and they will be angry."[63] With the passage of the USA FREEDOM Act in 2015,[64] Congress ended the bulk collection of business records under Section 215.

4. "Real Time" Non-content Communications Data

Although the SCA regulates government access to stored non-content data in the possession of certain types of third-party providers, Title III of ECPA (commonly referred to as the pen register and trap and trace device statute or simply as "Pen/Trap") governs law enforcement's ability to acquire real-time transactional information about phone calls.[65] While DOJ's public manual on *Searching and Seizing Computers* does not give a detailed list of all of the specific types of transactional information that can be obtained with a Pen/Trap order, it notes that the statute's "'dialing, routing addressing [and/or] signaling information'

61. Ibid.

62. Ibid. at 10.

63. Press Release, Senator Ron Wyden, *In Speech, Wyden Says Official Interpretations of Patriot Act Must Be Made Public* (May 26, 2011), http://wyden.senate.gov/newsroom/press/release/?id=34eddcdb-2541-42f5-8f1d-19234030d91e.

64. USA Freedmom Act of 2015, Pub. L. No. 114-23, 129 Stat. 268.

65. See 18 U.S.C. §§ 3121–3126 (2012). In foreign intelligence investigations, the government may also use FISA Pen/Trap authorities. See 50 U.S.C. § 1842 (2012 & Supp. 2014).

encompasses almost all non-content information in a communication."[66] The Electronic Frontier Foundation (EFF) has interpreted the scope of DOJ's potential collection ability to include: the numbers a phone calls and from which it receives incoming calls; the starting and ending time of each call; the duration of each call; whether each call was connected or went to voicemail; and (although a disputed, controversial use of the Pen/Trap authority) "post-cut-through dialed digits" (digits dialed after a call is connected, such as a banking PIN or a prescription refill number).[67]

Enacted seven years after *Smith v. Maryland*, the Pen/Trap statute was a congressional response to the Supreme Court's holding that the Fourth Amendment does not apply to transactional information associated with making phone calls. The USA PATRIOT Act then expanded the government's ability to use Pen/Traps to acquire real-time transactional information about email,[68] which DOJ asserts, once again, could encompass almost all non-content information in a communication[69] and EFF explains may include: addresses of sent and received email, the time each email is sent or received, the size of each email that is sent or received, and IP (Internet Protocol) addresses to include IP addresses[70] of other computers a target computer exchanges information with, as well as the communications ports and protocols used (which, in turn, can be used to determine the types of communications sent and the types of applications used).[71]

Concerns about how the Pen/Trap statute might facilitate systematic government access to third-party data primarily derive from: (1) the statute's low certification standard, (2) the scope and volume of information that can presumably be collected with a Pen/Trap order, and (3) documented use of the statute to authorize a method of collection that courts granting orders did not realize they were authorizing. To obtain a Pen/Trap order, the government must only certify to a court that the information likely to be obtained is "relevant to an ongoing criminal

66. US Dep't of Justice, Computer Crime and Intellectual Prop. Section, Criminal Div., *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* (3d ed., 2009) at 154 [hereinafter DOJ Manual].

67. See: https://ssd.eff.org/wire/govt/pen-registers. With respect to "post-cut-through dialed digits" or other communications content, the DOJ Manual, citing 18 U.S.C. § 3121(c), instructs that the "government must also use 'technology reasonably available to it' to avoid recording or decoding the contents of any wire or electronic communications . . . . Where there is no way to avoid the inadvertent collection of content though the use of reasonably available technology, DOJ policy requires that the government may not use any inadvertently collected content in its investigation." See DOJ Manual, above note 66 at 155–56.

68. See Public Law 107-56, Sec. 216 (Oct. 26, 2001).

69. See DOJ Manual, above note 66.

70. See *In re* Application of United States, 416 F. Supp. 2d 13, 18 (D.D.C. 2006) (approving Internet Pen/Trap order seeking specified non-content information, such as originating IP addresses).

71. See https://ssd.eff.org/wire/govt/pen-registers.

investigation."[72] Insofar as this certification does not require a court to *evaluate* any facts to determine if the information is likely to be relevant to an ongoing criminal investigation, there is no meaningful judicial oversight. Moreover, there is no limitation on the scope of information collected in a particular investigation, whether with single or multiple Pen/Trap orders. Although certain types of investigations require a broad collection of phone and email transactional information, if there is no meaningful judicial oversight regarding the scope of such collection, the potential for unmediated government access to third-party data looms large.

B. Financial Data: Right to Financial Privacy Act, NSLs

Just as the SCA and the Pen/Trap provisions of ECPA were a congressional response to the lack of Fourth Amendment protections afforded to electronic communications in the possession of third parties, Congress enacted the Right to Financial Privacy Act[73] in 1978, two years after the *Miller* decision, where Supreme Court held that there was no reasonable expectation of privacy in documents voluntarily conveyed to banks and exposed to their employees in the ordinary course of business. The statute provides that federal agencies may not access the financial records of a customer of a financial institution without that customer's consent, a search warrant, an administrative subpoena, a judicial subpoena, or a "formal written request."[74] The statute is subject to a number of exceptions, including disclosures required under other federal statues or rules. Moreover, the Act does not apply when the federal government obtains financial information from third parties that are *not* financial institutions, nor does it restrict disclosures to state or local governments or other private entities.[75] The Act also contains one of the five NSL authorities,[76] permitting the government to compel financial institution customer records in foreign intelligence investigations (for example, open and closed checking and savings accounts, transactions records from banks, private bankers, credit unions, thrift institutions, credit card companies, insurance companies, etc.).

After the September 11th attacks, it was reported that the government gained unprecedented access to the world's banking databases through a relationship with the Society for Worldwide Interbank Financial Telecommunications (SWIFT), a Belgium-based cooperative that serves as "the central nervous system of international banking."[77] At that time, SWIFT purportedly carried information for nearly 8,000 financial institutions, which conducted up to 12.7 million

72. 18 U.S.C. § 3122(b)(2) (2012).

73. 12 U.S.C. §§ 3401–3422 (2012).

74. 12 U.S.C. § 3402 (2012).

75. 12 U.S.C. §§ 3401(1)–(3) (2012).

76. 12 U.S.C. § 3414 (2012).

77. Josh Meyer and Greg Miller, "US Secretly Tracks Global Bank Data," *L.A. Times* (June 23, 2006), at A1.

financial transactions a day.[78] Although SWIFT executives insisted that their organization's participation had not been voluntary but, rather, was in compliance with US government NSLs, SWIFT's willing cooperation appeared to represent a major departure from typical practices.[79] The SWIFT example illustrates how the government may use statutory authorities to acquire vast amounts of information—in this case purportedly with mere NSLs—such that the information collection might be characterized as systematic government access *aided by* the cooperation of a "friendly" third party (likely due to circumstances surrounding the September 11th attacks).

Additional mystery regarding government access to financial data surrounds a government practice referred to as "hotwatch" orders, "issued pursuant to the All Writs Act. Such orders direct a credit card issuer to disclose to law enforcement each subsequent credit card transaction effected by a subject of [an] investigation immediately after the issuer records that transaction."[80] A DOJ presentation obtained through a Freedom of Information Act (FOIA) request suggests that law enforcement's preferred way of obtaining a "hotwatch" order is to contact the credit card security department and provide that department with an administrative subpoena and a court order for "non-disclosure."[81] Although the scope of information obtained from "hotwatch" orders is unclear, it is important to note that the data are provided in "real time" and presumably will include information about the subject of the transaction (i.e., the type of purchase made or service conducted) that, in turn, can also reveal the location of the user at the time she made the transaction (in the case of a "brick and mortar" business or institution). Indeed, the DOJ presentation characterizes credit card "hotwatch" orders as "real time tracking."[82]

C. Other Records in the Possession of Third Parties

As previously noted, data not protected by the Constitution or regulated by statute requiring a court order for its production can be compelled by the government with "low level" process (i.e., subpoena or NSL) or even provided voluntarily to the government without any legal process. Such lack of regulation can potentially facilitate the kind of reported public-private partnerships with Western Union, FedEx, and major airlines seen in the aftermath of the September

78. S*ee* Michaels, above note 23 at 916.

79. Ibid. at 917.

80. DOJ Memorandum to the Honorable James Orenstein, October 11, 2005 at 9, https://www.eff.org/document/government-reply-eff-brief.

81. See Christopher Soghoian, "DOJ's "Hotwatch" Real-Time Surveillance of Credit Card Transactions," *Slight Paranoia Blog* (December 2, 2010), http://paranoia.dubfire.net/2010/12/dojs-hotwatch-real-time-surveillance-of.html.

82. Ibid.

11th attacks. Shortly after the attacks, then CIA director George Tenet invited Western Union executives to his office to persuade them to "be patriots."[83] Some of the information provided by Western Union following the exchange may have been disclosed in response to subpoenas, whereas some may have been provided though "informal cooperation" rather than legal compulsion.[84] Since September 11th, FedEx has also reportedly "placed its databases at the government's disposal" and "demonstrated a willingness to open suspicious packages at the government's informal request (i.e. without a warrant)."[85] Major airlines were also reported to have turned over extensive amounts of passenger data to the government because "they thought they were obliged to do so."[86] Third-party desire and willingness to cooperate with the government post-September 11th in the fashion described is understandable and, moreover, legal. Indeed, government outreach to establish good working relationships with industry is often necessary and desirable. But if industry at large (such as supermarkets, hotels, travel agencies, etc.) routinely discloses information without minimal process, even when permitted under the law, then the government gets closer to achieving indiscriminate, systematic access to private-sector data.

V. CONCLUSION

DARPA's TIA program foreshadowed the potential of how machine learning techniques, when trained on the right data sets, might assist in "predictive policing"[87] and predictive intelligence efforts. Given this potential, the government's desire and need for more private-sector data will only continue to increase. Notwithstanding efforts to expand, contract, or more specifically regulate government access to third-party data, the ongoing public debates in this area must be informed by sufficient information about the government's interpretation and use of its criminal and foreign intelligence authorities, including government "informal" practices.

83. See Michaels, above note 23 at 914.

84. Ibid.

85. Ibid. at 915.

86. Ibid. at 928.

87. See *generally*, Michael L. Rich, "Machine Learning, Automated Suspicion Algorithms, and the Fourth Amendment," 164 *U. Penn. L.R.* 871 (2016).

9

Systematic Government Access to Private-Sector Data in the United States II

The US Supreme Court and Information Privacy

FRED H. CATE AND BETH E. CATE*

I. ABSTRACT

The US Supreme Court has written a great deal about "privacy" in a wide variety of contexts. These include what constitutes a "reasonable expectation of privacy" under the Fourth Amendment to the Constitution; privacy rights implicit in, and also in tension with, the First Amendment and freedom of expression; privacy rights the Court has found implied in the Constitution that protect the rights of adults to make decisions about activities such as reproduction, contraception, and the education of their children; and the application of the two privacy exemptions to the Freedom of Information Act (FOIA).

The Court not only uses the term "privacy" in a variety of different settings, but has identified at least three distinct meanings of the term:

1. The Court has found a constitutionally protected right of decisional privacy, generally meaning personal autonomy to make decisions without unwarranted government intervention in certain areas that the Court has concluded implicate "fundamental" individual liberties. These areas include marriage, procreation, contraception, family relationships, child-rearing, and education.
2. In its Fourth Amendment jurisprudence, the Court has provided a specific definition of privacy: whatever one "seeks to preserve as private, even in an area accessible to the public," provided that the individual has an "actual," subjective expectation of privacy and that expectation is

* The authors gratefully acknowledge the excellent research assistance provided by Lindsay Elizabeth Koenings.

Bulk Collection. Fred H. Cate and James X. Dempsey.

"one that society was prepared to recognize as 'reasonable.'" The Court has crafted many exceptions to this right; the most significant for the future of privacy protection is that information disclosed to or held by a third party may not be treated as private.

3. The Court has described both a statutory and constitutional "individual interest in avoiding disclosure of personal matters . . . ." In this context the Court repeatedly has found that even though information has been disclosed to and is held by third parties, this does not eliminate the existence of a lawfully protected privacy interest. This is a far more subtle and contextual view of privacy than the binary view of privacy that the Court has thus far applied in its Fourth Amendment jurisprudence.

II. INTRODUCTION

The US Supreme Court has written a great deal about "privacy" in a wide variety of contexts. Between 1970 and 2016, the Court used the term "privacy" in 645 opinions. In over half (342 opinions) an opinion significantly addressed some aspect of privacy.

The breakdown of those 342 opinions provides interesting insight into the contexts in which the Supreme Court concerns itself with privacy. (See Figure 9.1) Not surprisingly, most of these opinions addressed privacy rights that the Court has found are protected by the US Constitution. The largest single category by far was cases involving the "reasonable expectation of privacy" under the Fourth Amendment to the Constitution (220, or 64 percent of opinions). Opinions involving the First Amendment and freedom of expression issues accounted for 17 percent (59), a large portion of which involved reviews of obscenity regulations and prosecutions. Seventeen opinions (5 percent) involved what the Court has come to call "decisional privacy," namely the privacy rights the Court has found implied in the Constitution that protect the rights of adults to make

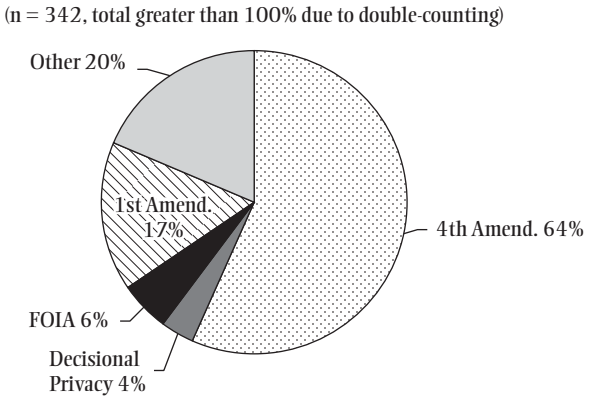

Figure 9.1 U.S. Supreme Court Cases Involving Privacy 1970–2016.

decisions about activities such as reproduction, contraception, and the education of their children. Highly controversial, decisions handed down by the Court in the last four years have affirmed by a bare majority a right to decisional privacy that extends to choosing civil marriage with a same-sex partner, and reaffirmed the right to choose abortion before the fetus is viable outside the womb.

Aside from constitutional privacy issues, 22 (6 percent) of the Court's opinions involving privacy addressed the application of the two privacy exemptions to the FOIA. Seventy opinions (20 percent) did not fit within any discrete category. The total number of opinions does not add up to 342 (or the total percentages to 100 percent) because a number of opinions addressed more than one aspect of privacy.

The breadth of the Court's constitutional (as opposed to statutory) privacy jurisprudence reflects the fact that even though privacy is not explicitly protected in the Constitution, the Court has interpreted many of the amendments constituting the Bill of Rights to provide protection to a variety of elements of privacy. These include an individual's right to be free from unreasonable searches and seizures by the government;[1] the right to make decisions about contraception,[2] abortion,[3] and other issues of "fundamental" individual liberty interests such as marriage, procreation, child-rearing, and education;[4] the right not to disclose certain information to the government;[5] the right to associate free from government intrusion;[6] and the right to enjoy one's own home free from intrusion by the government,[7] sexually explicit mail[8] or radio broadcasts,[9] or other intrusions.[10]

In this chapter we provide an overview of the Supreme Court's treatment of privacy, first in its constitutional exposition, and second in its statutory interpretation of FOIA, with brief comments on its recent treatment of other privacy-protecting statutes. We conclude with a brief analysis of the apparent inconsistency within the Court's jurisprudence of what constitutes a "reasonable expectation" of privacy and some thoughts on where the Court's privacy jurisprudence may be heading.[11]

1. *Katz v. United States*, 389 U.S. 347 (1967).

2. *Griswold v. Connecticut*, 381 U.S. 479 (1965).

3. *Roe v. Wade*, 410 U.S. 113 (1973).

4. Ibid. at 152–53.

5. *Whalen v. Roe*, 429 U.S. 589 (1977).

6. *NAACP v. Alabama*, 357 U.S. 449 (1958).

7. *Stanley v. Georgia*, 394 U.S. 557 (1969).

8. *Rowan v. Post Office*, 397 U.S. 728 (1970).

9. *Federal Commc'ns Comm'n v. Pacifica Found.*, 438 U.S. 726 (1978).

10. *Frisby v. Schultz*, 487 U.S. 474 (1988); *Carey v. Brown*, 447 U.S. 455 (1980).

11. The Court has little occasion to address common-law privacy protections, which typically apply via state tort law, unless it must consider whether they are pre-empted by federal statutory or constitutional provisions. In 2011, for example, the Court held that the First

III. CONSTITUTIONAL SOURCES OF A PRIVACY RIGHT

Fundamental rights in the United States are articulated in the federal Constitution. Two features of those rights are central to understanding the role of the Constitution in protecting privacy. First, rights articulated in the Constitution generally are protected only against government action.[12] All constitutional rights—whether to speak freely, confront one's accusers, be tried by a jury of one's peers—regulate the public, but not the private, sector. In the absence of state action, therefore, constitutional rights are not implicated in questions surrounding privacy.[13] The second significant characteristic of constitutional rights is that they are generally "negative"; they do not obligate the government to do anything, but rather to refrain from taking actions that abridge constitutionally protected rights.

A. Fundamental Rights of Personal Decision-Making

The US Supreme Court's most controversial constitutional right to privacy has developed within a series of cases involving decision-making about contraception, abortion, and other personal issues. In 1965, the Supreme Court decided in *Griswold v. Connecticut* that an 80-year-old Connecticut law forbidding the use of contraceptives violated the constitutional right to "marital privacy."[14] The justices voting to strike down the law identified a variety of constitutional sources for this right. Justice Douglas, writing the opinion for the Court, drew on notions of privacy implied within several provisions of the Bill of Rights:

> Various guarantees create zones of privacy. The right of association contained in the penumbra of the First Amendment is one . . . . The Third Amendment in its prohibition against the quartering of soldiers "in any house" in time of

Amendment protected protesters at a military funeral against a state tort law charge of intentional infliction of emotional distress. *Snyder v. Phelps*, 562 U.S. 443 (2011).

12. Only the Thirteenth Amendment, which prohibits slavery, applies directly to private parties. *Clyatt v. United States*, 197 U.S. 207, 216–20 (1905).

13. Although state action is usually found when the state acts toward a private person, the Supreme Court has also found state action when the state affords a legal right to one private party that impinges on the constitutional rights of another, see *New York Times Co. v. Sullivan*, 376 U.S. 264, 265 (1964), and in rare cases when a private party undertakes a traditionally public function, see *Marsh v. Alabama*, 326 U.S. 501 (1946), or when the activities of the state and a private entity are sufficiently intertwined to render the private parties' activities public, see *Evans v. Newtown*, 382 U.S. 296 (1966).

14. *Griswold v. Connecticut*, 381 U.S. 479 (1965). The Court later extended constitutional rights of access to contraception to unmarried individuals, see *Eisenstadt v. Baird*, 405 U.S. 438, 453 (1972) ("[i]f the right of privacy means anything, it is the right of the individual, married or single, to be free from unwarranted governmental intrusion into matters so fundamentally affecting a person as the decision whether or not to bear or beget a child").

> peace without the consent of the owner is another facet of that privacy. The Fourth Amendment explicitly affirms the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." The Fifth Amendment in its Self-Incrimination Clause enables the citizen to create a zone of privacy which government may not force him to surrender to his detriment. The Ninth Amendment provides: "The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people."[15]

Justice Douglas wrote that the "specific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance."[16] Justices Goldberg and White, in concurring opinions, focused on the Ninth Amendment and wrote that the autonomy of married couples to decide whether or not to have children was a fundamental and traditional right retained by the people. Justice Harlan's concurrence grounded the privacy right in the due process clause of the Fourteenth Amendment,[17] which he believed protected certain "values implicit in the concept of ordered liberty," among them the right of married couples to engage in contraception without interference by the government.

Justice Harlan's reliance on the due process clause emerged in subsequent cases as the dominant view of the constitutional basis for decisional privacy rights. Most controversially, eight years after *Griswold*, the Court, in *Roe v. Wade*, recognized a constitutional privacy right, grounded in due process, that encompasses "a woman's decision whether or not to terminate her pregnancy."[18] The Court looked to "the Fourteenth Amendment's concept of personal liberty and restrictions upon state action. . . ."[19] To guard against the potential for justices to greatly limit the scope of permissible legislative action by transforming their own policy preferences into constitutionally protected "liberties," the Court in *Roe v. Wade* emphasized that the constitutional "guarantee of personal privacy" only includes "personal rights that can be deemed 'fundamental' or 'implicit in the concept of ordered liberty' . . . ."[20] The Court specified that those fundamental rights include activities concerning marriage, procreation, contraception, family relationships, and child-rearing and education.[21] Government regulation of those activities "may be justified only by a 'compelling state interest,'" and

15. Ibid. at 484.

16. Ibid.

17. The Fourteenth Amendment provides, in relevant part: "No State shall make or enforce any law which shall . . . deprive any person of life, liberty, or property, without due process of law . . . ." U.S. Constitution amend. XIV. The Fifth Amendment applies an identical prohibition to the federal government. U.S. Constitution amend. V.

18. 410 U.S. 113, 153 (1973).

19. Ibid.

20. *Roe v. Wade*, 410 U.S. at 152 (quoting *Palko v. Connecticut*, 302 U.S. 319, 325 (1937)).

21. Ibid. at 152–53.

they must be "narrowly drawn to express only the legitimate state interests at stake"[22]—a standard described as "strict scrutiny."

Although the Supreme Court indicated that government intrusion into inherently private areas of personal life would be subject to strict scrutiny, the Court over time has come to apply a lesser form of scrutiny to regulations involving abortion, and to emphasize the importance of balancing privacy with the government's valid regulatory interests.[23] Currently regulations imposed on pregnant women seeking abortions prior to fetal viability will be upheld as long as they do not impose an "undue burden" on access to abortion.[24] The Court has defined an "undue burden" as a regulation that has the "purpose or effect of imposing a substantial obstacle" to getting a pre-viability abortion.

This standard is not without force and meaning. On the final day of its 2015–2016 term, the Court reaffirmed a woman's right to choose abortion pre-viability and in *Whole Woman's Health v. Hellerstedt*,[25] struck down a Texas law that imposed two requirements on abortion providers, purportedly to protect women's health. The Court examined the factual record and approved drawing "common sense" inferences from the facts, finding that the new rules had no demonstrated health benefits while making access to safe abortion considerably more difficult. In doing so the Court served notice that at least with respect to health-based abortion regulations, it would take a direct and close look at the evidence and not defer to legislative characterizations or judgments about a law's impact on this privacy right.

The Court's decisional privacy jurisprudence generally does not concern issues of informational privacy.[26] In the abortion context, however, the Court has addressed certain rules that implicate informational privacy concerns. For a number of years following *Roe v. Wade*, the Court struck down state laws that required pregnant women, including minors, to obtain spousal or parental consent to abortion (at least in the absence of an alternative when parental consent

22. Ibid. at 155.

23. *Planned Parenthood of Southeastern Pennsylvania v. Casey*, 505 U.S. 833 (1992).

24. Ibid. After viability a state's interest in preserving the potentiality of the life of the fetus outweighs the mother's privacy rights and the state may ban abortion altogether except when needed to save the life or protect the health of the mother. *Stenberg v. Carhart*, 530 U.S. 914 (2000). But see *Gonzales v. Carhart*, 550 U.S. 124 (2007) (rejecting facial challenge to federal Partial-Birth Abortion Act of 2003, which does not contain an exception to the ban on partial-birth abortions to protect a woman's health, but not ruling out challenges to individual applications of the law).

25. 579 U.S. ___ (2016).

26. Decisional "privacy" rights are better thought of as rights of personal autonomy, as Justice Ginsburg emphasized in her dissenting opinion on *Gonzales v. Carhart*, 550 U.S. at 172 ("legal challenges to undue restrictions on abortion procedures do not seek to vindicate some generalized notion of privacy; rather, they center on a woman's autonomy to determine her life's course, and thus to enjoy equal citizenship stature.")

is unavailable or inappropriate),[27] and also struck down rules requiring women to receive information about risks and alternatives that the Court found to be designed to deter a woman from having an abortion.[28] In 1992, however, the Court upheld a requirement that abortion patients receive an "informed consent" booklet with information on risks and alternatives, a 24-hour waiting period, and a requirement that minors get the written consent of at least one parent, finding that none of these requirements unduly interfered with the right to access abortion.[29]

In recent years, states have passed additional laws requiring women seeking abortions to be given various types of information—for example, mandatory ultrasounds and fetal heartbeat audio, information on perinatal hospice care for fetuses likely to die shortly after birth, statements about studies showing that fetuses respond to pain stimuli at 20 weeks, and statements that "human physical life begins at conception." Some lower courts struck down, on First Amendment grounds, laws requiring healthcare providers to perform ultrasounds on women seeking abortions and to display and describe their results in detail. The Supreme Court declined to review those rulings. After *Whole Woman's Health* any future attempts to impose informational requirements may be in jeopardy if challengers demonstrate that the information has little to no relevance to making an informed decision about abortion but erects a substantial hurdle to getting an abortion.

As with abortion rights, the Court's decisions involving same-sex relationships and marriage have at once restated the importance of the constitutional liberty at stake and employed less than strict scrutiny to judge laws abridging that liberty. In *Lawrence v. Texas*,[30] the Court held that a state law criminalizing private sexual conduct between consenting same-sex couples failed to pass muster under the due process clause. Although affirming that the freedom to make intimate personal choices is central to the liberty protected by due process, the Court effectively employed a much lower standard of review than strict scrutiny and found that the state law was not rationally related to furthering any legitimate government interest.[31] A decade later, in striking down federal and state bans on same-sex marriage, the Court once again used an amorphous but lesser standard, and focused on a form of privacy right grounded in dignity—the right to choose one's partner and to have that choice respected by the government.

27. For example, *Planned Parenthood of Central Missouri v. Danforth*, 428 U.S. 52 (1976); *Bellotti v. Baird,* 443 U.S. 622 (1979); *City of Akron v. Akron Center for Reproductive Health,* 462 U.S. 416 (1983).

28. *Akron*, supra note 28; *Thornburgh v. American College of Obstetricians & Gynecologists*, 476 U.S. 747 (1986).

29. *Casey*, 505 U.S. 833.

30. 539 U.S. 558 (2003).

31. Ibid. at 573–74, 577–78.

B. Protection against Government Disclosure of Personal Matters

The Supreme Court has addressed privacy in the context of a general constitutional right against government-compelled "disclosure of personal matters."[32] In 1977, the Supreme Court decided *Whalen v. Roe*, a case involving a challenge to a New York statute requiring that copies of prescriptions for certain drugs be provided to the state, on the basis that the requirement would infringe patients' privacy rights. Echoing *Griswold*, the unanimous Court wrote that the constitutionally protected "zone of privacy" included "the individual interest in avoiding disclosure of personal matters . . . ."[33]

Nevertheless, having found this new privacy interest in nondisclosure of personal information, the Court did not apply strict scrutiny, a standard typically reserved for cases involving "fundamental" interests. Instead, applying a lower level of scrutiny, the Court found that the statute did not infringe the individuals' interest in nondisclosure.[34] The Court also explicitly rejected the application of the Fourth Amendment right of privacy to broad government data collection programs for regulatory purposes, writing that Fourth Amendment cases "involve affirmative, unannounced, narrowly focused intrusions."[35] The Court has never decided a case in which it found that a government regulation or action violated the constitutional privacy right recognized in *Whalen*.[36]

In *Whalen*, however, the Court provided a comparatively subtle and modern understanding of what "privacy" means:

> We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files. The collection of taxes, the distribution of welfare and social security benefits, the supervision of public health, the direction of our Armed Forces, and the enforcement of the criminal laws all require the orderly

32. *Whalen v. Roe*, 429 U.S. 589, 599–600 (1977).

33. Ibid.

34. Ibid. at 603–04.

35. Ibid. at 604, n.32.

36. Several federal appeals courts have relied on *Whalen* to find that a government regulation or action violated an individual's constitutional privacy right in nondisclosure of personal information. See, e.g., *Tavoulareas v. Washington Post Co.*, 724 F.2d 1010 (D.C. Cir. 1984); *Barry v. City of New York*, 712 F.2d 1554 (2d Cir. 1983); *Schacter v. Whalen*, 581 F.2d 35 (2d Cir. 1978); *Doe v. Southeastern Pennsylvania Transportation Authority*, 72 F.3d 1133 (3d Cir. 1995); *United States v. Westinghouse Electric Corp.*, 638 F.2d 570 (3d Cir. 1980); *Plante v. Gonzalez*, 575 F.2d 1119 (5th Cir. 1978); and *Doe v. Attorney General*, 941 F.2d 780 (9th Cir. 1991). Courts in the Fourth and Sixth Circuits, in contrast, have severely limited the scope of the *Whalen* nondisclosure privacy right, see *Walls v. City of Petersburg*, 895 F.2d 188, 192 (4th Cir. 1990), and *J.P. v. DeSanti*, 653 F.2d 1080 (6th Cir. 1981). Taking *Whalen*'s lead, those courts that have relied on the right of nondisclosure have applied only intermediate scrutiny, instead of the strict scrutiny typically used to protect fundamental constitutional rights. See *Doe v. Attorney General*, 941 F.2d at 796.

> preservation of great quantities of information, much of which is personal in character and potentially embarrassing or harmful if disclosed. The right to collect and use such data for public purposes is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures.[37]

The Court recognized that "in some circumstances that duty [to avoid unwarranted disclosures] arguably has its roots in the Constitution."[38] The New York statute did not violate the Constitution because it "evidence[d] a proper concern with, and protection of, the individual's interest in privacy."[39] The Court concluded: "We therefore need not, and do not, decide any question which might be presented by the unwarranted disclosure of accumulated private data—whether intentional or unintentional—or by a system that did not contain comparable security provisions."[40]

C. First Amendment

The Court has identified a number of privacy interests implicit in the First Amendment.[41] For example, in *NAACP v. Alabama*,[42] the Court struck down an Alabama ordinance requiring the NAACP to disclose its membership lists, finding that such a requirement constituted an unconstitutional infringement on NAACP members' First Amendment right of association.[43]

In *Stanley v. Georgia*,[44] the Court explicitly linked privacy and free expression by identifying the mutual interests they serve. The Court overturned a conviction under Georgia law for possessing obscene material in the home. Although the "[s]tates retain broad power to regulate obscenity," Justice Marshall wrote for the unanimous Court, "that power simply does not extend to mere possession by the individual in the privacy of his own home."[45] The Court based its decision squarely on the First Amendment, which the Court found included the "right to be free, except in very limited circumstances, from unwanted governmental intrusion into one's privacy."[46]

37. *Whalen,* 429 U.S. at 605.

38. Ibid.

39. Ibid.

40. Ibid. at 605–06.

41. "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceable to assemble . . . ." U.S. Constitution amend. I.

42. 357 U.S. 449 (1958).

43. Ibid. at 464–65.

44. 394 U.S. 557 (1969).

45. Ibid. at 568.

46. Ibid. at 564.

A 2013 case posed the link between privacy and First Amendment rights in the digital age, even more starkly than *Stanley*. Amnesty International and other lawyers, activists, and journalists communicating with clients and witnesses abroad claimed that the National Security Agency's (NSA) reportedly sweeping surveillance of phone and email communications under an amended foreign intelligence law had "chilled" their speech, silenced witnesses, and caused plaintiffs to travel abroad to have privileged and confidential conversations.

In a controversial 5-4 decision in *Clapper v. Amnesty International*,[47] the Court dodged plaintiffs' claims, finding that plaintiffs lacked standing to sue because they could not show with sufficient certainty that the NSA, under the relevant law, would in fact monitor their particular communications with foreign contacts. Rejecting evidence suggesting that such monitoring would indeed occur—in particular the NSA's interception of client communications under an earlier and more stringent surveillance law—the majority characterized plaintiffs' concerns as "speculation" and (in the case of current travel costs) "simply the product of their fear of surveillance," neither of which could establish standing.

Importantly, the *Clapper* majority acknowledged that proven surveillance can raise significant First Amendment issues, and the national security context of the surveillance in question goes a long way toward explaining the majority's reluctance to permit the plaintiffs' claims to proceed to discovery. More often, however, the Court identifies privacy as an interest in tension with the First Amendment's protection for freedom of expression and press. In *Breard v. City of Alexandria*,[48] for example, the Court upheld an ordinance prohibiting solicitation of private residences without prior permission. The Court found in the First Amendment's free speech guarantee an implicit balance between "some householders' desire for privacy and the publisher's right to distribute publications in the precise way that those soliciting for him think brings the best results."[49]

The Court has invoked this same implied balancing test in numerous other cases. In *Kovacs v. Cooper*,[50] the Court upheld a Trenton, New Jersey, ordinance prohibiting the use of sound trucks and loudspeakers:

> [t]he unwilling listener is not like the passer-by who may be offered a pamphlet in the street but cannot be made to take it. In his home or on the street he is practically helpless to escape this interference with his privacy by loudspeakers except through the protection of the municipality.[51]

In *Rowan v. U.S. Post Office*,[52] the Court upheld a federal statute that permitted homeowners to specify that the Post Office not deliver to their

47. *Clapper v. Amnesty Int'l USA*, 568 U.S. ___, 133 S. Ct. 1138 (2013).

48. 341 U.S. 622 (1951).

49. Ibid. at 644.

50. 336 U.S. 77 (1949).

51. Ibid. at 86–87.

52. 397 U.S. 728 (1970).

homes "erotically arousing" and "sexually provocative" mail. In *Federal Communications Commission v. Pacifica Foundation*,[53] the Court allowed the Federal Communications Commission to sanction a radio station for broadcasting "indecent" programming, finding that "the individual's right to be left alone plainly outweighs the First Amendment rights of an intruder."[54] In *Frisby v. Schultz*,[55] the Court upheld a local ordinance that banned all residential picketing, writing that the home was "the one retreat to which men and women can repair to escape from the tribulations of their daily pursuits"[56] and "the last citadel of the tired, the weary, and the sick."[57] In *Carey v. Brown*,[58] the Court wrote that "the State's interest in protecting the well-being, tranquility, and privacy of the home is certainly of the highest order in a free and civilized society."[59]

When privacy rights conflict with free expression rights before the Court, the latter usually prevail. When information is true and obtained lawfully, the Court has repeatedly held that the state may not restrict its publication without showing a very closely tailored, compelling governmental interest. Under this requirement, the Court has struck down laws restricting the publication of confidential government reports,[60] and of the names of judges under investigation,[61] juvenile suspects,[62] and rape victims.[63] Moreover, there can be no recovery for invasion of privacy unless the information published is highly offensive to a reasonable person and either false[64] or not newsworthy.[65] And the Court

53. 438 U.S. 726 (1978).

54. Ibid. at 748.

55. 487 U.S. 474 (1988).

56. Ibid. at 484 (quoting *Carey*, 447 U.S. at 455).

57. Ibid. (quoting *Gregory v. City of Chicago,* 394 U.S. 111, 125 (1969) (Black, J., concurring)).

58. 447 U.S. 455 (1980). The Court in *Carey* struck down an Illinois ordinance that generally prohibited residential picketing but permitted certain labor picketing; the Court rejected the state's argument that the law properly balanced privacy interests with special solicitude for labor-related speech, emphasizing that picketing rules designed to protect privacy should be drawn without regard to the content of the speech. Ibid. at 470–71.

59. Ibid. at 471.

60. *New York Times Co. v. United States*, 403 U.S. 713 (1971).

61. *Landmark Communications, Inc. v. Virginia*, 435 U.S. 829 (1978).

62. *Smith v. Daily Mail Publishing Co.*, 443 U.S. 97 (1979).

63. *Florida Star v. B.J.F.,* 491 U.S. 524 (1989); *Cox Broadcasting Corp. v. Cohn*, 420 U.S. 469 (1975).

64. *Cantrell v. Forest City Publishing Co.*, 419 U.S. 245 (1974).

65. *Florida Star*, 491 U.S. 254.

has accorded a variety of procedural protections to all expression, whether true or false.[66]

The Court recently revisited the balance between freedom of expression and privacy in *Sorrell v. IMS Health Inc.*[67] *Sorrell* involved a First Amendment challenge to a Vermont law prohibiting the sale, disclosure, or use of prescriber-identifiable information in pharmacy and related records for use in marketing or promoting prescription drugs. The law was aimed at combating expensive, targeted "detailing" campaigns by drug representatives using prescribed-specific data obtained from pharmacies, insurers, and so on via data mining companies; the state also argued, however, that the law was designed to safeguard prescriber privacy.[68]

Justice Kennedy, writing for the six-justice majority, assumed that "for many reasons, physicians have an interest in keeping their prescription decisions confidential," and strongly suggested that a state law that closely guarded the confidentiality of such information and allowed its disclosure and use "in only a few narrow and well justified circumstances" would be upheld against the type of challenge brought by the pharmaceutical companies.[69] The majority concluded, however, that prescriber data were widely available without prescriber consent to others, including "counterdetailers" promoting non-prescription drugs, and therefore the law was insufficiently tailored to serve its stated privacy goals.[70]

Strikingly, though, Justice Kennedy ended the majority opinion with a strong statement—one that echoes to some extent the concluding observations in *Whalen*, above—about the importance of privacy and the risks posed to it by technology-enabled access to and use of personal data held by the government or elsewhere:

> The capacity of technology to find and publish personal information, including records required by the government, presents serious and unresolved issues with respect to personal privacy and the dignity it seeks to secure. In considering how to protect those interests, however, the State cannot engage in content-based discrimination to advance its own side of a debate.

66. *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242 (1986) (requiring that the standard for summary judgment motions take into account the plaintiff's burden at trial); *Bose Corp. v. Consumers Union*, 466 U.S. 485 (1984) (requiring independent appellant review).

67. 564 U.S. 552 (2011).

68. No patient-identifiable information was involved the disclosures.

69. 564 U.S. at 560.

70. The dissent argued that the majority overstated the access by others to prescriber data, citing state professional responsibility rules limiting disclosure of such data, the similarity of the exceptions in Vermont's law to exceptions in the major federal health privacy law (the Health Insurance Privacy and Accountability Act, or HIPAA), and the absence of record evidence indicating the widespread use of prescriber data for counterdetailing. Ibid. at 580 (Breyer, J., dissenting).

> If Vermont's statute provided that prescriber-identifying information could not be sold or disclosed except in narrow circumstances then the State might have a stronger position. Here, however, the State gives possessors of the information broad discretion and wide latitude in disclosing the information, while at the same time restricting the information's use by some speakers and for some purposes, even while the State itself can use the information to counter the speech it seeks to suppress. *Privacy is a concept too integral to the person and a right too essential to freedom to allow its manipulation to support just those ideas the government prefers.*[71]

D. Fourth Amendment

One of the colonists' most potent grievances against the British government was its use of general searches. The hostility to general searches found powerful expression in the Fourth Amendment:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[72]

1. Framework

The Fourth Amendment does not purport to keep the government from conducting searches or seizing personal information. It only prohibits "unreasonable" searches and seizures, but is silent about what makes a search or seizure "unreasonable." In 1886, the Supreme Court first applied the term "priva[cy]" to the interests protected by the Fourth Amendment,[73] and for 80 years focused its Fourth Amendment jurisprudence on whether a search required government officials to trespass on private property. In *Olmstead v. United States*,[74] for example, five of the nine justices found that wiretapping of telephone wires by federal officials did not constitute a search or seizure as there had been no physical trespass and nothing tangible had been taken.

In 1967, the Court decided *Katz v. United States*,[75] a case involving the constitutionality of federal authorities' use of an electronic listening device attached to the outside of a telephone booth used by Charles Katz, whom the authorities suspected of violating gambling laws. The Court found that this method of gathering evidence infringed on Katz's Fourth Amendment rights, even though his property had not been invaded. The Court wrote that "[t]he Fourth Amendment

71. Ibid. at 580 (emphasis added).

72. U.S. Constitution amend. IV.

73. *Boyd v. United States*, 116 U.S. 616, 625–26 (1886).

74. 277 U.S. 438 (1928).

75. 389 U.S. 347 (1967).

protects people not places," and therefore applies to whatever one "seeks to preserve as private, even in an area accessible to the public . . . ."[76]

In his concurrence, Justice Harlan introduced what was later to become the Court's test for what was "private" within the meaning of the Fourth Amendment.[77] Justice Harlan wrote that the protected zone of Fourth Amendment privacy was defined by the individual's "actual," subjective expectation of privacy, and the extent to which that expectation was "one that society was prepared to recognize as 'reasonable.' "[78] The Court adopted that test for determining what was "private" within the meaning of the Fourth Amendment in 1968 and has applied it with somewhat uneven results ever since.[79] The Court has found "reasonable" expectations of privacy in homes,[80] businesses,[81] sealed luggage and packages,[82] and even drums of chemicals,[83] but no "reasonable" expectations of privacy in voice or writing samples,[84] phone numbers,[85] conversations recorded by concealed microphones,[86] and automobile passenger compartments,[87] trunks,[88] and glove boxes.[89]

The Supreme Court interprets the Fourth Amendment generally to require that searches be conducted only with a warrant issued by a court, even though this is not a requirement contained in the amendment itself.[90] For a court to issue a warrant, the government must show "probable cause" that a crime has been or is likely to be committed and that the information sought is germane to that crime.[91] The Court also generally requires that the government provide the subject of a search with contemporaneous notice of the search.[92]

76. Ibid. at 351.

77. Ibid. at 360–61 (Harlan, J., concurring).

78. Ibid. at 361 (Harlan, J., concurring).

79. *Terry v. Ohio*, 392 U.S. 1 (1968).

80. *Camara v. Municipal Court*, 387 U.S. 523 (1967).

81. *G.M. Leasing Corp. v. United States*, 429 U.S. 338 (1977).

82. *United States v. Chadwick*, 433 U.S. 1 (1977); *Arkansas v. Sanders*, 442 U.S. 753 (1979); *Walter v. United States*, 447 U.S. 649 (1980).

83. *United States v. Knotts*, 460 U.S. 276 (1983).

84. *United States v. Dionisio*, 410 U.S. 1 (1973).

85. *Smith v. Maryland*, 442 U.S. 735 (1979).

86. *United States v. White*, 401 U.S. 745 (1971).

87. *New York v. Belton*, 453 U.S. 454 (1981).

88. *United States v. Ross*, 456 U.S. 798 (1982).

89. *South Dakota v. Opperman*, 428 U.S. 364 (1976).

90. Akihl Reed Amar, *The Constitution and Criminal Procedure* 3–4 (1997).

91. 68 *American Jurisprudence* 2d, Searches and Seizures § 166 (1993).

92. *Richards v. Wisconsin*, 520 U.S. 385 (1997).

The Fourth Amendment's protection, although considerable, is not absolute. The Supreme Court has carved out a number of exceptions to the warrant requirement; for example, warrants are not required to search or seize items in the "plain view" of a law enforcement officer,[93] for searches that are conducted incidental to valid arrests,[94] for searches that serve "special needs" unrelated to law enforcement (e.g., warrantless drug tests of high school athletes and railway employees),[95] and for searches specially authorized by the attorney general or the president involving foreign threats of "immediate and grave peril" to national security.[96]

Moreover, the Supreme Court interprets the Fourth Amendment to apply only to the *collection* of information, not its *use*. Even if information is obtained in violation of the Fourth Amendment, the Supreme Court has consistently found that the Fourth Amendment imposes no independent duty on the government to refrain from using it. "The Fourth Amendment contains no provision expressly precluding the use of evidence obtained in violation of its commands, and an examination of its origin and purposes makes clear that the use of fruits of a past unlawful search or seizure '[works] no new Fourth Amendment wrong.'"[97]

Under the Court's "exclusionary rule," illegally seized data may still be used if the government agent acted in good faith,[98] to impeach a witness,[99] or in other settings in which the link between the unconstitutional conduct and the discovery of the data is "too attenuated to justify suppression"[100] or "the officer committing the unconstitutional search or seizure" has "no responsibility or duty to, or agreement with, the sovereign seeking to use the evidence."[101] Citing the significant societal costs imposed by excluding evidence relevant to a prosecution, the Court suppresses the use of information obtained in violation of the Fourth Amendment only when doing so would have deterred the conduct of the government employee who acted unconstitutionally when collecting the information.

So, for example, the Court has allowed records illegally seized by criminal investigators to be used by tax investigators, on the basis that restricting the subsequent

93. *Coolidge v. New Hampshire*, 403 U.S. 443 (1971).

94. *United States v. Edwards*, 415 U.S. 800 (1974).

95. *Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646 (1995); *Skinner v. Railway Labor Executives' Ass'n.*, 489 U.S. 602 (1989).

96. 68 *American Jurisprudence* 2d, Searches and Seizures § 104 (1993).

97. *United States v. Leon*, 468 U.S. 897, 906 (1984).

98. Ibid. (quoting *United States v. Calandra*, 414 U.S. 338, 354 (1974)); see also *Utah v. Strieff*, 579 U.S. ___ (2016).

99. *Walder v. United States*, 347 U.S. 62 (1954).

100. *Utah,* 579 U.S. ___.

101. *United States v. Janis*, 428 U.S. 433, 455 (1975).

use would not deter the original unconstitutional conduct.[102] Protecting privacy is not a consideration. The Court wrote in 1974 that the exclusionary rule operates as "a judicially created remedy designed to safeguard Fourth Amendment rights generally through its deterrent effect, rather than a personal constitutional right of the party aggrieved."[103] If the Court finds no independent Fourth Amendment basis for restricting the use of illegally obtained information, obviously the Court does not apply the Fourth Amendment to restrict the use of lawfully obtained information. The Fourth Amendment today thus poses no limit on the government's use of lawfully seized records, and in the case of unlawfully seized material restricts its use only to the extent necessary to provide a deterrent for future illegal conduct.

2. The *Miller* Exclusion of Third-Party Records

The Supreme Court held in 1976 in *United States v. Miller*[104] that there can be no reasonable expectation of privacy in information shared with a third party. The case involved canceled checks, to which, the Court noted, "respondent can assert neither ownership nor possession."[105] Such documents "contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business,"[106] and therefore the Court found that the Fourth Amendment is not implicated when the government sought access to them:

> The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government. This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.[107]

The Court's decision in *Miller* is remarkably sweeping. The bank did not just happen to be holding the records the government sought. Instead, the Bank Secrecy Act required (and continues to require) banks to maintain a copy of every customer check and deposit for six years or longer.[108] The government thus compelled the bank to store the information, and then sought the information from the bank on the basis that as the bank held the data, there could not be any reasonable expectation of privacy and the Fourth Amendment therefore did not

102. Ibid.

103. *Calandra*, 414 U.S. at 354.

104. *United States v. Miller*, 425 U.S. 435 (1976).

105. Ibid. at 440.

106. Ibid. at 442.

107. Ibid. at 443 (citation omitted).

108. 12 U.S.C. § 1829b(d) (2012); see 425 U.S. at 436; *California Bankers Ass'n v. Shultz*, 416 U.S. 21 (1974).

apply.[109] The Supreme Court was not troubled by this apparent end-run around the Fourth Amendment: "even if the banks could be said to have been acting solely as Government agents in transcribing the necessary information and complying without protest with the requirements of the subpoenas, there would be no intrusion upon the depositors' Fourth Amendment rights."[110]

The Court reinforced its holding in *Miller* in the 1979 case of *Smith v. Maryland*, involving information about (as opposed to the content of) telephone calls.[111] The Supreme Court found that the Fourth Amendment is inapplicable to telecommunications "attributes" (e.g., the number dialed, the time the call was placed, the duration of the call, etc.), because that information is necessarily conveyed to, or observable by, third parties involved in connecting the call.[112] "[T]elephone users, in sum, typically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information; and that the phone company does in fact record this information for a variety of legitimate business purposes."[113]

As a result, under the Fourth Amendment, the use of "pen registers" (to record outgoing call information) and "trap and trace" devices (to record incoming call information) does not require a warrant because they only collect information about the call that is necessarily disclosed to others.[114] As with information disclosed to financial institutions,[115] Congress reacted to the Supreme Court's decision by creating modest statutory requirements applicable to pen registers,[116] but the Constitution does not apply.

Although the *Miller* third-party doctrine and its binary view of privacy have never been overruled and have generally been followed by lower courts, the Supreme Court has declined to apply the doctrine in at least one case in which the Court found extensive and routine involvement of law enforcement in the design and administration of the third party's collection of data. In *Ferguson v. Charleston*,[117] the Court held that a hospital drug-screening program for pregnant women that provided the results to local police without the women's consent, in order to use threats of prosecution to prompt them to seek counseling and treatment, violated the Fourth Amendment. Justice Scalia dissented, noting: "Until today, we have never held—or even suggested—that material which a

109. 425 U.S. at 443.

110. Ibid. at 444.

111. 442 U.S. 735 (1979).

112. Ibid. at 743.

113. Ibid.

114. *Smith v. Maryland*, 442 U.S. 735, 742 (1979).

115. Right to Financial Privacy Act, 12 U.S.C. §§ 3401–3422 (2012).

116. 18 U.S.C. §§ 3121, 1841 (2012).

117. 532 U.S. 67 (2001).

person voluntarily entrusts to someone else cannot be given by that person to the police, and used for whatever evidence it may contain."[118]

Advances in technologies, and the development of new products and services in response to those changes, have significantly expanded the potential impact of *Miller*'s "third party doctrine." Today there are vastly more personal data in the hands of third parties, they are far more revealing, and they are much more readily accessible than was the case in the 1970s. Moreover, for the first time, the government has the practical ability to exploit huge data sets. Nodding to these developments, Justice Sotomayor suggested in 2012 that it may be time for the Court to revisit *Miller* and the third-party doctrine:

> More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks . . . . I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.[119]

3. Recent Developments

The explosive growth in digital data creation, communication, and storage has led the Supreme Court to slowly, and somewhat reluctantly, confront how the Fourth Amendment will apply to protect privacy in this brave new world. The Court's reluctance was evident in *United States v. Jones*,[120] in which four justices (Scalia, Roberts, Kennedy, and Thomas), joined by Justice Sotomayor, found that attaching a GPS device to the bumper of a suspect's car without a warrant constituted an unlawful search *irrespective of any expectations of privacy,* because the government's action constituted a trespass to private property. The Court wrote that "the *Katz* reasonable-expectation-of-privacy test has been *added to*, not *substituted for*, the common-law trespassory test."[121]

Although one could argue that the Court's resurrection of common-law trespass as an independent basis for invoking the Fourth Amendment—after 45 years of reliance on the *Katz* standard—worked an expansion of privacy rights, four concurring justices (Alito, Ginsburg, Breyer, and Kagan) argued that the majority's focus on trespass obscured the real privacy violation by the government: "[T]he Court's reasoning largely disregards what is really important (the use of a GPS for the purpose of long-term tracking) and instead attaches great significance to something that most would view as relatively minor (attaching to the bottom of a car a small, light object that does not interfere in any way

118. Ibid. at 95 (Scalia, J., dissenting).

119. *United States v. Jones*, 565 U.S. __, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring).

120. 565 U.S. __, 132 S. Ct. 945 (2012).

121. Ibid. at 955 (emphasis in original).

with the car's operation)."[122] This, the justices argue, is particularly problematic in the modern age when around-the-clock monitoring of a vehicle's location can be accomplished by activating the vehicle's stolen vehicle detection system or tracking one of the occupant's cell phones.

Justice Scalia, writing for the Court, rejected the need to grapple yet with the thorny issues presented by the increasing ability to monitor human movements without physical contact: "We may have to grapple with these 'vexing problems' in some future case where a classic trespassory search is not involved and resort must be had to *Katz* analysis; but there is no reason for rushing forward to resolve them here."[123]

Likewise, while upholding a "special needs" search of a police officer's work-issued pager messages, the Court bypassed the question of whether the officer had a reasonable expectation of privacy with respect to the pager, and found that even if the officer had a privacy expectation, the scope of the search was reasonable and therefore constitutional. Justice Kennedy, writing for the Court, noted that "[r]apid changes in the dynamics of communication and information transmission are evidence not just in the technology itself but in what society accepts as proper behavior . . . . At present, it is uncertain how workplace norms, and the law's treatment of them, will evolve." He concluded:

> The Court must proceed with care when considering the whole concept of privacy expectations in communications made on electronic equipment owned by a government employer. The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear.[124]

In general the Court has expressed discomfort with using constitutional jurisprudence, rather than statutory rules, to strike the right balance between protecting personal privacy and allowing legitimate governmental access. But even the Court has its limits, and has invoked the Constitution to shut down wanton misuse by the government of predigital doctrine in a strikingly different digital context. In the consolidated cases *Riley v. California* and *United States v. Wurie*, the Court confronted a constitutional challenge to the warrantless search of defendants' cell phone contents following arrest. The Court held unanimously that the warrant exception permitting a "search incident to arrest" did not extend to the contents of a seized cell phone. Emphasizing that modern cell phone owners generally carry with them a massive amount of sensitive and highly revealing personal data, the Court required the police to get a warrant. Chief Justice Roberts, writing for the Court, dismissed the government's attempt to analogize to searching the contents of a seized wallet or pack of cigarettes ("That is like saying a ride on horseback is materially indistinguishable from a flight to the

122. Ibid. at 961 (Alito, J., concurring).

123. Ibid. at 954.

124. *City of Ontario v. Quon*, 560 U.S. 746 (2010).

moon.")[125] Even as the government's extreme position forced a constitutional response, however—or perhaps, precisely for that reason—Justice Alito urged a statutory solution, writing that "it would be very unfortunate if privacy protection in the 21st century were left primarily to the federal courts using the blunt instrument of the Fourth Amendment."[126] As Congress has not yet updated the decades-old legislative framework for privacy in the crime-fighting (as opposed to counterterrorism and intelligence gathering) context, the Court stepped in to impose Fourth Amendment boundaries on the government's remarkable claim to cell phone data.

The Court also rejected the government's claim that officers could at least search the cell phones' call logs without a warrant because the Court had allowed warrantless access to a phone company's pen register in *Smith v. Maryland*. The Court distinguished *Smith* on the grounds that "[t]he Court in that case . . . concluded that the use of a pen register was not a 'search' at all under the Fourth Amendment," and noted too that call logs typically include identifying information along with phone numbers. The Court did not discuss the third-party doctrine, either with respect to call logs or in noting the difficulties presented in cell phone data that are stored in the cloud; the government conceded that the warrant exception for searches incident to arrest did not cover a search of remotely stored files.

The *Riley* and *Wurie* cases, and to some extent *Jones*, reflect an unsurprising judicial rebuff of government assertions of near-limitless investigatory power using the tools and capacity of the digital age. In other recent Fourth Amendment cases, however, a majority of justices has given the government[127] considerable latitude in developing and using broad databases for crime-fighting.

For example, in *Utah v. Strieff*, five justices allowed the use of drug and drug paraphernalia evidence in prosecuting a man who had been detained, and his identity demanded, without the necessary reasonable suspicion. The officer had checked the man's identity against a database and found an outstanding traffic-based arrest warrant; he then searched the man pursuant to the arrest authorized by the warrant, and found the drug evidence.

The Court held that discovery of the outstanding warrant was an "intervening event" that sufficiently attenuated the link between the original unlawful stop and the discovery of the evidence, so that the evidence need not be suppressed. The dissenting justices argued that running a check for outstanding warrants is a standard practice when officers conduct a stop, and there are a tremendous number of outstanding warrants for minor offenses; so, the upshot is a broad power for police to engage in dragnet-style searches of people on the street.

Likewise, in *Maryland v. King*,[128] a five-justice majority upheld a state law requiring DNA cheek-swab tests of persons arrested for violent offenses and entry

125. *Riley v. California*, 573 U.S. ___, 134 U.S. 2473, 2488 (2014).

126. Ibid. at 2497 (Alito, J., concurring).

127. 579 U.S. ___ (2016).

128. 569 U.S. ___ (2013).

of the data into a national database. Justice Kennedy, writing for the Court, reasoned that arrestees have a decreased expectation of privacy and that DNA swabs, like fingerprinting, are valuable for ascertaining the arrestee's identity and making informed decisions about bail and pretrial release. The dissent argued strenuously that the true purpose of the tests is to match DNA against samples in the database in order to solve cold cases, and predicted that soon anyone who is arrested for any reason, great or small, rightly or wrongly, may have his or her DNA taken and placed into a national database for crime-solving purposes.

IV. FOIA

Not all of the Supreme Court's privacy jurisprudence addresses constitutional issues. The federal Freedom of Information Act (FOIA) permits "any person" to obtain access to all federal "agency records," subject to nine enumerated exemptions.[129] Two of the nine exemptions are designed to protect privacy: Exemption 6 precludes disclosure of "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of privacy," and Exemption 7(C) bans release of "records or information compiled for law enforcement purposes [which] . . . could reasonably be expected to constitute an unwarranted invasion of privacy."[130]

The Supreme Court has decided cases interpreting the extent of both exemptions and, in the process, of "privacy." In 1989, the Court decided *U.S. Department of Justice v. Reporters Committee for Freedom of the Press*,[131] which involved press access to law enforcement rap sheets. The press argued that because the information in an individual's rap sheet was compiled from local, publicly available law enforcement and court records, the individual could not assert any privacy right. The Court disagreed, writing: "We reject respondents' cramped notion of personal privacy."[132]

The Court wrote, "both the common law and the literal understandings of privacy encompass the individual's control of information concerning his or her person. In an organised society, there are few facts that are not at one time or another divulged to another."[133] According to the Court, previous disclosure does not automatically remove the privacy interest. Instead, "the extent of the protection accorded a privacy right at common law rested in part on the degree of dissemination of the allegedly private fact and the extent to which the passage of time rendered it private."[134] The Court went on to note that according

129. 5 U.S.C. § 552 (1997).

130. Ibid. § 552(b)(6)–(7)(C).

131. 489 U.S. 749 (1989).

132. Ibid. at 763.

133. Ibid.

134. Ibid.

to "Webster's initial definition, information may be classified as 'private' if it is 'intended for or restricted to the use of a particular person or group or class of persons: not freely available to the public.' "[135]

Based on this nuanced interpretation of privacy, the Court found that FBI rap sheets, even if they contain only material that is held by local law enforcement agencies and courts and that material has been made public, are nevertheless "private" within the meaning of FOIA because of the passage of time, the limited purposes motivating that disclosure, and the fact that rap sheets aggregate otherwise disparate pieces of information.

The Court in *Reporter's Committee* quoted approvingly from a speech by then-justice William Rehnquist: "In sum, the fact that 'an event is not wholly "private" does not mean that an individual has no interest in limiting disclosure or dissemination of the information.' "[136] The Court concluded its analysis: "The privacy interest in a rap sheet is substantial. The substantial character of that interest is affected by the fact that in today's society the computer can accumulate and store information that would otherwise have surely been forgotten long before a person attains age 80, when the FBI's rap sheets are discarded."[137]

Five years later, the Supreme Court relied on its broad definition of privacy from *Reporter's Committee* in a case involving FOIA's other privacy exemption, Exemption 6, which applies to "personnel and medical files and similar files the disclosure of which would constitute a clearly un-warranted invasion of personal privacy."[138] In *United States Department of Defence v. Federal Labor Relations Authority*,[139] the Court was faced with a request by two unions for certain federal employees' home addresses.

Addressing the issue of whether information as public as home addresses could ever be considered private, the Court wrote: "It is true that home addresses often are publicly available through sources such as telephone directories and voter registration lists, but 'in an organised society, there are few facts that are not at one time or another divulged to another.' "[140] The Court noted that the "individual's interest in controlling the dissemination of information regarding personal matters does not dissolve simply because that information may be

135. Ibid. at 763–64.

136. Ibid. at 710–71 (quoting William Rehnquist, *Is an Expanded Right of Privacy Consistent with Fair and Effective Law Enforcement?*, Nelson Timothy Stephens Lectures, University of Kansas Law School, pt. 1, p. 13 (Sept. 26–27, 1974)).

137. Ibid. at 771. In *National Archives and Records Administration v. Favish*, 541 U.S. 157 (2004), the Supreme Court further expanded its understanding of the "privacy" at issue in FOIA cases, by extending Exemption 7(C) to family members of an individual who committed suicide.

138. 5 U.S.C. § 552(b)(6) (2012).

139. 510 U.S. 487 (1994).

140. Ibid. at 550 (quoting *Reporters Comm.*, 489 U.S. at 763).

available to the public in some form."[141] The Court found that "it is clear that [individuals] have some nontrivial privacy interest in nondisclosure."[142] The Court, therefore, found that Exemption 6 prohibited the disclosure of federal employees' addresses.

Most recently, the Court has rejected a corporation's claim that disclosure of records provided to a federal agency in the course of an investigation would intrude on the corporation's "personal privacy," and therefore the records may be withheld under Exemption 7(C).[143] Applying familiar principles of statutory interpretation, the Court found that the word "personal" in both Exemption 6 and 7 connotes the privacy concerns of individuals, not entities.

V. ASSESSMENT

It is not surprising that many commentators have considered the Supreme Court's privacy jurisprudence to be confused and disjointed. The Court not only uses the term in a variety of different settings, but has defined it to have at least three distinct meanings.

The first, which the Court has described variously as a "right of personal privacy" or "areas or zones of privacy,"[144] is constitutionally protected to the extent the right can be deemed to involve decisions whose personal nature is "'fundamental'" or "'implicit in the concept of ordered liberty.'"[145] The Court has found fundamental rights of private decision-making concerning marriage, procreation, contraception, consensual sexual relations, family relationships, child-rearing, and education.[146] Although this right generally does not implicate information privacy, in certain cases it does, such as when abortion restrictions require women to receive, or provide, certain information regarding the pregnancy or fetus, as in the case of mandatory ultrasound or fetal heartbeat results, or mandatory spousal or parental notification. The Court has struck down spousal, but not parental, notification as imposing an unconstitutional "undue burden" on the right to access abortion before viability. It has upheld some mandatory informational requirements aimed at promoting informed consent, while declining to review cases striking down more recent, and controversial, provisions such as mandatory ultrasounds or fetal heartbeat results. The Court's recent decision in *Whole Woman's Health*, which signaled its willingness to question state government assertions about both the benefits and burdens of new abortion regulations, may invigorate further challenges to such regulations.

141. Ibid.

142. Ibid. at 501.

143. *Federal Commc'ns Comm'n v. AT&T Inc.*, 562 U.S. 397 (2011).

144. *Roe v. Wade*, 410 U.S. at 152.

145. Ibid. (quoting *Palko*, 302 U.S. at 325).

146. 410 U.S. at 152–53; *Lawrence v. Texas*, 539 U.S. 558 (2003).

The second meaning of privacy comes from the Court's Fourth Amendment jurisprudence. In this setting, the Court has provided a specific definition: whatever one "seeks to preserve as private, even in an area accessible to the public,"[147] provided that the individual has an "actual," subjective expectation of privacy, and that expectation is "one that society was prepared to recognize as 'reasonable.'"[148] The Court has crafted many exceptions to this right; the one with the most significant implications for the digital age is that for information to be treated as private, it must not have been disclosed to, or be held by, a third party.[149] As a result, this understanding of privacy is essentially binary: information is either not disclosed and therefore private, or it has been disclosed and therefore is not private. And this constitutional understanding of privacy is solely concerned with the collection of data, not with its retention, use, or sharing.

The Court describes its third meaning of privacy as "the individual interest in avoiding disclosure of personal matters . . . ."[150] In the constitutional context, the Court has explicitly noted that information that the government constitutionally may require an individual to disclose for one purpose, may nevertheless remain sensitive and subject to privacy protections. Many legitimate government activities "all require the orderly preservation of great quantities of information, much of which is personal in character and potentially embarrassing or harmful if disclosed. The right to collect and use such data for public purposes is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures."[151] Despite the fact that the information has been disclosed to, and is held by, someone other than the data subject, "in some circumstances that duty [to avoid unwarranted disclosures] arguably has its roots in the Constitution."[152] This interest in nondisclosure was recognized in *Whalen*, a case upholding the compelled disclosure of prescription information, and has not yet invoked strict scrutiny by the Court to assess a government data-related activity. At the same time, the Court's discussion in *Sorrell* suggests that a statute properly framed and even-handedly applied to protect privacy, might withstand a First Amendment challenge asserting rights to disclose and access such data.

In the statutory context, the Court has used this third meaning of privacy to block disclosure under FOIA. Repeatedly, the Court has found that even though information has been disclosed to and is held by third parties, this does not eliminate the existence of a lawfully protected privacy interest. "[T]he fact that 'an event is not wholly "private" does not mean that an individual has no

147. *Katz*, 389 U.S. at 351.

148. Ibid. at 361 (Harlan, J., concurring); *Terry*, 392 U.S. 1.

149. *Miller*, 425 U.S. 435; *Smith*, 442 U.S. 735.

150. *Whalen*, 429 U.S. at 599–600.

151. Ibid. at 605.

152. Ibid.

interest in limiting disclosure or dissemination of the information.' "[153] This is a far more subtle view of privacy, in which privacy is measured on a spectrum, rather than the binary view of privacy that the Court has applied so far in its Fourth Amendment jurisprudence.

The fact that there is inconsistency in the Court's privacy jurisprudence is not surprising. In fact, the Court itself noted in *Reporter's Committee* that the "question of the statutory meaning of privacy under the FOIA is, of course, not the same as the question whether a tort action might lie for invasion of privacy or the question whether an individual's interest in privacy is protected by the Constitution."[154] However, the Court is inconsistent even within its constitutional privacy jurisprudence, employing the term in *Whalen* to mean something broad and subtle and requiring protection beyond mere collection limits, and in the Court's Fourth Amendment cases to refer to something that can be eliminated by disclosure, and requires no protection beyond collection limits.

Even more significant than the inconsistency, however, is that the meaning of privacy that the Court has so far articulated in its Fourth Amendment jurisprudence—with minor exceptions—is inconsistent with popular perceptions about the meaning of privacy, and renders the Fourth Amendment impotent to protect against government intrusions into vast collections of personal information, given the extraordinary increase in both the volume and sensitivity of information about individuals necessarily held by third parties.

Professor Daniel Solove writes: "We are becoming a society of records, and these records are not held by us, but by third parties."[155] Thanks to the proliferation of digital technologies and networks such as the Internet, and tremendous advances in the capacity of storage devices and parallel decreases in their cost and physical size, those records are linked and shared more widely and stored far longer than ever before, often without the individual consumer's knowledge or consent.[156] This is especially true as more activities move online, where merchants record data not only on what individuals buy and how we pay for our purchases, but also on every detail of what we look at, what we search for, how we navigate through websites, and with whom we communicate.

The *Miller* exclusion from the Fourth Amendment of information disclosed to third parties means that all of this information, no matter how sensitive or how revealing of a person's health, finances, tastes, or convictions, is available to the

153. 489 U.S. at 710–11 (quoting William Rehnquist, *Is an Expanded Right of Privacy Consistent with Fair and Effective Law Enforcement?*, Nelson Timothy Stephens Lectures, University of Kansas Law School, pt. 1, p. 13 (Sept. 26–27, 1974)).

154. 489 U.S. at 763 n.13.

155. Daniel J. Solove, "Digital Dossiers and the Dissipation of Fourth Amendment Privacy," 75 *Southern California Law Review* 1083, 1089 (2002).

156. Ibid.; James X. Dempsey and Lara M. Flint, "Commercial Data and National Security," 72 *George Washington Law Review* 1459 (2004); Jeffrey Rosen, *The Unwanted Gaze: The Destruction of Privacy in America* (2001).

government without constitutional limit. The government's demand need not be reasonable, no warrant is necessary, and no judicial authorization or oversight is required. *Jones* and *Riley* suggest that the Court has begun to recognize the impact of technological change on the Fourth Amendment's protection for privacy, and that some justices may even be willing to revisit *Miller*. The outcome is uncertain however, and the Court plainly desires Congress, rather than the Constitution, to play the major role in balancing privacy and government access needs.

Asia and the Pacific

10

Systematic Government Access to Private-Sector Data in Australia

DAN JERKER B. SVANTESSON AND REBECCA AZZOPARDI*

I. ABSTRACT

This study of systematic government access to private-sector data in Australia suggests that, although the Australian government has a range of powers to obtain such data, those powers appear primarily aimed at obtaining specific data for specific purposes. Little was found by way of direct unmediated access by the government to private-sector data or government access to private-sector data in bulk.

II. NATIONAL LEGAL CONTEXT AND FUNDAMENTAL PRINCIPLES

Australia has a federal system of government with power distributed among six states, two territories, and the federal government. The Australian Constitution provides the federal government with the exclusive power to make laws on matters such as trade and commerce, taxation, defense, external affairs, and immigration and citizenship. It also outlines concurrent powers where both tiers of government are able to enact laws. The states and territories have independent legislative power in all matters not specifically assigned to the federal government.[1] Both state/territory law and federal law affect the issues examined here. However, the most significant legislative initiatives are found on the federal level.

* The opinions expressed in this chapter are the authors' own and do not reflect the view of any particular entity. The authors are grateful for the valuable feedback provided by Nigel Waters.

1. Australian Government, "How Government Works," http://www.australia.gov.au/about-government/how-government-works (last visited April 25, 2017).

Bulk Collection. Fred H. Cate and James X. Dempsey.

Discussions[2] have taken place aimed at the possible introduction of a federal Bill of Rights, but Australia currently lacks such an instrument. The Australian Human Rights Commission is responsible for promoting and encouraging protection of human rights in Australia. However, although Australia is a signatory to international instruments, such as the International Covenant on Economic, Social and Cultural Rights and the International Covenant on Civil and Political Rights with its Optional Protocol 2, there are no *binding* human rights principles on a federal level. Nevertheless, a Statement of Compatibility with Human Rights is required to accompany any new legislation proposed at the federal level and is considered by the Joint Parliamentary Committee on Human Rights.[3] Due to these protections and the ongoing debate about the role of a charter or bill of human rights in Australia, the Australian Human Rights Commissioner has indicated that there is currently no intention to pursue a charter at the federal level.[4] If we turn to the state/territory level, the Australian Capital Territory introduced its Human Rights Act in 2004. Section 12 of that Act specifically protects privacy.[5] Similarly, the Charter of Human Rights and Responsibilities Act 2006 (Vic) of Victoria contains such protection.[6] Further, other states also, for example New South Wales, have considered implementing such human rights protection.

Australian privacy law underwent a major overhaul in 2014 following the release of a 2,694 page report, in 2008, by the Australian Law Reform Commission (ALRC).[7] That report made a number of recommendations, which the government implemented in part in amendments to the Privacy Act 1988 (Cth) and the introduction of the Australian Privacy Principles (APPs), which came into force in March 2014. In addition to establishing the APPs, which apply to both federal government agencies and some private sector organizations, the amended Privacy Act established more comprehensive credit reporting obligations on credit providers and provided the Privacy Commissioner with enhanced powers to deal with privacy complaints.

As part of its 2008 report the ALRC recommended that Australia introduce a statutory cause of action for serious invasions of privacy.[8] This recommendation

2. https://www.humanrights.gov.au/our-work/rights-and-freedoms/projects/lets-talk-about-rights-human-rights-act-australia (last visited July 22, 2016).

3. Human Rights (Parliamentary Scrutiny) Act 2011 (Cth), § 8.

4. Australian Human Rights Commission, *Rights and Responsibilities Consultation Report* (2015) 49, https://www.humanrights.gov.au/sites/default/files/document/publication/rights-and-responsibilities-report-2015.pdf.

5. Human Rights Act 2004 (ACT).

6. Charter of Human Rights and Responsibilities Act 2006 (Vic), § 13.

7. ALRC, *For Your Information: Australian Privacy Law and Practice* (May 2008) ALRC 108, available at http://www.alrc.gov.au/publications/report-108.

8. Ibid.

was not adopted as part of the Privacy Act reform, and was renewed by the ALRC in a subsequent report in 2014 with the specific suggestion that the statutory cause of action be contained in a tort in Commonwealth legislation, separate to the Privacy Act. The recommendation was for the tort to apply only to intentional or reckless invasions of privacy and to be available to people who have a reasonable expectation of privacy.[9] The government has not indicated a willingness to adopt the recommendations to date, and commentators have suggested that "uncertainty and inconclusiveness is destined to continue for some time yet" in relation to this issue.[10]

III. STATUTORY AND REGULATORY OVERVIEW

In addition to the key areas of data access focused on below, other examples of more or less systematic government access to private-sector data can be found, such as in the context of government use of private entity CCTV footage,[11] ID scanning at clubs,[12] special reporting duties placed on selected healthcare providers,[13] private, or semiprivate operators of toll roads and public transport smartcards.[14] More recently, health information is collected by the newly developed Australian Digital Health Agency when individuals register for an eHealth record.[15]

A. Laws Requiring, Explicitly Authorizing, or Restricting Governmental Access to Private-Sector Data

The Privacy Act 1988 (Cth) contains 13 APPs that regulate, in general terms, the use of personal information by federal "agencies," a term used to include, for example, Ministers, Departments, bodies and tribunals established or appointed for a public purpose, persons holding or performing the duties of a government office, federal courts, and the Australian Federal Police.[16] State, territory, and

9. ALRC, *Serious Invasions of Privacy in the Digital Era: Final Report* (2014) ALRC 123, http://www.alrc.gov.au/sites/default/files/pdfs/publications/final_report_123_whole_report.pdf.

10. Margaret Jackson and Gordon Hughes, *Private Life in a Digital World* (2015) at 191.

11. See for example: Victorian Law Reform Commission, *Surveillance in Public Places: Final Report* (2010) VLRC 18, http://www.austlii.edu.au/cgi-bin/disp.pl/au/other/lawreform/VLRC/2010/18.html?stem=0&synonyms=0&query=CCTV.

12. See further, Australian Privacy Foundation, "Identity Scanning by Registered Clubs" (last visited July 15, 2016), http://www.privacy.org.au/Papers/ClubIDScans.html.

13. See, for example Health Insurance Act 1973 (Cth), § 23DS.

14. See further: Nigel Waters, *Government Surveillance in Australia* (August 2006), http://www.pacificprivacy.com.au/Government%20Surveillance%20in%20Australia%20v6.pdf.

15. Australian Digital Health Agency, at: http://digitalhealth.gov.au (last visited July 16, 2016).

16. Privacy Act 1988 (Cth), § 6.

local government bodies are not covered and are instead regulated in state or territory law.[17] The Privacy Act also does not apply to Australian intelligence agencies.

Agencies regulated by this scheme shall not collect personal information (other than "sensitive information," which has additional protections) unless the information is reasonably necessary for, or directly related to, one or more of the "entity's functions or activities."[18] Further, the collector must collect personal information only by lawful and fair means[19] and take reasonable steps to ensure that the personal information collected is "accurate, up to date and complete."[20] Similar regulation can be found on the state level in some states.

Sensitive information, which includes information or opinion about an individual's racial or ethnic origin; political opinions; membership in a political, professional or trade association or trade union; religious beliefs or affiliations; philosophical beliefs; sexual orientation or practices; criminal record; or health, genetic, or biometric information,[21] can only be collected by an agency if the individual consents to the collection and "the information is reasonably necessary for, or directly related to, one or more of the agency's functions or activities" or if there is a relevant exception.[22] Those exceptions include if:

(a) the collection of the information is required or authorized by or under an Australian law or a court/tribunal order; or
(b) a "permitted general situation" exists, which includes where it is unreasonable or impracticable to obtain the individual's consent to the collection and the agency reasonably believes the collection is necessary to lessen or prevent a serious threat to life, health, or safety of an individual, or to public health and safety;[23] or
(c) the agency is a prescribed "enforcement body" and the agency reasonably believes that "the collection of the information is reasonably necessary for, or directly related to, one or more of the [agency's] functions or activities."[24]

17. Privacy and Personal Information Protection Act 1998 (NSW), Privacy and Data Protection Act 2014 (Vic), Information Privacy Act 2009 (Qld), Personal Information Protection Act 2004 (Tas), Information Act 2002 (NT) and Information Privacy Act 2014 (ACT).

18. Australian Privacy Principle 3.1.

19. Australian Privacy Principle 3.5.

20. Australian Privacy Principle 10.1.

21. Privacy Act 1988 (Cth), § 6.

22. Australian Privacy Principle 3.3.

23. Privacy Act 1988 (Cth), § 16A.

24. Australian Privacy Principle 3.4.

The impact of this regulation on systematic government access to private-sector data is interesting. On the one hand, it clearly sets boundaries for how governmental access to private-sector data may be had, and its broad scope of application means that it affects a wide range of government functions. On the other hand, this regulation is significantly undermined by the ease by which it can be circumvented. For example, AusCheck—a branch of the National Security Law and Policy Division of the Attorney-General's Department—has the role of undertaking background checking for persons to hold certain identification cards. The AusCheck Act 2007 (Cth) explicitly authorizes AusCheck to collect, use, and disclose personal information for AusCheck purposes. Importantly for the discussion here, such collection, use, and disclosure is "taken to be authorised by law for the purposes of the Privacy Act 1988."[25] Thus, specific legislation can be used to nominate data use practices as being authorized by law so as to fit within the regulation discussed above.

On a more general level, it is worth noting how one expert has observed that:

> Government agencies generally appear to consider any information lawfully obtained as "fair game" for any subsequent lawful function. Moreover, the cumulative effect of the various statutory disclosure provisions is that information obtained by one agency for a specific purpose becomes at least potentially available to a range of other agencies for quite different purposes.
>
> Information privacy laws, in those Australian jurisdictions which have them, purport to limit use and disclosure to the purpose for which information is obtained, but this principle is substantially undermined by the many exceptions, including where "required or authorised by law" and "where reasonably necessary for [a range of public purposes]."[26]

B. Separate Laws for Law Enforcement Access, Regulatory Access, and/or National Security Access

Under current law, the Privacy Act 1988 (Cth) does not apply to some Australian government agencies "involved in law enforcement, intelligence gathering and national security" such as intelligence and defense intelligence agencies,[27] and there are special rules regulating access by prescribed enforcement bodies for "enforcement related activities" broadly referring to activities such as the "prevention, detection, investigation, prosecution or punishment of criminal offences

25. AusCheck Act 2007 (Cth), § 13(1).

26. Nigel Waters, *Government Surveillance in Australia* (August 2006), http://www.pacificprivacy.com.au/Government%20Surveillance%20in%20Australia%20v6.pdf (internal footnote omitted).

27. Office of the Australian Information Commissioner, "Which Law Enforcement Agencies Are Covered by the Privacy Act?" https://www.oaic.gov.au/individuals/faqs-for-individuals/law-enforcement-surveillance-photos/resources-on-law-enforcement (last visited April 25, 2017). See for example Privacy Act 1988 (Cth), § 7. The term "intelligence agency" is defined in § 6(1) of the Privacy Act 1988 (Cth).

or breaches of a law imposing a penalty or sanction" and also surveillance, intelligence gathering and monitoring activities, among others.[28]

The Crimes Act 1914 (Cth), Part 1AA, Division 4B, gives the Australian Federal Police (AFP) "notice to produce powers." For example, section 3ZQM provides power to request information or documents about terrorist acts from operators of aircraft or ships. That section allows an authorized AFP officer, who believes on reasonable grounds that an operator of an aircraft or ship has information or documents (including in electronic form) that are relevant to a matter that relates to the doing of a terrorist act (whether or not a terrorist act has occurred or will occur), to "ask the operator questions relating to the aircraft or ship, or its cargo, crew, passengers, stores or voyage, that are relevant to the matter"[29] and to "request the operator to produce documents relating to the aircraft or ship, or its cargo, crew, passengers, stores or voyage: (i) that are relevant to the matter; and (ii) that are in the possession or under the control of the operator."[30]

Section 3ZQN provides similar powers where "an authorised AFP officer considers on reasonable grounds that a person has documents (including in electronic form) that are relevant to, and will assist, the investigation of a serious terrorism offence."[31] No prior court approval is required for these categories of requests. In contrast, where an AFP officer considers, on reasonable grounds, that the person has documents (including in electronic form) that are relevant to, and will assist, the investigation of a serious offense, an application can be made to a judge of the Federal Circuit Court for a "notice to produce" order. To grant such an order, the Judge must be satisfied, on the balance of probabilities, by information on oath or by affirmation, that: "(a) the person has documents (including in electronic form) that are relevant to, and will assist, the investigation of a serious offence; and (b) giving the person a notice under this section is reasonably necessary, and reasonably appropriate and adapted, for the purpose of investigating the offence."[32] On state-level, most jurisdictions require warrants issued either by judges or magistrates.[33]

28. Privacy Act 1988 (Cth), § 6(1), definition of "enforcement related activity." This definition also includes the conduct of protective or custodial activities; the enforcement of laws relating to the confiscation of the proceeds of crime; the protection of the public revenue; the prevention, detection, investigation, or remedying of misconduct of a serious nature; or the preparation for, or conduct of, proceedings before any court or tribunal; or the implementation of court/tribunal orders.

29. Crimes Act 1914 (Cth), § 3ZQM.

30. Crimes Act 1914 (Cth), § 3ZQM.

31. Crimes Act 1914 (Cth), § 3ZQN.

32. Crimes Act 1914 (Cth), § 3ZQO.

33. Nigel Waters, *Government Surveillance in Australia* (August 2006), http://www.pacificprivacy.com.au/Government%20Surveillance%20in%20Australia%20v6.pdf, p. 4. See, for example, Law Enforcement (Powers and Responsibilities) Act 2002 (NSW), Victoria Police Act 2013 (Vic).

Special rules apply to data gathering by the Australian Security Intelligence Organisation (ASIO). ASIO's data collection powers, particularly relating to computer and data access and surveillance devices, were modernized and broadened in 2014 following the passing of the National Security Legislation Amendment Act 2014 (Cth).

Part III, Division 2 of the Australian Security Intelligence Organisation Act 1979 (Cth) provides ASIO with a range of special powers relating to matters such as search warrants,[34] requesting information or documents from operators of aircraft or vessels,[35] inspection of postal articles and delivery service articles,[36] the use of surveillance devices,[37] the use of tracking devices,[38] and the collection of foreign intelligence within Australia.[39] Most important here, section 25A grants computer access powers. The Director-General may request the Minister to issue a warrant for computer access. The Minister must only issue such a warrant if: "satisfied that there are reasonable grounds for believing that access by the Organisation to data held in a computer (the target computer) will substantially assist the collection of intelligence in accordance with this Act in respect of a matter (the security matter) that is important in relation to security."[40]

Prior to recent amendments, this provision referred to access to data held in "a particular computer." A submission in May 2011 cautioned against the use of the phrase "data held in a particular computer" and suggested that with an increasing uptake in cloud computing, it may be difficult for ASIO to accurately predict in advance whether a person has stored relevant data locally on the "target computer" or "in the cloud."[41] It also noted that, under the previous wording, ASIO would appear restricted from accessing data stored in the cloud where a warrant has been granted for access to a target computer, even if, for example, the suspect in question has stored his/her login details for the cloud storage on that computer.[42]

34. Australian Security Intelligence Organisation Act 1979 (Cth), § 25.

35. Australian Security Intelligence Organisation Act 1979 (Cth), § 23.

36. Australian Security Intelligence Organisation Act 1979 (Cth), §§ 27 & 27AA.

37. Australian Security Intelligence Organisation Act 1979 (Cth), § 26, 26A, 26B, 26C and 26D.

38. Australian Security Intelligence Organisation Act 1979 (Cth), §§ 26E.

39. Australian Security Intelligence Organisation Act 1979 (Cth), §27A.

40. Australian Security Intelligence Organisation Act 1979 (Cth), § 25A(2).

41. Dan Svantesson, "Submission in relation to the Legal and Constitutional Affairs Legislation Committee's inquiry into the Intelligence Services Legislation Amendment Bill 2011" (May 26, 2011), http://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Legal_and_Constitutional_Affairs/Completed_inquiries/2010-13/intelligenceservices/submissions.

42. Dan Svantesson, "Submission in relation to the Legal and Constitutional Affairs Legislation Committee's Inquiry into the Intelligence Services Legislation Amendment Bill 2011" (May

In 2014, the definition of "computer" was broadened to include multiple computers, computer systems, or networks, and to enable the target computer of a computer access warrant to extend to all computers at a particular premises or operating in a network, and all computers associated with, used by or likely to be used by, a person (whose identity may or may not be known).[43] The effect of this is that ASIO now has broadened powers to "use the computers of innocent third parties to gain access to a computer used by a suspected terrorist or criminal" and to "target information stored in the cloud or to intercept information flows between computers."[44]

It is also worth noting that, the Attorney-General has issued guidelines for the operation of ASIO. Under those Guidelines, information is to be obtained by ASIO in a lawful, timely, and efficient way. Further, the obtaining of information must take place in accordance with the following: (1) any means used for obtaining information must be proportionate to the gravity of the threat posed and the probability of its occurrence, and (2) inquiries and investigations into individuals and groups should be undertaken using as little intrusion into individual privacy as is possible. Further, the more intrusive the investigative technique, the higher the level of officer that should be required to approve its use, and wherever possible, the least intrusive techniques of information collection should be used before more intrusive techniques.[45] Finally, the Director-General "shall take all reasonable steps to ensure that personal information shall not be collected, used, handled, or disclosed by ASIO unless that collection, use, handling, or disclosure is reasonably necessary for the performance of its statutory functions (or as otherwise authorised, or required, by law)."[46]

26, 2011), http://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Legal_and_Constitutional_Affairs/Completed_inquiries/2010-13/intelligenceservices/submissions.

43. Australian Security Intelligence Organisation Act 1979 (Cth), §§ 22 and 25A(3) as amended by National Security Amendment Act 2014 (Cth).

44. K. Lachmayer and N. Witzleb, "The Challenge to Privacy from Ever Increasing State Surveillance: A Comparative Perspective," 37(2) *UNSWLawJl* 770 (2014), http://www.austlii.edu.au/cgi-bin/download.cgi/cgi-bin/download.cgi/download/au/journals/UNSWLawJl/2014/28.pdf.

45. Australian Security Intelligence Organisation, *Attorney-General's Guidelines in relation to the performance by the Australian Security Intelligence Organisation of its function of obtaining, correlating, evaluating and communicating intelligence relevant to security (including politically motivated violence)*, https://www.asio.gov.au/sites/default/files/Attorney-General's%20Guidelines.pdf (last visited April 27, 2017), Guideline 10.4.

46. Australian Security Intelligence Organisation, *Attorney-General's Guidelines in relation to the performance by the Australian Security Intelligence Organisation of its function of obtaining, correlating, evaluating and communicating intelligence relevant to security (including politically motivated violence)*, https://www.asio.gov.au/sites/default/files/Attorney-General's%20Guidelines.pdf (last visited April 27, 2017), Guideline 13.2.

If we look specifically at the legislative powers to access communications data, section 313 of the Telecommunications Act 1997 (Cth) imposes obligations on all carriers[47] and carriage service providers[48] "to provide assistance to officers and authorities of the Commonwealth, states and territories as is reasonably necessary for enforcing the criminal law and laws imposing pecuniary penalties, assisting the enforcement of the criminal laws in force in a foreign country, protecting revenue or safeguarding national security."[49] Significantly, this includes, amongst other obligations, providing assistance to agencies in relation to the interception of communications and access to stored communications. [50]

Further, although sections 276–278 of the Telecommunications Act 1997 (Cth) place restrictions on the use and disclosure of telecommunications data, special exemptions apply for law enforcement and national security agencies. There are also different powers available for access to telecommunications "data," generally considered to be metadata, as opposed to the content of the communications themselves.

When dealing with telecommunications data, a distinction is drawn between "voluntary disclosure" on the one hand and "authorised disclosure" on the other. Voluntary disclosure of information or a document to ASIO is allowed provided the disclosure is in connection with the performance by ASIO of its functions.[51] Similarly, section 177 allows such voluntary disclosure to "an enforcement agency if the disclosure is reasonably necessary for the enforcement of the criminal law, or a law imposing a pecuniary penalty, or for the protection of the public revenue."[52] In the context of such disclosure, there is a risk of "oversupply" in that telecommunications employees might disclose more than what is necessary.[53]

Authorized disclosure can relate to data held by the telecommunications operator, or so-called prospective information or documents. ASIO[54] and enforcement

47. That is, somewhat simplified, the holder of a carrier license. See further Telecommunications Act 1997 (Cth), § 7.

48. That is, somewhat simplified, a person who supplies, or proposes to supply, a listed carriage service to the public. See further Telecommunications Act 1997 (Cth), § 87.

49. Australian Government, "Overview of legislation: The Telecommunications Act 1997," https://www.ag.gov.au/NationalSecurity/TelecommunicationsSurveillance/Pages/Overviewoflegislation.aspx (last visited July 17, 2016).

50. Telecommunications Act 1997 (Cth), § 313(7).

51. Telecommunications (Interception and Access) Act 1979 (Cth), § 174(1).

52. Sharon Rodrick, "Accessing Telecommunications Data for National Security and Law Enforcement Purposes," 2009 *UMonashLRS* 15, http://www.austlii.edu.au/au/journals/UMonashLRS/2009/15.html, p. 28.

53. Ibid., p. 29.

54. Telecommunications (Interception and Access) Act 1979 (Cth), § 175.

agencies[55] may authorize the disclosure of specific information or documents held by a telecommunications operator without a warrant. More interestingly, they can also authorize disclosure of prospective data on an ongoing basis, such as specific web browsing activities or the real-time location of phones or other devices,[56] excluding the content or substance of communications.[57] As far as enforcement agencies are concerned, authorization must not be made unless the disclosure is reasonably necessary for the investigation of an offense punishable by imprisonment for at least three years.[58] Further, before making the authorization, the authorized officer "must be satisfied on reasonable grounds that any interference with the privacy of any person or persons that may result from the disclosure or use is justifiable and proportionate" having regard to certain matters, including the gravity of any conduct in relation to which the authorization is sought, the likely relevance and usefulness of the information or documents, and the reason the disclosure or use is proposed to be authorized.[59] Notably, these rules do not apply to ASIO.[60]

Although the ability of certain government agencies to access telecommunications data has been in place for some time, there were previously no requirements on service providers to retain the data for any particular period of time or to specify the types of data that were to be retained. Mandatory retention requirements were implemented in the Telecommunications (Interception and Access) Act 1979 (Cth) from October 2015 and rationalized on the basis that the value of the tools previously available to national security and law enforcement agencies to access telecommunications data were being "undermined by the level of change in the telecommunications environment,"[61] including the development of new technologies and the globalization of the telecommunications industry. The

55. Telecommunications (Interception and Access) Act 1979 (Cth), §§. 178, 178A & 179. Recent amendments restricted the types of agencies that are able to access data under the TIA Act. By § 176A, the Telecommunications (Interception and Access) Act 1979 (Cth), now applies to certain "criminal law enforcement agencies" or an agency declared by the Minister to be an "enforcement agency" for the purposes of the Act.

56. For ASIO, see Telecommunications (Interception and Access) Act 1979 (Cth), § 176, and for enforcement agencies, refer to Telecommunications (Interception and Access) Act 1979 (Cth), § 180. See further, Sharon Rodrick, "Accessing Telecommunications Data for National Security and Law Enforcement Purposes," 2009 *UMonashLRS* 15 http://www.austlii.edu.au/au/journals/UMonashLRS/2009/15.html, pp. 31–35.

57. Telecommunications (Interception and Access) Act 1979 (Cth), § 172.

58. Telecommunications (Interception and Access) Act 1979 (Cth), § 180(4).

59. Ibid., § 180F.

60. Sharon Rodrick, "Accessing Telecommunications Data for National Security and Law Enforcement Purposes," 2009 *UMonashLRS* 15, http://www.austlii.edu.au/au/journals/UMonashLRS/2009/15.html, p. 34.

61. Parliament of Australia, *Explanatory Memorandum to Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*, paragraph 1.

changes also recognize the government's view of the importance of telecommunications data in the investigation of serious criminal investigations including "counter-terrorism, organized crime, counter-espionage and cyber security . . . murder, rape and kidnapping."[62] There is now a statutory obligation on telecommunications and Internet service providers to retain certain prescribed telecommunications data, including identification and contact information; the source and destination of a communication; the date, time, and duration of a communication; and the type of communication, for a period of two years.[63] That data is then available for access by certain enforcement agencies.

Of note, the retention requirements do not require service providers to retain the content or substance of a communication,[64] such as the content of emails or telephone calls, or web browsing history,[65] and the service provider must protect the confidentiality of the information by encrypting it and protecting it from unauthorized interference or unauthorized access.[66]

Certain national security and law enforcement agencies still have the ability to access or intercept the content or substance of a communication (for example the content of an email or SMS) by obtaining an interception warrant[67] or stored communications warrant[68] for certain purposes or in a life threatening emergency.[69] In relation to both interception and stored communication warrants the issuing authority must have regard to certain matters including how much the privacy of any person would be likely to be interfered with, the gravity of the conduct constituting the serious offense or contravention, how much the information would be likely to assist in connection with the investigation, and to

62. Ibid., paragraph 5.

63. Telecommunications (Interception and Access) Act 1979 (Cth), Part 5.1A.

64. Ibid., § 187A(4)(a).

65. Ibid., § 187A(4)(b).

66. Ibid., § 187BA.

67. For example, under § 9 of Telecommunications (Interception and Access) Act 1979 (Cth), the Attorney-General may issue a warrant on request by the Director General to assist ASIO in carrying out its function of obtaining intelligence relating to security. Part 2.5 allows certain agencies to apply for interception warrants where the information is likely to assist in connection with the investigation of a serious offense (which is defined in § 5D as including murder, kidnapping, acts of terrorism, people smuggling/trafficking etc.).

68. Telecommunications (Interception and Access) Act 1979 (Cth), Part 3.3. Section 116(1) sets out when an issuing authority can issue a stored communications warrant that includes where the information would be likely to assist in connection with an investigation by the agency or a foreign country of a serious contravention in which the person is involved (including as a victim). A serious contravention is defined in section 5E as including an offense punishable by imprisonment of at least three years or a fine of at least 180 penalty units for an individual.

69. Telecommunications (Interception and Access) Act 1979 (Cth), § 30.

what extent other investigative methods have been used by or are available to the agency.[70] These powers were not increased by the Amendment Act.

Taken together, this provides Australian law enforcement and national security agencies with broad access to private-sector data. At the same time, it appears that, on most occasions, the regulatory framework outlined in this section would be used for "small scale" access to data in individual cases as the requirements imposed, for example by the Attorney-General Guidelines, ought to ensure that, typically only specific data for specific purposes is collected rather than data in bulk. Having said that, one can of course imagine scenarios where access is sought to larger volumes of for example, airline cargo or crew data, or indeed, systematic access in the sense of repeated access is being sought. Further, the powers granted to ASIO could be used for systematic, direct and unmediated, access to private-sector data.

C. Laws Requiring Broad Reporting of Personal Data by Private-Sector Entities

There are some examples of Australian law requiring broad reporting of personal data by private-sector entities, such as the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth), the Income Tax Assessment Act 1997 (Cth), and the Customs Act 1901 (Cth).

1. Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth)

On December 12, 2007, Australia introduced its Anti-Money Laundering and Counter-Terrorism Financing programs. The programs are regulated in the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth) (AML/CTF Act). These programs—which apply to private entities such as banks, non-bank financial services, remittance (money transfer) services, bullion dealers, and gambling businesses[71]—explicitly require broad reporting of personal data by private-sector entities. More specifically, the aim is for reporting entities to help identify, mitigate, and manage the risk of their products or services facilitating money laundering or terrorism financing.[72] The scheme is overseen by Australian Transaction Reports and Analysis Centre (AUSTRAC).[73]

Where a private entity provides a "designated service," it is classed as a reporting entity and must adopt, maintain, and comply with an AML/CTF program.[74]

70. Ibid., § 46(2), § 116(2).

71. Australian Government, "An introduction to AML/CTF programs" (July 29, 2016), http://www.austrac.gov.au/chapter-6-amlctf-programs.

72. Ibid.

73. http://www.austrac.gov.au/.

74. Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth), § 5.

Such a program includes several obligations (e.g., relating to the training and screening of staff, ensuring that an adequate monitoring system is in place, etc.) but most important for our purposes, it includes an obligation to submit three different types of reports.

- **Suspicious Matter Reports (SMRs)**[75]—where a reporting entity suspects that a matter may be related to an offense, tax evasion, or the proceeds of crime, it must submit a SMR within three business days, or where the suspicion relates to the financing of terrorism, within 24 hours. Such a report is to include all details known about the suspicious matter, the person/organization(s) to which the matter relates, and any transactions related to the matter.[76]
- **Threshold Transaction Reports (TTRs) (where applicable)**[77]—where a reporting entity provides or commences to provide a designated service to a customer that involves the transfer of physical currency or e-currency of AUD10,000 or more it must complete a TTR within 10 business days. The information to be provided within a TTR includes details of the customer of the designated service, the individual conducting the transaction (if different from the customer), the recipient of the proceeds of the transaction (if different from the customer), and the transaction, including cash and other components.[78]
- **International Funds Transfer Instruction (IFTI) reports (where applicable)**[79]—where a reporting entity sends or receives a funds transfer instruction to or from a foreign country, it must complete an IFTI report within 10 business days. The information to be provided within a IFTI includes details of the transfer instruction, the parties involved in the transaction, or details of the ordering and beneficiary customers for the remittance, the originating and destination country's remittance service providers (if applicable), and any additional information relating to the instruction.[80]

The AML/CTF Act contains a set of tables in section 6 that outlines in detail what constitutes a "designated service." Examples include where the service is

75. Ibid., §§ 41–42.

76. Australian Government, "Reporting requirements," http://www.austrac.gov.au/files/reporting-requirements_dec2010.pdf (last visited April 25, 2017).

77. Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth), §§ 43–44.

78. "Reporting requirements," http://www.austrac.gov.au/files/reporting-requirements_dec2010.pdf.

79. Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth), §§ 45–46.

80. "Reporting requirements," http://www.austrac.gov.au/files/reporting-requirements_dec2010.pdf.

provided in the course of carrying on a business: opening an account, accepting deposits or allowing withdrawals, making a loan, issuing a debit or credit card, supplying goods through a finance lease, supplying goods by way of hire purchase, issuing traveler's checks, providing remittance services that transfer money or property, dealing with certain superannuation-related transactions or services, issuing or accepting liability under life insurance policies, issuing or selling securities and derivatives, exchanging foreign currency, receiving or accepting a bet, placing or making a bet, allowing a person to play a game on an electronic gaming machine, paying out winnings on bets, and exchanging money for gaming chips or tokens and vice versa.

2. Customs Act 1901 (Cth)

The Australian government collects passenger data, and where an operator of an international passenger air service fails to provide ongoing access to that data in a manner and form requested by the government, that operator commits an offense.[81] The Act makes clear that: "The obligation to provide access must be complied with even if the information concerned is personal information (as defined in the Privacy Act 1988)."[82]

3. Taxation and Employment

The Australian Taxation Office (ATO) collects private-sector data systematically in a range of ways. For example, upon hiring a new employee, the employer must collect, and report to the ATO, the employee's tax file number (a unique identifier allocated by the ATO).[83] Systematic reporting is also required under the Income Tax Assessment Act 1997 (Cth), which requires all employers and financial institutions in Australia to report all earned and unearned (investment) income to the ATO.[84]

4. Education

In Australia, providers of higher education (some of which, such as Bond University, are private entities) must report certain data to the government. In particular, systematic reporting requirements relate to the personal information of students on student visas (international students), and students who have access to government benefits.[85]

81. Customs Act 1901 (Cth), § 64AF(1).

82. Customs Act 1901 (Cth), § 64AF(1) Note 2.

83. Taxation Administration Act 1953 (Cth).

84. Nigel Waters, *Government Surveillance in Australia* (August 2006), http://www.pacificprivacy.com.au/Government%20Surveillance%20in%20Australia%20v6.pdf, p. 15.

85. See further, Higher Education Support Act 2003 (Cth). That Act contains specific provisions dealing with privacy protection. See, Part 5-4, Division 179.

D. Laws Permitting or Restricting Private-Sector Entities from Providing Government Officials with Voluntary Broad Access to Data

The APPs in the Privacy Act 1988 (Cth) also regulate when private-sector entities may provide government officials with voluntary broad access to data, as well as the disclosure of specific data. However, due to a range of significant exemptions (e.g., the Act does not apply to some organizations with an annual turnover of AUS $3 million[86] or less), that Act is only applicable to a small proportion of Australian private-sector entities. Thus, the majority of Australian private-sector entities are unregulated in their voluntary provision of data to the government.[87]

Entities that do fall under the Privacy Act's regulation must not use or disclose personal information about an individual for a purpose (the secondary purpose) other than the primary purpose of collection unless the individual has consented to the use or disclosure or one of the following relevant exceptions applies:

(a) the individual would reasonably expect the information to be used or disclosed for the secondary purpose and the secondary purpose is:
  (i) if the information is sensitive information—directly related to the primary purpose; or
  (ii) if the information is not sensitive information—related to the primary purpose; or
(b) "the use or disclosure of the information is required or authorised by or under an Australian law or a court/tribunal order;" or
(c) a "permitted general situation" exists in relation to the use or disclosure of the information which includes (subject to certain conditions) where the entity reasonably believes that the use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of an individual or to public health or safety, where the entity has reason to suspect that unlawful activity or misconduct of a serious nature that relates to the entity's functions or activities has been, is being or may be engaged in, or the entity reasonably believes that the use or disclosure is reasonably necessary to assist an entity to locate a person who has been reported as missing; or
(d) the disclosure is by an organization and a "permitted health situation" exists in relation to the use or disclosure of the information, which includes where the disclosure of health information is necessary for research or the compilation or analysis of statistics, relevant to

86. Roughly equal to US $3 million.

87. Nigel Waters, *Government Surveillance in Australia* (August 2006), http://www.pacificprivacy.com.au/Government%20Surveillance%20in%20Australia%20v6.pdf, p. 3.

public health or public safety where it is impracticable to obtain the individual's consent, the disclosure is conducted in accordance with approved guidelines and the organisation reasonably believes that the recipient will not disclose the information; or

(e) the entity reasonably believes that the use or disclosure of the information is reasonably necessary for an "enforcement related activity" conducted by, or on behalf of, a prescribed enforcement body, including:
  (i) the prevention, detection, investigation, prosecution or punishment of criminal offences or breaches of a law imposing a penalty or sanction; or
  (ii) the conduct of surveillance activities, intelligence gathering activities or monitoring activities; or
  (iii) the conduct of protective or custodial activities; or
  (iv) the enforcement of laws relating to the confiscation of the proceeds of crime; or
  (v) the protection of the public revenue; or
  (vi) the prevention, detection, investigation, or remedying of misconduct of a serious nature, or other conduct prescribed by the regulations; or
  (vii) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal.[88]

E. Judicial Authorization Requirements for Major Categories of Data

As noted throughout, warrants issued by judges play a major role in Australia. However, exceptions can be found, such as in relation to the Telecommunications (Interception and Access) Act 1979 (Cth) that, for example, allows an authorized officer of a criminal law-enforcement agency to authorize data disclosure.

F. Standards for Use Once the Government Acquires Data

The Privacy Act 1988 (Cth)'s APPs also regulate how the federal government agencies may use data once it has been acquired. Importantly, the regulations referred to above (contained in APP6) similarly apply to the use and disclosure of personal information that is collected by a government agency.

In addition to these obligations, the APPs impose obligations on both agencies and organizations to take reasonable steps to ensure that the personal information collected is accurate, up to date, and complete;[89] to check the accuracy and

88. Australian Privacy Principle 6; Privacy Act 1988 (Cth), §§ 6, 16A and 16B.

89. Australian Privacy Principle 10.

relevancy of personal information before it is used or disclosed;[90] to provide access to the information it holds on an individual to that individual on request (subject to some exceptions such as those under the Freedom of Information Act 1982 (Cth) for example);[91] to provide information about the data it holds;[92] and to take reasonable steps to protect the information from misuse, interference, and loss and from unauthorized access, modification or disclosure.[93]

Examples of similar legislation can be found on state-level.

G. Cross-Border and Multi-jurisdictional Issues

Section 5B of the Privacy Act 1988 (Cth) regulates the extraterritorial reach of the Act. That section extends the application of the Privacy Act 1988 (Cth) to acts done, or practice engaged in, outside Australia and the external territories by an organization or small business operator provided that: (1) the overseas act was not required by an applicable foreign law, and (2) the relevant organization meet one of the following two tests, described as the "Australian link."

The first test, found in section 5B(2) is met where the organization in question is: (1) an Australian citizen, (2) a person whose continued presence in Australia is not subject to a limitation as to time imposed by law, (3) a partnership formed in Australia or an external Territory, (4) a trust created in Australia or an external Territory, (5) a body corporate incorporated in Australia or an external Territory, or (6) an unincorporated association that has its central management and control in Australia or an external Territory.

The second test, outlined in section 5B(3) is met where the organization in question: (1) is not described in subsection (2) (i.e., does not meet the first test), (2) carries on business in Australia or an external Territory, and (3) "the personal information was collected or held by the organisation or operator in Australia or an external Territory, either before or at the time of the act or practice."

Section 5B has not been subject to any extensive judicial interpretation and several aspects of its application (particularly in relation to the second test mentioned above) must be seen as unclear. For example, it is not clear under which circumstances an organization is held to be "carrying on business in Australia or an external Territory."[94] The APP Guidelines issued by the Office of the Australian Information Commissioner (APP Guidelines) acknowledge that the phrase "carries on business in Australia" is not defined in the Privacy Act 1988 (Cth), but note that guidance can be drawn from judicial consideration of this phrase in

90. Australian Privacy Principle 10.

91. Australian Privacy Principle 12.

92. Australian Privacy Principle 1.

93. Australian Privacy Principle 11.1.

94. See further, Dan Svantesson. "Protecting Privacy on the 'Borderless' Internet—Some Thoughts on Extraterritoriality and Transborder Data Flow" (2007) *Bond Law Review* 19.1, http://works.bepress.com/dan_svantesson/3.

corporations and consumer law, whilst stressing that these concepts must be assessed in the context of the Privacy Act 1988 (Cth).[95] The APP Guidelines provide the following factors that may be considered in assessing whether an entity is carrying on a business in Australia:

(a) the entity has a place of business in Australia;
(b) people who undertake business acts for the entity are located in Australia—for example, an entity may carry on business in Australia where an agent acting on its behalf carries on its business from some fixed place in Australia;
(c) the entity has a website that offers goods or services to countries including Australia;
(d) Australia is one of the countries on the drop-down menu appearing on the entity's website;
(e) web content that forms part of carrying on the business, was uploaded by or on behalf of the entity, in Australia;
(f) business or purchase orders are assessed or acted upon in Australia; or
(g) the entity is the registered proprietor of trademarks in Australia.[96]

However, the APP Guidelines caution that the presence or absence of one of these factors will not be determinative, and provides the example that an entity will not generally be regarded as carrying on business in Australia solely on the basis that a purchase order can be placed in Australia.[97]

Further, APP8 (and section 16C of the Privacy Act 1988 (Cth)) deal specifically with cross border disclosures of personal information. That framework requires the relevant entity to ensure that an overseas recipient will handle the personal information in accordance with the APPs. There are however, exceptions, including where the overseas recipient is subject to a similar protection regime as the APPs, where the disclosure is required or authorized by or under an international agreement relating to information sharing (noting that this does not apply to organizations[98]), or where the entity is an agency and that agency reasonably believes that the disclosure is reasonably necessary for an enforcement related

95. Office of the Australian Information Commissioner, *Australian Privacy Principle Guidelines*, B13 (internal footnotes omitted), available at https://www.oaic.gov.au/resources/agencies-and-organisations/app-guidelines/APP_guidelines_complete_version_1_April_2015.pdf (last visited July 15, 2016).

96. Ibid., B19.

97. Ibid., B20 and B21.

98. Office of the Australian Information Commissioner, *Australian Privacy Principle Guidelines*, 8.47, available at https://www.oaic.gov.au/resources/agencies-and-organisations/app-guidelines/APP_guidelines_complete_version_1_April_2015.pdf (last visited July 15, 2016).

activity by an (Australian) enforcement body and the recipient performs functions or exercises powers that are similar to those of an enforcement body.

H. Impacts of Snowden Leaks on Australia

The amendments to national security legislation by the National Security Legislation Amendment Act 2014 (Cth) also attempted to address potential shortfalls in the provisions addressing the protection of intelligence-related information arising from the leaks of documents revealing surveillance matters by Edward Snowden, a former National Security Agency (NSA) contractor in the United States.[99] While working as a computer analyst, Snowden collected and later leaked to journalists thousands of documents allegedly describing the surveillance activities of the NSA.

The impact on Australia from those leaks is reported to be:

> Australian intelligence agencies are understood to have scoped the potential damage for future leaks from the Snowden affair and have assessed that between 15,000 and 20,000 secret Australian intelligence files could have been accessed by Snowden through his computer at NSA, although it is unknown how many of these he actually stole before seeking refuge in Russia.
>
> The majority of the stolen reports are likely to discuss political, economic and military intelligence gleaned by Australian agencies, especially the Australian Signals Directorate (formerly the Defence Signals Directorate, DSD), in the Asia-Pacific region.[100]

The Australian Signals Directorate is an intelligence agency within the Australian Department of Defence, responsible for collecting and analyzing foreign signals intelligence to support military and strategic decision-making.[101]

Most significantly from an Australian perspective, the documents leaked by Snowden reportedly revealed:[102]

> (a) that Australian diplomatic facilities throughout the Asia-Pacific region were involved in an NSA-led covert signals intelligence

99. Department of Parliamentary Services, *National Security Legislation Amendment Bill (No.1) 2014 Bills Digest* (2014–2015) 19 http://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/bd/bd1415a/15bd019.

100. P. Maley and C. Stewart, "Snowden Stole up to 20,000 Aussie Files," *The Australian* (December 5, 2013), p. 1 http://www.theaustralian.com.au/national-affairs/foreign-affairs/edward-snowden-stole-up-to-20000-aussie-files/story-fn59nm2j-1226775491490, and as reported in Department of Parliamentary Services, *National Security Legislation Amendment Bill (No.1) 2014 Bills Digest* (2014–2015) 19, http://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/bd/bd1415a/15bd019.

101. Australian Signals Directorate, www.asd.gov.au (last visited July 17, 2016).

102. R. Tanter, "Indonesia, Australia and the Edward Snowden Legacy: Shifting Asymmetries of Power," 12(10) *The Asia-Pacific Journal* (2014), http://apjjf.org/-Richard-Tanter/4088/article.pdf.

program codenamed STATEROOM in which surveillance collection units operated within embassies and diplomatic missions to monitor certain signals (microwave, Wi-Fi and satellite signals for example). The documents reportedly demonstrate that data intercepted by STATEROOM in Australian embassies was automatically shared with the NSA.

(b) that the NSA and the DSD conducted a surveillance operation on Indonesia during the United Nations climate change conference in Bali in 2007.

(c) that the DSD monitored and intercepted the 3G cell phone calls of Indonesian president Susilo Bambang Yudhoyono, his wife, and inner circle of advisers. The relevant documents were DSD Powerpoint slides held by the NSA explaining the DSD's achievements in monitoring and intercepting activities in relation to Indonesian leadership targets.

The reported impact of these leaks was not only the revelation of the types of activities the Australian intelligence agencies conduct but also the technical capacities of the ASD and the extent of the collaboration with the US NSA, and caused significant damage to Australia's relationship with Indonesia.[103] The Australian foreign minister responded to the Snowden affair by condemning his actions, seeking to "manage the impact of [our] relationships with others targeted by the Snowden allegations," and commenting that the Australian government is "satisfied with the robust oversight and collection management arrangements that apply to Australia's intelligence activities."[104]

103. Ibid.

104. J. Bishop, "US-Australia: The Alliance in an Emerging Asia" (2014), http://foreignminister.gov.au/speeches/Pages/2014/jb_sp_140122.aspx?ministerid=4.

11

Systematic Government Access to Private-Sector Data in China

ZHIZHENG WANG

I. ABSTRACT

In accordance with facilitating Chinese e-government construction, many laws made for the purpose of state security, public security, censorship, and taxation have granted the Chinese government extensive power of access to private-sector data generated in such businesses as information, finance, trade, travel, entertainment, and so on, operated in China. There are no laws or practices related to governmental systematic access currently found in China. However, this kind of systematic data access will certainly find itself any time in the future enforcement and ensuing legislation once the Chinese government realizes it is necessary with the evolution of e-government strategy.

II. NATIONAL LEGAL CONTEXT AND FUNDAMENTAL PRINCIPLES

Although it is a mixed system,[1] with elements of civil law, common law, socialist law, and to a limited extent, traditional law, and is officially named the Socialist System of Laws with Chinese Characteristics,[2] China's legal system in fact has a formal structure approximately resembling the civil law model despite its distinctive Chinese Characteristics. China is also a very centralized country with a powerful government controlled by the Chinese Communist Party (CCP). The CCP maintains its power of absolute control over the law through its highly effective mechanisms and its absolute majority of members in the three branches

1. Randall Peerenboom, "The X-Files: Past and Present Portrayals of China's Alien 'Legal System,'" 2 *Wash. U. Global Stud. L. Rev.* 37 (2003).

2. White paper released by State Council Information Office, *The Socialist Legal System with Chinese Characteristics* (2011).

of government: the executive, the legislative, and the judicial.[3] Executive officials also make up almost two-thirds of the legislature. Technically, Politics and Law Committees are installed in the CCP at the national and local levels to oversee the direction and cooperation of courts, procuratorate, and police to ensure CCP's leadership over judicial issues.[4] Usually laws are shadows of the CCP's policies, and courts, procuratorate, and police share the same interest.[5] It is often said that "Police prepare all the food, prosecutors serve it, and the courts eat it."[6] In addition, it is the government not the congress that practically plays an initiating, driving, and decisive rule in legislation.[7]

"The People's Republic of China practices ruling the country in accordance with the law and [is] building a socialist country of law,"[8] was first incorporated into the Constitution as a "ruling strategy"[9] in 1999, but rule of law or even rule by law at most is still on the arduous odyssey. As the Chinese delegation described in the 56th session of the United Nations Commission on Human Rights:

> The Chinese society is now in the process of transition from too much emphasis on the rule of person and insufficient emphasis on the rule of law to establishing concept of the rule of law, from supremacy of the power to supremacy of the law, from too much emphasis on duties and insufficient emphasis on rights to establishing a correct notion about rights and obligations.[10]

China was indeed "in transition toward rule of law but still falling short of the minimal standard of achievement required to be considered rule of law"[11] 10 years ago, and the situation remains much the same now and will be not much

3. Xianhong Qin, "CCP's Influence on Legislation" (2001), http://www.usc.cuhk.edu.hk/PaperCollection/Details.aspx?id=2357.

4. Migalhas International, "The Legal System of China" (2007), http://lexuniversal.com/en/articles/3656.

5. Dingjian Cai, *History and Reform: New China's Journey to Legal Construction* (CUPL Press, 1999), at 259.

6. Zhiwei Tong, "Let Sunshine of Constitution Shed on Penal Laws Application" (2010), http://article.chinalawinfo.com:81/article_print.asp?articleid=54698.

7. Jun Feng, "Sixty Years Administrative Legislation: Retrospect and Perspective" (2009), http://www.iolaw.org.cn/showArticle.asp?id=2836.

8. Constitution of the People's Republic of China, Article 5, Amendment 3.

9. White paper released by State Council Information Office, *The Socialist Legal System with Chinese Characteristics* (2011).

10. Delegate Briefs UN Commission on China's Human Rights Achievements (2007), http://english.people.com.cn/english/200004/07/eng20000407_38494.html.

11. Randall Peerenboom, "Let One Hundred Flowers Bloom, One Hundred Schools Contend: Debating Rule of Law in China," 23 *Mich. J. Int'l L.* 471, 525 (2002).

changed in the near future under the current political system of this one-party socialist state unless a substantial political reform takes place.

In 2004, "The State respects and preserves human rights"[12] was included in the Constitution and human rights are thus endowed with a certain legal concept. However, the idea and scope of human rights in China, especially in terms of the official interpretation, is somewhat different from what is universally held in most countries. China stresses the right to development and group rights more than political rights and individual rights. "While China has acknowledged the importance and legitimacy of human rights, it has also challenged the pretense of a universal consensus on human rights issues, or at least the consensus among much of the cosmopolitan elite in economically advanced Western liberal democracies."[13]

Privacy as a fundamental human right is still relatively new to China. In the Chinese language, the word for privacy—"yinsi"—connotes "illicit secrets and selfish, conspiratorial behavior."[14] Furthermore, necessary protection of the right to be let alone is assumed in most people's minds in China to be from fellow citizens rather than from the government because of the long-standing dossiers system, household registration system (*Hukou*), and misleading education and propaganda imposed on people.[15] The awareness of people about governmental intrusion has grown in recent years but is still very vague and weak.[16]

There was not a legal term named "right of privacy" in laws and regulations before the end of 2009 when the new Tort Liability Law was enacted and the word first appeared, but without a definition or further interpretation.[17] It is interesting to note that privacy clearly as a legal right is first present in the Chinese private law instead of the public law because this facet of privacy protection is not related to restriction of government power.

Articles 37, 38, 39, and 40 of the Constitution do promise that the freedom of a person, his dignity, his residence, and the secrecy of his correspondence are "inviolable" and protected from "unlawful" infringements, which altogether indirectly sets a vague privacy protection framework to provide a minimum level of protection for the privacy of the citizen for the purpose of social

12. Constitution of the People's Republic of China, Article 33, Amendment 4.

13. Randall Peerenboom, "Law and Development of Constitutional Democracy: Is China a Problem Case?," 19 *Colum. J. Asian L.* 185 (2006).

14. "China: The Long March to Privacy," *The Economist* (January 12, 2006), http://www.economist.com/node/5389362.

15. Changqiu Liu, "Role of Perception, Awareness and Law in Citizen's Personal Information Protection," *Social Science Weekly* (2009) at 49.

16. Hao Wang, "Legal Consciousness and Root of Chinese Citizen's Right of Privacy Protection," *Journal of Senyang Normal University* (Social Science Edition) (2007) 31(1).

17. Tort Liability Law of the People's Republic of China Article 2.

stability.[18] However, in constitutional law, penal laws, penal litigation laws, state security laws, and other public-sector laws there are many exemption rules and vague definitions that grant government extensive rights and sizable flexibility for investigation, seizure and, search, especially in the matter of state security or keeping social order.[19]

The reasons there is a lack of a more comprehensive and unified privacy and data protection law in China are complex, but the situation is not accidental. Privacy is an interest and a right more important to citizens than to the government. The absence of the real representative system for people's interests, the dominant role of government in legislation, and government's desire to strengthen and extend its power inevitably result in the long time vacancy of privacy protection, which, in turn, benefits and facilitates the construction of a powerful e-government and electronic dossier society. In fact, the surveillance and censorship systems in China, considered to be the largest and most sophisticated in the world,[20] are exactly the confluence of prolonged privacy underprotection and rapid e-government development.

Under the above context, it is really hard to define the boundaries of governmental access to private-sector data, but it's not difficult to conclude that the government's systematic access to data held by anyone will become possible and realistic with the evolution of the e-government strategy in accordance with its vital interest in maintaining the state's control on information and "preserving stability" of the society.

III. STATUTORY AND REGULATORY OVERVIEW

A. Laws Requiring, Explicitly Authorizing, or Restricting Governmental Access to Private-Sector Data

As discussed above, communications privacy is protected from "unlawful" infringements, which are supposed to be committed by citizens not by government. In fact government enjoys an extensive and unrestricted power of investigation and censorship of communications whenever state security or public security is involved. Article 40 of the Constitution provides,

> The freedom and privacy of correspondence of citizens of the People's Republic of China are protected by law. No organisation or individual may, on any ground, infringe upon the freedom and privacy of citizens' correspondence

18. Qianzhe Wang, "On the Constitutional Establishment of Right to Privacy," *Legal System and Society* (2011) 23.

19. Jian Shi, "Reflection and Reconstruction of Criminal Investigation Procedure," *Social Sciences Journal of Colleges of Shanxi* (2004) 16(8).

20. OpenNet Initiative, *Internet Filtering in China* (2009), http://opennet.net/research/profiles/china-including-hong-kong.

> except in cases where, to meet the needs of state security or of investigation into criminal offences, public security or procuratorial organs are permitted to censor correspondence in accordance with procedures prescribed by law.[21]

As for procedures prescribed by law, they either lack explicit interpretation or are not known to citizens. This constitutional provision, in the name of privacy protection, actually becomes the primary source of legal authority for many national laws or departmental regulations related to criminal investigation, censorship, or surveillance, any of which normally involves governmental access to data.

As illustrated below, those kinds of governmental access to data are usually explicitly authorized, and there are no explicit restrictions.

1. State Security Law (1993)

Because of the particular importance attached to state security and social stability by the Chinese government, China's State Security Law is instrumental in the role of authorizing governmental access to the private-sector data, and its legislative foundation is laid according to Articles 1, 4, 28, 36, 51, and 54 of the Constitution, which prohibit the sabotage of the socialist system; acts detrimental to the security, honor, and interests of the motherland; and infringement upon the interests of the state, of society, and of the collective.[22]

There are two articles in the State Security Law permitting the state security organization to accede, when necessary, to any information or data held by anyone in China. Article 11 stipulates that "where state security requires, a state security organisation may inspect the electronic communication instruments and appliances and other similar equipment and installations belonging to any organisation or individual,"[23] and Article 18 states "When a State security organisation investigates and finds out any circumstances endangering State security and gathers related evidence, citizens and organisations concerned shall faithfully furnish it with relevant information and may not refuse to do so."[24] The only restriction for this access is that state security officials must go through their own internal strict approval procedures in accordance with the relevant provisions of the state.[25]

The Penal Law of China further makes a crime the refusal to provide information. Article 311 requires "Whoever, while clearly knowing that another person has committed a crime of espionage, and when a state security organisation inquires him about relevant circumstances and collects relevant evidence from him, refuses to provide them shall, if the circumstances are serious, be sentenced

21. Constitution of the People's Republic of China Article 40.

22. Constitution of the People's Republic of China article 1, article 4, article 28, article 36, article 51, and article 54.

23. State Security Law, art. 11.

24. State Security Law, art. 18.

25. State Security Law, art. 10.

to fixed-term imprisonment of not more than three years, criminal detention or public surveillance."[26]

2. Law of Guarding State Secrets (2010 Revision)

Article 28 of Law of the People's Republic of China on Guarding State Secrets (2010 Revision) stipulates that "Operators and service providers of the Internet or any other public information network shall cooperate with the public security organisation, the national security organisation and the procuratorial organisation in the investigation of secret leakage cases. Where any operator or service provider finds that any information disclosed via the Internet or any other public information network involves any state secret, it shall immediately stop transmitting it, keep the relevant records, and report to the public security organisation, national security organisation or secrecy administrative department. Operators and service providers shall delete information which involves state secrets as required by the public security organisation, the national security organisation or the secrecy administrative departments."[27]

3. Criminal Procedure Law of the People's Republic of China (2012 revision)

Search and seizure procedure is found here in sections 5 and 6 of this law. Any belongings related to crime are subject to search, and any evidence including material evidence and documentary evidence shall be seized. The search warrants are obtained not from court but through their own internal approval procedures or may not be required if an emergency occurs when an arrest or detention is being made.

> Article 101 Investigators shall conduct an inquest or examination of the sites, objects, people and corpses relevant to a crime. When necessary, experts may be assigned or invited to conduct an inquest or examination under the direction of the investigators.
>
> Article 109 In order to collect criminal evidence and track down an offender, investigators may search the person, belongings and residence of the criminal suspect and anyone who might be hiding a criminal or criminal evidence, as well as other relevant places.
>
> Article 110 Any unit or individual shall have the duty, as required by the People's Procuratorate or the public security organ, to hand over material evidence, documentary evidence or audio-visual material which may prove the criminal suspect guilty or innocent.
>
> Article 111 When a search is to be conducted, a search warrant must be shown to the person to be searched. If an emergency occurs when an

26. Penal Law of China, art. 311.

27. Law of the People's Republic of China on Guarding State Secrets, art. 28.

> arrest or detention is being made, a search may be conducted without a search warrant.

The electronic data is included as evidence in the newly amended version passed by the National People's Congress on March 14, 2012. The phrase of "respecting and protecting human rights" is also included in this revision, but is considered by many legal scholars as an empty promise because this new amendment vests more powers than ever before in the public security and state security organization.[28]

B. Separate Laws for Law Enforcement Access, Regulatory Access, and/or National Security Access

The core part of the above-mentioned surveillance and filtering system is the well-known golden shield project run by the Ministry of Public Security (MPS). There are another 11 nationwide golden projects[29] managed or overseen by other relative government departments such as the State Administration of Taxation, China Customs, the People's Bank of China (PBOC), Ministry of Industry and Information Technology (MIIT), etc. The 12 golden projects together with "two networks,"[30] "one website,"[31] and "four databases"[32] are a series of ambitious initiatives to build an advanced e-government as a national informatization process. These projects and databases are loosely based on a framework set by Guiding Opinion on Construction of E-Government in our Country by the State Informatisation Leading Group (2002). This Opinion is technically of a very low level legal authority but quite crucial in actual authorization of government access to private-sector data in the name of e-government "designed to reinforce its surveillance capabilities."[33] Accordingly, all the provinces have enacted their own local Informatisation Rules to join the informatization process.

28. "China Passes New Law Allowing Secret Detentions," *CNN* (March 14, 2012), http://edition.cnn.com/2012/03/14/world/asia/china-criminal-law/; see also "Article 73 Sparks Controversy on Secret Detentions," *Caixin* (March 12, 2012), http://www.caixinglobal.com/2012-03-12/101015879.html.

29. "Golden Macro Economy, Golden Tax, Golden Customs, Golden Finance, Golden Cards, Golden Auditing, Golden Insurance, Golden Agriculture, Golden Bridge, Golden Quality, Golden Travel, Golden Medical" *Sina* (2009), http://tech.sina.com.cn/it/2009-09-15/20423440557.shtml.

30. One intranet for internal use, one extranet connected with the Internet.

31. Government portal site.

32. Basic Population Information Database, Basic Legal Person Information Database, Natural Resource, Space and Geography Information Database, Macro Economy Information Database.

33. Jeffrey Seifert et al., "Using E-Government to Reinforce Government–Citizen Relationships: Comparing Government Reform in the United States and China," *Social Science Computer Review*, Vol. 27, No. 1, http://unpan1.un.org/intradoc/groups/public/documents/un-dpadm/unpan043654.pdf.

One of the four databases is the national Basic Population Information Database by the MPS. It is based on the resident identification system, which has the basic information of 1.3 billion people.[34] The individual fingerprint will be included in the ID system in the near future.[35] Besides the four databases, other databases include the national Individual Credit Information Database,[36] completed in 2006[37] and overseen by the PBOC; and the Basic Internet Database coordinated by the MPS and being built by local police at the provincial level.[38]

The Basic Internet Database is mainly made of data collected monthly since 2006 from ISPs (Internet Service Providers), ICPs (Internet Content Providers), IDCs (Internet Data Centers), and email services.[39] No explicit authorization for building this database can be found in any laws, and there are only orders from local police compelling the businesses to submit monthly reports with a data collection template designed by the MPS.[40] The data collected include all users' account and registration information, both individual and corporate, and other data in which the government is interested.[41]

Building those projects and databases involves systematic data digitalization and data collection of almost every aspect of a person's life. Data held in the private sector are compelled to contribute to the projects and databases in accordance with the e-government construction based on requirements of various laws related to public security, state security, finance, taxation, insurance, and so on.

The vague language and exemption rules in many laws and regulations give the government substantial flexibility and higher demand for data access. What is more, extensive mandatory data retention imposed on telecommunications, ISPs, ICPs, and IDCs increase much ease of this government access to data.

All of the kinds of governmental access discussed above or below, with explicit mandate or not, take the form of a mediated report that is obviously not the

34. National Health and Family Planning Commission of the PRC, "Q&A: Guiding Opinions on Accelerating Population Health Information Construction" (2013), http://www.nhfpc.gov.cn/guihuaxxs/s10742/201312/2519dea9a4b14318a0736881116275ee.shtml.

35. Cao Yin, "ID Cards May Carry Fingerprint Data," *China Daily* (Oct. 25, 2011), http://www.chinadaily.com.cn/china/2011-10/25/content_13966191.htm.

36. Built according to Interim Measures for the Administration of the Basic Data of Individual Credit Information.

37. "Individual Credit Information Database Covers 570 Mln Persons," *Xinhua News Agency* (August 30, 2007), http://www.china.org.cn/china/national/2007-08/30/content_1222501.htm.

38. *A Notice for Collection of Data in the Name of Security Inspection from Inner Mongolia Public Security Bureau* (Retrieved: March 7, 2012).

39. Ibid.

40. Templates found in the compressed file (Retrieved: March 7, 2012), http://huhehaote.cyberpolice.cn/news/2008-10-8-102831.rar.

41. Ibid.

systematic access we mean here. One reason for the absence of systematic access and relative laws may be the government's efforts to accelerate the adoption rate of cloud service in China.[42] However, observing the way and practice of e-government construction ongoing, we can imagine that the systematic access will find its way in one form or another once the government realizes it is necessary, and e-government evolves into a new stage.

1. Accounting Law

Article 35 of Accounting Law of the People's Republic of China (1999 Revision) requires "all units must . . . accept the supervision and inspection . . . by the relevant supervisory and inspection departments" and "honestly furnish accounting documents, account books, financial accounting statements and other accounting materials and relevant situations, and may not refuse inspection, conceal materials or report falsely." The relevant supervisory and inspection departments include "departments in charge of finance, auditing and taxation, the people's banks as well as securities regulatory and insurance regulatory authorities."[43]

All companies no matter whether publicly listed or not are subject to this supervision. This law also gives different government departments the right to gain access to private-sector data.

2. Tax Laws

One of China's taxation administration regimes is invoice management.[44] Since early 2001,[45] most of the businesses involved in the sale of products and services have been forced, in the name of the taxation reform starting from Beijing and three other provinces,[46] to buy certified fiscal cash registers called tax-control cashier in China to record detailed business transactions and invoice use including many personally identifiable pieces of information.[47] Those recorded data are required to be stored in an IC card to send regularly to local taxation authorities.[48]

42. *The State Council's Opinion on Promoting Innovative Development of Cloud Computing and Breeding New Business Patterns of Information Industry* (2015), http://www.sic.gov.cn/News/473/5471.htm.

43. Accounting Law of the People's Republic of China, art. 35.

44. Invoice Management Measures of the People's Republic of China.

45. "Chaos of Tax Control Devices Result in Fall of Top Beijing Local Taxation Officials" (2011), http://finance.sina.com.cn/roll/20110915/053210482508.shtml.

46. Ibid.

47. *Notice of the State Administration of Taxation on Printing and Distributing the Opinions on Promoting Application of Tax Control Devices and Cashiers* (2004), http://www.chinatax.gov.cn/n810341/n810765/n812193/n812983/c1202387/content.html.

48. *Operator's Manual of Tax Control Cashier* (2006), http://www.chinaacc.com/upload/news/2006/1/27/lvxin7118200612715481642090.doc.

The taxation authority can also use a taxation management access card to collect those data from the tax-control cashier.[49] This practice is authorized by Article 23 of Law of the People's Republic of China on the Administration of Tax Collection and the Notice[50] from the State Administration of Taxation to provincial taxation authorities in accordance with the building of the Golden Tax Project, one of China's 12 e-government projects mentioned above.[51] "Promotion of using online invoice management system" is included in the Invoice Management Measures of the People's Republic of China when amended 2010.[52]

3. Internet-Related Laws

As indicated below, the public security organizations and other various government departments have been given extensive powers in the name of protection of information security by a series of computer, Internet, and telecommunication laws to censor the "illegal and harmful" content and to investigate criminal activities. These laws will be significant in helping government gain the systematic data access in the future when deemed necessary.

For example, according to current regulation, any Internet Data Center (IDC) and web hosting services must be licensed and required to verify, record, and report actual users' information and online activities.[53] In some provinces and local municipalities IDC services are even required to provide police with an administrator account for regular inspection.[54]

An order dated April 11, 2011, from local police of Langfang, a small city near Beijing, explicitly requires any businesses or institutions providing nonprofit Internet access service in a public place, such as shops, hotels, restaurants, bars, bookstores, schools, etc., to install police-licensed monitoring software, in the name of computer security, to record customers' identities and Internet activities and send those recorded data to the police system in real time.[55]

49. Ibid.

50. *Notice of the State Administration of Taxation on Printing and Distributing the Opinions on Promoting Application of Tax Control Devices and Cashiers* (2004), http://www.chinatax.gov.cn/n810341/n810765/n812193/n812983/c1202387/content.html.

51. *Tax Control Device for the Golden Tax Project* (2006), http://www.csj.sh.gov.cn/pub/xxgk/zcfg/swzsgl/200609/t20060907_284636.html.

52. Invoice Management Measures of the People's Republic of China, art. 23.

53. Regulation on Telecommunications of the People's Republic of China, art. 7; see also Regulation on Internet Information Service of the People's Republic of China, arts. 4 & 14.

54. Changzhou Municipal Measures of Administration of Data Center, art. 15; see also Baoding Municipal Measures of Security Administration of Data Center, art. 15.

55. *Notice from Langfang Public Security Bureau on Further Implementing Security Measures for Nonprofit Internet Service Providers* (2011).

4. Regulation on Internet Information Service of the People's Republic of China (2000)

This law promulgated by the state council imposes mandatory data retention on many Internet- related businesses and grants many government departments power of access to data retained.

It requires that "Internet information service providers that engage in the provision of such services as news, publishing, or electronic bulletin board services, etc. shall keep a record of the information they provide, the times of dissemination and the URLs or domain names. Internet access service providers shall keep a record of such information as the times online subscribers are online, the subscribers' account numbers, the URLs or domain names, the callers' telephone numbers, etc. Internet information service providers and Internet access service providers shall keep copies of such records for 60 days and shall provide them to the relevant State authorities when the latter make inquiries in accordance with the law."[56]

5. Provisions on the Technical Measures for the Protection of the Security of the Internet 2005

These provisions enacted by the MPS further include IDCs into data retention. Any ISPs, ICPs, and IDCs are required to record and keep for at least 60 days the users' registration information, web addresses visited, IP addresses, time stamp, content published etc. for the possible use of police later.[57] Furthermore, a BBS service provider must have "the function of auditing the information as registered by users and information as publicised."[58] The law authorizes the public security organization to "offer guidance to and carry out supervision and examination" on the implementation of the cybersecurity measures.[59]

6. Regulations on the Administration of Business Sites of Internet Access Services 2002

This law governs Internet cafes and similar places and vests both the MPS and culture authority the power of access to data. Article 23 requires that "An operating entity shall verify and register the identification cards or other valid certificates of the Internet users, and shall record the relevant net information. The registration and records reserved shall be kept for at least 60 days, and shall be provided when the departments of culture administration or public security consult them pursuant to law. The registration and records reserved may not be

56. Regulation on Internet Information Service of the People's Republic of China, art. 14.

57. Provisions on the Technical Measures for the Protection of the Security of the Internet, art. 10.

58. Provisions on the Technical Measures for the Protection of the Security of the Internet, art. 9.

59. Provisions on the Technical Measures for the Protection of the Security of the Internet, art. 16.

modified or deleted during the period of keeping."[60] The actual practice is to send those recorded data to the police system in real time.[61]

7. Interim Measures for the Trading of Commodities and Services through the Internet 2010

This regulation governs online sales and is promulgated by the State Administration for Industry and Commerce. It requires that "A network trading platform service provider shall file operating statistics about network commodity transactions and the relevant services with the local administrative department for industry and commerce on a regular basis."[62]

The mandatory data retention in this interim law requires that a network trading platform service provider shall examine, record, and retain the information about network commodity transactions. Information about the business license or individual identity of a business operator shall be preserved for at least two years from the date when the business operator is removed from the network trading platform. The backups of trading records and other information shall be retained for at least two years from the date when a transaction is concluded.[63]

8. Measures for the Administration of Internet E-mail Services 2006

These measures by the MIIT provide that "Citizens' privacy of correspondence in using Internet e-mail services shall be protected by law. Unless the public security organisation or procuratorial organisation makes an inspection on the contents of correspondence pursuant to the procedures prescribed in law when required by national security or investigation of crimes, no organisation or individual shall infringe upon any citizen's privacy of correspondence on any pretext."[64]

"The procedures prescribed in law" are not, as usual, further detailed. The exemption rule and vague expression of language virtually grants the police much room to gain access when the police consider it necessary. Actually there is an email data collection template designed by the MPS required to report to police on a monthly basis.[65]

60. Regulations on the Administration of Business Sites of Internet Access Services, art. 23.

61. Wang Na, "Real Time Monitoring on Computers in Internet Cafe to Be Installed within the Year" (2006), http://www.china.com.cn/zhuanti/2006/wldd/txt/2006-05/14/content_6208216.htm.

62. Interim Measures for the Trading of Commodities and Services through the Internet, art. 30.

63. Ibid. art. 29.

64. Measures for the Administration of Internet E-mail Services, art. 3.

65. Collection Template for Email Service found in the compressed file (Retrieved: Mar. 7, 2012), http://huhehaote.cyberpolice.cn/news/2008-10-8-102831.rar.

9. Interim Provisions on the Administration of Internet Culture (2011 Revision)

This law enacted by the Ministry of Culture governs online music, online games, online shows, online works of art, online cartoons, etc. Article 20 stipulates that "an Internet cultural entity shall record the contents in the back-up of the cultural products, the time and Internet web address or domain name of the back-up. The back-up of the records shall be kept for 60 days, and be provided when the relevant department of the state makes an inquiry in accordance with the law."[66]

10. Interim Provisions on the Administration of Internet Publication 2002

This provisions jointly promulgated by the General Administration of Press and Publication and the former Ministry of Information Industry (MII), now the MIIT, govern online books, newspapers, periodicals, audio and video products, electronic publications, etc. Article 22 requires that Internet publishers shall keep a record of the published contents, time, and IP address, and the record shall be kept for 60 days and be provided when the relevant departments of the state make inquiries pursuant to law.[67]

11. Provisions for the Administration of Internet News Information Services 2005

Article 21 provides that an Internet news service provider shall record the contents of the news information it has published or transmitted, the time, etc. The backup of the records shall be preserved for at least 60 days, and be provided when the relevant department inquires them in accordance with the law.[68]

12. Management Provisions on Electronic Bulletin Services in Internet 2000

Enacted by the former MII, this department rule governs BBS, online chat, and other online interactive service. It requires that user accounts, interactive contents, time stamp, and telephone number, and other information be recorded and kept for 60 days, and be provided when the relevant state organization inquires about them.[69]

66. Interim Provisions on the Administration of Internet Culture, art. 20.

67. Interim Provisions on the Administration of Internet Publication, art. 22.

68. Provisions for the Administration of Internet News Information Services, art. 21.

69. Management Provisions on Electronic Bulletin Services in Internet, art. 14.

13. Several Provisions on Regulating the Market Order of Internet Information Services 2011

Article 11 of this law is another example of an exemption rule for government access and states that "without obtaining the permission of users, an Internet information service provider may not collect information which is relevant to users and can serve to identify users solely or in combination with other information (hereinafter referred to as the "personal information of users"), and nor may it provide the personal information of users to others, unless it is otherwise provided by laws or administrative regulations."[70]

This law was issued at the end of 2011—shortly after a widespread leakage of accounts (including emails) and passwords affecting more than 10 million users of several Chinese websites[71] to appease the wild anger of Chinese netizens. The leakage is said to be a protest against the real name registration regulation for microblogs (Chinese social media like Twitter) effective from March 2012.[72] Most people couldn't understand why passwords were stored without even a simple encryption in those commercial websites. It was rumored that the unencrypted practice of password storage was required by police for their convenience of access. Considering Tom-Skype (Skype in China) practice[73] leaked in 2008, the rumor is not really ungrounded.

As for the intelligence access, there is no unified law or much regulation governing intelligence activities. Due to China's special political system, all government and semi-government agencies including press might be mobilized to collect and analyze intelligence for governmental decision-making although there are sometimes no explicit legal mandates. For example, *People's Daily*, a national newspaper, has established a department and uses software to monitor and collect users' comments, opinions, and sentiments about government through its news portal as a kind of intelligence for government.[74]

Generally speaking, the Chinese intelligence system is primarily made up of the military intelligence service and the state security organization and public security organization. The state security organization is similar to the CIA but enjoys law enforcement powers including arrest, search, and seizure according

70. Several Provisions on Regulating the Market Order of Internet Information Services, art. 11.

71. Lea Yu and Xuyan Fang, "100 Million Usernames, Passwords Leaked," *Caixin* (December 29, 2011), http://www.caixinglobal.com/2011-12-29/101016125.html.

72. "12 Detained or Punished over Fabricating Massive Leak of Online Personal Data" *People's Daily Online* (January 11, 2012), http://english.people.com.cn/90882/7701857.html.

73. John Markoff, "Surveillance of Skype Messages Found in China," *The New York Times* (October 1, 2008), http://www.nytimes.com/2008/10/02/technology/internet/02skype.html.

74. For details of the department see http://yq.people.com.cn/service/index.html.

to the State Security Law and Criminal Procedure Law.[75] Based on broad definitions and interpretations from the various laws about public security, state security, and defense the public security organizations are mainly responsible for domestic intelligence whereas the state security organizations and military intelligence service are responsible for foreign intelligence including Taiwan and Hong Kong. The construction of the Basic Internet Database noted above is part of the so called "greater intelligence" strategy employed by the MPS.[76]

C. Laws Requiring Broad Reporting of Personal Data by Private-Sector Entities

1. Anti-money Laundering Laws

Article 3 of the Anti-Money Laundering Law of the People's Republic of China 2006 requires that all financial institutions inside China "develop and improve the system for client identity identification, system to keep the materials of client identity and trading record, and system to report large amount trading and suspicious trading, and implement their duties of anti-money laundering."[77] The Measures on the Administration of Client Identity Identification and Materials and Transaction Recording of Financial Institutions further stipulates that a financial institution shall "appropriately preserve client identity materials and transaction records, guarantee that each transaction be reflected, so as to provide information needed" and "so as to facilitate anti-money laundering investigation, supervision, and administration."[78]

The Anti-Money Laundering Monitoring Analysis Centre (CAMLMAC), as China's Financial Intelligence Unit (FIU), was established in 2004 according to the requirement of the Anti-Money Laundering Law. CAMLMAC is operated under the central bank the POBC and is the main agency authorized to collect and analyze reports of large and suspicious transactions from all financial institutions, including banks, insurances, securities, fund managements, etc. and some other specific non-financial institutions such as payment and clearing organizations.[79]

Accounting firms and law firms, pawn stores, lotteries, and sales of real estate, jewelry, and precious metals are classified as specific non-financial institutions according to the law, have not been immediately incorporated into the

75. State Security Law of the People's Republic of China, art. 26; Criminal Procedure Law of the People's Republic of China, art. 4.

76. See http://www.pzhga.com/c/24/2308.html; see also http://www.mps.gov.cn/n2256871/n2256873/c5105621/content.html.

77. Anti-Money Laundering Law of the People's Republic of China, art. 3.

78. The Measures on the Administration of Client Identity Identification and Materials and Transaction Recording of Financial Institutions, art. 3.

79. http://www.camlmac.gov.cn/com/info.do?action=detail&id=183.

transaction-reporting mechanisms, and may be required to comply with anti-money laundering rules and regulation in the future.[80]

In addition, for the last few years, a considerable number of regulations and rules have been made to provide more detailed directions. Currently, large-value and doubtful transactions are required to send reports regularly to local branches of the POBC electronically.[81]

Under the pressure of supervision and inspection and in fear of missed reports of suspicious transactions, many financial institutions report indiscriminately to the CAMLMAC large amounts of ordinary transactions. The CAMLMAC collects more than 50 million reports annually, of which only a few are useful data for anti-money laundering operations.[82]

China has joined several international anti-money laundering conventions including the United Nations Convention against Transnational Organised Crime, United Nations Convention against Transnational Organised Crime, and United Nations Convention against Corruption.[83]

2. Measures for the Control of Security in the Hotel Industry 1987

Measures for the Control of Security in the Hotel Industry 1987 by the MPS require "A hotel shall register guests" and "the guest's identification card shall be examined and an accurate registration of all stipulated items shall be made. If accommodation is provided to a foreign guest, the accommodation registration form shall be submitted to the local public security organisation within 24 hours of the guest's arrival."[84] It also authorizes provincial, autonomous region, and directly administered municipal public security departments to formulate detailed implementing rules.

All provincial detailed rules enacted require hotels to upload within two hours the detailed registered personal information of both domestic and foreign guests including photos and credit cards to the Hotel Public Order Administration Information System controlled by the MPS formerly through certified desktop software and now through websites.[85] The Hotel Public Order Administration

80. Director's Speech on Financial Intelligence in 2005 (Retrieved March 7, 2012), http://www.camlmac.gov.cn/com/info.do?action=detail&id=180.

81. Administrative Measures for the Financial Institutions' Report of Large-Sum Transactions and Doubtful Transactions, arts. 7, 8, and 17.

82. "A Survey and Suggestion on the Anti-Money Laundering Report System" (December 31, 2011), http://www.zjfn.com.cn/infoweb/wnewsdetail.asp?id=3672; see also "More than 50 Million Suspicious Reports Received Annually," *21st Century Network* (December 14, 2011), http://finance.jrj.com.cn/2011/12/14092411827388.shtml.

83. See *CAMLMAC Introduction* (Retrieved March 7, 2012), http://www.camlmac.gov.cn/com/info.do?lmId=15&action=query.

84. Measures for the Control of Security in the Hotel Industry, art. 6.

85. Shanghai Municipal Detailed Rules for Public Security Administration in Hotel Industry, art. 11.

Information System is closely related with the Basic Population Information Database and other databases such as motor vehicles management system, criminal information system, etc. in the police system.[86]

3. Interim Measures for the Administration of Air Transport Itineraries/Receipts of E-tickets (2008)

It stipulates that the electronic data of itineraries/receipts of passengers shall be properly kept by the distributing entities as authorized by the Civil Aviation Administration of China for five years, and after the expiration of that period, that data shall be eliminated after being reported to and approved by the Civil Aviation Administration of China and the State Administration of Taxation.[87]

In addition, all Chinese passengers' information is processed by a state-owned company called TravelSky and connected with the airport security system.[88]

4. Regulation on the Administration of Entertainment Venues 2006

The "Entertainment Venues" refers to the singing, dancing, and gaming places that are operated for profit and are open to the general public and for the self-entertainment of consumers.[89] This regulation requires that these places shall keep the video materials as recorded down by the closed circuit television for 30 days for future investigation, and shall not delete them or use them for other purposes.[90] These places are also required to establish a roster of working staff members, which shall indicate the true names and photocopies of identity cards, and to set up a log of business operations that indicates the duties, working hours, and working places of its working staff, and shall not delete or alter the log of business operations, and shall keep it for 60 days.[91]

Measures for the Public Security Administration of Entertainment Venues by the MPS further requires these businesses "to cooperate with the public security organ in establishing an information system for public security administration of Entertainment Venues according to the relevant provisions on informatisation of the State, and input, at real time and faithfully, the information on the working staff, log of business operations and safe patrolling, and transmit and report it to the public security organ."[92]

86. See Beijing Wen Tong Technology Co., Ltd., *Solution for Hotel Security Information System* (2010), http://www.99rfid.com/fangan/NewsList.Asp?DonforType=628002868072010102516l0.

87. Interim Measures for the Administration of Air Transport Itineraries/Receipts of E-tickets, art. 23.

88. See http://www.travelsky.net/publish/english/index.html.

89. Regulation on the Administration of Entertainment Venues, art. 2.

90. Ibid. arts. 15, 32.

91. Ibid. arts. 25, 32.

92. Measures for the Public Security Administration of Entertainment Venues, art. 26.

D. Laws Permitting or Restricting Private-Sector Entities from Providing Government Officials with Voluntary Broad Access to Data

There are no laws currently governing this issue. The government can always find an excuse or reason to gain data access through the vague language of relative laws. In other cases private-sector entities might provide government officials with voluntary broad access to data in seeking favorable policy or government investment.

E. Role of the Courts for Major Categories of Data

The role of courts in China is minor as long as the government is involved.[93]

F. Standards for Use

As noted above, most of data acquired have been used to build the e-government projects and databases. The Guiding Opinion on Construction of E-Government and provincial Informatisation rules encourage interdepartmental data sharing to reduce costs and to maximize utilization of the resources except when state secrets are involved.[94]

The Anti-Money Laundering Law and Statistics Law do clearly impose a restriction of use solely for anti-money laundering or survey purpose.[95]

G. Cross-Border and Multi-jurisdictional Issues

Current China laws only claim jurisdiction on corporations with data servers established inside China. There are no laws found on governing cross-border data flow.

93. GWU Professor Donald Clarke even said, "The courts are not necessarily where you would go to seek justice in China." This is particularly true if a criminal case, or if public or state security is involved. As noted earlier, courts always accept what the police prepare.

94. Guiding Opinion on Construction of E- Government and provincial Informatization § 2.

95. Law of the People's Republic of China on Anti-money Laundering, art. 5; Statistics Law of the People's Republic of China, art. 25.

12

Systematic Government Access to Private-Sector Data in India*

SUNIL ABRAHAM

I. ABSTRACT

India does not have many laws that explicitly prescribe or prohibit systematic government access to private-sector data apart from some provisions in laws such as the Information Technology Act, Anti-Money Laundering Act, and Epidemic Diseases Act. Security consultants and employees of private-sector organizations impacted by such regulation who spoke under conditions of anonymity did not agree regarding the existence and scope of systematic government access. Security consultants paint a picture of comprehensive and unfettered access to databases of personal information, while employees claim strict adherence to the letter and spirit of the law both in terms of proactive and reactive systematic access to data. The truth must lie somewhere in-between.

The appetite in some parts of the government for systematic access appears to be growing. In February 2012, the Intelligence Bureau (IB) wrote to the Department of Telecom demanding that telecom operators and ISPs cooperate to enable comprehensive real-time tracking of Internet usage on mobile phones. This included plans for India-centric "Skype" for use by government officials and to address national security and the establishment of a core group "for finalisation of Internet Protocol Detail Record (IPDR) for Internet and GPRS service, and standardisation of parameters that will have to be stored by mobile phone companies in a log."[1] This is because apparently the telecom operators and ISPs were unable to identify mobile customers who had visited specific websites.

* *Editor's Note: This chapter has not been updated since originally published in 2012.*

1. ET Bureau, "Intelligence Bureau Want Telcos to Keep Eye on Internet Traffic on Mobile Phones," *The Economic Times* (February 23, 2012), *http*://articles.economictimes.indiatimes.com/2012-02-23/news/31091065_1_phones-ip-internet-usage.

Bulk Collection. Fred H. Cate and James X. Dempsey.

A month later, a national newspaper obtained documents that revealed that the government was planning amendments to the operator licenses to ensure real-time monitoring of "location data" of all mobile phones.[2] Combined with large scale surveillance projects in the Unique Identity (UID), National Population Registry (NPR), NATGRID, and CMS project, it would be fair to say that systematic access of private-sector data in India is growing steadily. This chapter provides an overview of the policies and practices around systematic access.

II. NATIONAL LEGAL CONTEXT AND FUNDAMENTAL PRINCIPLES

In India, the Constitution establishes a federal structure of governance comprised of a central government and multiple national states. Both the central government and the states have various levels of legislative and executive authority. The Indian Constitution also establishes a framework for the judiciary that is composed of the Supreme Court, High Courts, and subordinate courts that exist at the state and substate level. In this system courts are granted jurisdiction over issues found in both federal and state laws, while the higher judiciary is empowered to take decisions on constitutional issues. Additionally, a range of tribunals and special courts have been established with authority over specific sectoral issues.

Provisions defining what information can be disclosed and accessed by a government in Indian law are typically found under specific sectoral legislation, and are reflections of an intent to protect a broad and fundamental right to privacy. Currently, in India there is no explicit or fundamental right to private and no horizontal privacy law. Instead, various statutes covering other subject matters contain provisions that either implicitly or explicitly protect privacy rights. In addition, the right to privacy has been read into the Constitution of India by the Supreme Court as a component of the right to life and personal liberty under Article 21. The Indian judicial system has also addressed a right to privacy. A recent example of this is the Naz Foundation case. In 2009, the Delhi High Court reinterpreted Section 377 of the Indian Penal Code, which up until this point in time was routinely used to criminalize homosexuality in India. A critical aspect of the ruling was the court's recognition of the citizen's fundamental right to privacy. However, in 2013 the Supreme Court of India overturned the decision on the basis that only the parliament can change a law.

Currently, the Department of Personnel and Training (DoPT) and the Ministry of Law have been working on a draft privacy bill. Several versions of the draft bill have leaked. When the bill becomes law it would serve as the umbrella of privacy legislation, defining key principles and instituting the office of the ombudsman or privacy commissioner. In the absence of such overarching privacy legislation,

2. Atideb Sarkar, "Soon, Govt Will Keep Track of Where Every Mobile User Is," *The Indian Express* (February 16, 2012), http://www.indianexpress.com/news/soon-govt-will-keep-track-of-where-every-mobile-user-is/912681/0.

questions of jurisdiction and boundaries of governmental access to private-sector data are currently defined predominantly through case law, other sectoral acts and rules, and executive orders. But not all sectors have addressed the question. For instance, there is no explicit policy or case law addressing government access to images captured on CCTV cameras by private companies. Furthermore, sectors that have defined boundaries have defined them at varying levels. For example, in the financial sector, there are provisions that clearly limit governmental access to information held by private companies, whereas in the telecommunications sector a multi-tiered blanket surveillance regime exists.

III. STATUTORY AND REGULATORY OVERVIEW

In the context of governmental access and disclosure to information held by the private sector, there are legal requirements for private industry to report transactions to the government in order to prevent the carriage of offenses, and to protect public order and health. For example, typically all employers must disclose business transactions to the government, doctors must report the occurrence of specific diseases, and banks must report suspicious transactions that could be connected to money laundering. A growing global trend, though, that has also begun in India, is systematic governmental access, disclosure, retention, and collection of information for the purposes of surveillance, national security, and crime detection.

The four mechanisms—access, disclosure, collection, and retention—are interrelated, but signify different levels of surveillance. Systematic access often bypasses traditional safeguards in place to protect against excessive access to information by the government. Systematic disclosure is based on a requirement from the government that the private entity routinely disclose information. Proactive disclosure by default allows systematic access by the government. Augmenting the extent of systematic access and disclosure of information are data collection and retention standards. The more information collected, the longer the retention of information, the more information available for access or disclosure to the government.

In India, the adoption of these practices is slowly being incorporated into already established legislation through rules and amendments, is emerging in draft legislation, and at the same time is largely being practiced outside the legislative scope. Each sector in India has a set of laws that establishes provisions regulating governmental access to information held by businesses. In some cases, like for the telecommunication sector, governmental access bypasses traditional safeguards, whereas in other cases the access still must be mediated and substantiated with a court order.

A. Systematic Access

In India, systematic access to information by the government does not necessarily entail a complete bypassing of traditional safeguards, but is enabled instead

through generic application of provisions, extended data retention periods, and broad collection of data. Three bodies of Indian law that enable systematic access to information by the government include legislation pertaining to: traditional search and seizure, banking and securities, and health.

B. Search and Seizure Law

The government has always had generic access to information held by private entities via the technologically neutral Section 91 of The Code of Criminal Procedure, 1973 (CrPc),"any court or any officer in charge of a police station" to issue "summons to produce document or other thing" and Section 92, which enables "commissioner of police or District Superintendent of police" to "cause search to be made for and to detain such document, parcel or thing pending the order of a document, parcel or thing." Even today, law enforcement officials approach private-sector organizations using CrPc Section 91 and 92, instead of relevant sections under the appropriate legislation. Though access to information under the CrPc is subject to traditional safeguards, as a court order must be issued by a magistrate before accessing information, the generic use of the provision transforms it into a policy tool that can be used for systematic access.

C. Banking Law

Under the Reserve Bank Act, the Reserve Bank of India (RBI) is the authority responsible for collecting information. For the government to access documents, it must either request access from the Reserve Bank, or obtain a court order and request information from the banking branches themselves. As a safeguard to access, the provisions of the Bankers Book Evidence Act applies to all information or documents maintained by the system provider. Under the Bankers Book Evidence Act, banks are not compelled to produce a Bankers Book in a case to which they are not a party—unless ordered to by a court or judge. The RBI is allowed to disclose information only in four instances: (1) protect the integrity, effectiveness, and security of the payment system; (2) in the interest of banking or monetary policy; (3) in the operation of the banking system; (4) or in the public interest. System providers are allowed to disclose information in only three instances: (1) when it is required under the provisions of the Act; (2) if it is expressly consented to by the system participant; or (3) if it is in obedience to the orders passed by a court or statutory authority.

The Reserve Bank Act established the Know Your Customer (KYC) norms as a transparency and accountability measure for clients. The purpose of the KYC norms is to enable banks to monitor customer transactions in order to detect illegal activities such as ghost accounts [Benami], tax fraud, money laundering, financing of terror, and phishing. According to the KYC norms, full details of the name and address as well as copies of ID documents must be kept on record. Banks are permitted to create customer profiles based on risk categorization that

include information pertaining to the customer's identity, social and financial status, nature of business, and clients. Banks must also monitor and proactively disclose complex large transactions, and all unusual patterns that do not seem to have an economic or lawful purpose. All transaction records are to be retained for at least five years. Banks must ensure that a record of transactions in the accounts is preserved and maintained. Access to KYC information is currently governed by the regulations in the Reserve Bank Act, which requires a court order for access.

D. Securities Law

The legislation was passed for the purposes of protecting and regulating the interests of investors in the financial market. In the Act, systematic access by the government is enabled through the SEBI Board, which is empowered with broad access to private-sector data. For example, the board is vested with the same powers as a civil court, including requiring the discovery and production of account books and other documents. The board also has the authority to call for information, undertake inspection, and make inquiries into the stock exchanges and mutual funds of: intermediaries, self-regulatory organizations, banks, or any other corporation established under a Central or State Act in the securities market. As a safeguard to unauthorized access and disclosure, the board is permitted to undertake inspection only if it has reasonable grounds to believe that the company has been indulging in insider trading or fraudulent and unfair trading practices. Expanding the amount of systematic access possible, documents collected as evidence must be retained by the authority for a period of six months. Last, the Act enforces a penalty for failure of companies to furnish information on returns, and a penalty for nondisclosure of acquisition of shares and takeovers.[3]

E. Health Law

The Persons with Disabilities (Equal Opportunities, Protection of Rights and Full Participation) Act, 1996 which mandates the reservation of job posts for persons with disabilities, allows for systematic access. To do this the Act permits any person who is authorized by the Special Employment Exchange as well as persons authorized by general or special order by the government, to access, inspect, question, and copy any relevant record, document or information in the possession of any establishment.[4]

3. The Securities and Exchange Board of India Act, 1992.

4. Chapter 5 Employment, Persons With Disabilities (Equal Opportunities, Protection of Rights and Full Participation) Act (1996).

IV. SYSTEMATIC ACCESS TO LAW ENFORCEMENT/NATIONAL SECURITY

In India, legislation that enables systematic access specifically to law enforcement agencies or on the grounds of national security often (1) does not require law enforcement or government agencies to produce a court or executive order for access; (2) does not define how the agency can use the accessed information; (3) does not restrict access to information to specific ranks of officials, but instead allows for any officer of any agency to access information; and (4) penalizes the private entity noncompliance with disclosure or access requests. Systematic access to information by law enforcement agencies or for reasons of national security can be found under India's Internet law, communications law, and terrorist legislation.

A. Internet Law

The Information Technology Act (ITA) 2008 allows the governmental security agencies for investigation purposes broad systematic access to user information held by the private sector. The provisions are unique in the fact that though they grant broad access to security agencies, they do not establish grounds for access, that is, national security. This augments the amount of access possible as it removes a standard for permitted access. The following sections and rules are relevant:

1. **"Data Protection" section and the "Reasonable Security Practices and Procedures and Sensitive Personal Information" rules:** Systematic access by the government is allowed by (a) not requiring security agencies to gain prior authorization before accessing information; (b) permitting access to any governmental agency; (c) permitting access to any type of "sensitive personal data or information"; and (d) permitting accessed data to be used for broad and generic purposes. For instance, body corporates are required to share information on receipt of merely a written request from any governmental agency. These agencies are not required to state in writing the reason for requesting information; thus the provision does not protect against the nonspecific collection of personal information. When obtained, sensitive personal information may be used by governmental agencies broadly for: verification of identity, prevention, detection, investigation including cyber incidents, prosecution, and punishment of offenses. The rules represent a dilution from traditional procedure established under the CrPc as they do not require a court order from a specified authority to access information, and they do not require the type of information sought to be identified.
2. **Intermediary Liability section and due diligence rules:** These provisions facilitate systematic access in two ways. First, by requiring

intermediaries to provide any authorized governmental agency with information that is requested in writing, and second, by enforcing extensive data retention for a period of 90 days to aid with investigation after take-down notices are received, thus lowering the standard for what types of data can be retained as any affected party can send a take-down notice.

3. **The "Cyber Café" rules:** These rules facilitate access to law enforcement and security agencies by mandating ID disclosure and a one year of data retention at the Cyber Café. Also, the seniority level of the authorized official and circumstances for data access are lowered. Any Inspector authorized by the registering agency is allowed to inspect the premises of any Cyber Café whenever he/she chooses. The Cyber Café owner must, and is held legally responsible for, providing every related document, register, and necessary information to the inspecting officer on demand. The scope of access by the government is augmented by the amount of personal information collected and retained by Cyber Cafés. In addition to systematic access, the rules require monthly disclosure of the log register showing data-wise usage details to an agency identified by the registration agency.

B. Communications Law

Systematic access by governmental security agencies can be found in Indian interception law. The three laws that address the interception of communications are the Indian Post Office Act 1898, the Information Technology Act 2008, and the Telegraph Act 1885. When compared, it is possible to see a weakening of standards among the interception regulations found in these Acts. For example, under the Post Office Act, interception of postal articles is permitted in the occurrence of a public emergency, or in the interest of public safety or tranquility. Under the Telegraph Act, interception of telephone calls is permitted in the interests of the sovereignty and integrity of India, the security of the state, friendly relations with foreign states, or public order, or for preventing incitement to the commission of an offense. Under the IT interception of electronic communications is permitted for the additional reason of preventing incitement to the commission of a cognizable offense relating to the above.

Furthermore, the ITA legal access to information begins with permission to intercept communication data, which must be granted by the Competent Authority. According to the ITA, conditions in which interception, monitoring, and decryption are permitted include: in the interest of the sovereignty or integrity of India, the defense of India, the security of the state, friendly relations with foreign states, or public order, or for preventing incitement to the commission of any cognizable offense, or for investigation of any offense. These conditions are a dilution of the conditions laid out in the Telegraph Act as they allow for information to be intercepted for the additional purpose of investigation.

Furthermore, under the ITA the Competent Authority may issue directions to any agency of the government to monitor and collect traffic data for a range of "cybersecurity" purposes including, inter alia, "identifying or tracking of any person who has breached, is suspected of having breached, or being likely to breach cybersecurity." Also under the ITA, if permission is granted, any agency of the government may intercept, monitor, or decrypt information transmitted, received, or stored in any computer resource. Thus, intermediaries must provide all facilities, cooperation, and assistance for the interception, monitoring, and decryption of information to authorized agencies. This includes assisting in: the installation of equipment of the authorized agency; the maintenance, testing, or use of such equipment; the removal of such equipment; and any action required for accessing stored information under the direction. This requirement is also not found in the Telegraph Act, which requires service providers only to appoint nodal officers in charge of handling the interception orders.

Augmenting the degree of access to information under the ITA are three mechanisms:

1. Decryption Key Holders are required to disclose both the decryption key and provide assistance in decrypting information to authorized authorities. Thus, once the government is in possession of the disclosed decryption key, hypothetically it can access the information at any point of time.
2. If an intermediary fails to comply with directions issued by governmental agencies, they are held criminally liable.
3. Real-time collection of traffic data from any computer resource either in transit or in storage is permitted; thus agencies have the ability to access large amounts of unspecified data.

Though authorized agencies are prohibited from using or disclosing contents of intercepted communications for any purpose besides investigation, they are permitted to share the contents with other security agencies for the purpose of investigation or in judicial proceedings, and, additionally, if a security agency of the central government asks for intercepted information from agencies at the state level.

C. Terrorist Legislation

Systematic access is also found in Indian terrorist legislation. Since its independence, India has seen the enactment of many central and state legislations focused on containing and combating terrorism. Out of these, at least three have imparted greater powers of systematic access to police, security agencies, and the government by lowering interception standards. These include: The Maintenance of Internal Security Act (1971–1978), the Maharashtra Control of Organised Crime Act (1999), The Prevention of Terrorism Act (2002), and the Unlawful Activities Prevention Act (1967) amended in (2004). Through these acts, wiretapping standards at the time have been diluted by: (1) permitting wiretapping

without authorization or warrant, (2) permitting wiretaps to be conducted without a given time limit, (3) permitting all wiretaps (authorized and unauthorized) to be used as evidence in court, and (4) removing traditional wiretapping safeguards found in Indian law.

For the private sector, the rules allowing systematic access are dangerous as they hold specific actors responsible for providing information to the government, while failing to provide a form of redress if an official abuses this power, or if the information is used for unauthorized purposes. Additionally, the rules do not establish if the government is responsible for the security of collected or inspected data. Thus, it is unclear who will be held liable if there is a data breach.

V. BROAD DISCLOSURE

In India there are three categories of legislation and policy that explicitly require the proactive disclosure of information to the government: banking laws (including anti-money laundering), health laws (including legislation pertaining to epidemics), and ISP policy found under communication law.

A. Banking Laws

Private-sector banks are most directly implicated by proactive disclosure requirements in Indian law. The Prevention of Money Laundering Act, 2002 (PMLA) mandates all banking companies, financial institutions, and intermediaries to maintain records pertaining to suspicious client transactions to be disclosed to the RBI.[5] Though these records are not disclosed directly to the government, they are indirectly disclosed because the central government, through the RBI, establishes the procedure and manner of maintaining and furnishing these records. Additionally, if the principal officer of a banking company, financial institution, or intermediary notices suspicious transaction, the officer must furnish the information to the RBI within the prescribed time. Records are to be maintained for a period of 10 years from the date of cessation of the transactions.

B. ISP and Telecom Policy

The government of India has put in place a proactive disclosure regime specifically for communication data through powers established in the ISP license [called the UASL: Unified Access Service License] The license provides the government with expansive access to communication data held by ISPs and Telcos. They are required to maintain and make available to different authorities a wide range of information including:

- A list of all subscribers to its services on a password-protected website for easy access by government authorities. This website should also

5. Prevention of Money Laundering Act of 2002 § 15.

contain a traceable identity and the geographical location of any subscriber at any given time. ISPs must also be prepared to make available a log of all users connected to its service, and a record of the service they are using (mail, telnet, http, etc.). The log must be available to the government "at any prescribed moment."
- User logs along with copies of the packets originating from the Customer Premises Equipment of the ISP must be available to the Telecom Authority.
- A log of commercial records with regard to the communications exchanged on the network for a period of "at least one year" must be made available to the licensor for security reasons.[6]

Though ISP agreements are rooted in the Telegraph Act and thus are subjected to its safeguards, the proactive disclosure regime under the ISP license is so expansive because (1) there is no regulation governing how long information held by intermediaries can be retained, and (2) there is no differentiation in terms of levels of access and disclosure protection between different categories of data; user logs are subjected to the same protection as the geographical location of an individual.

For the private sector the implications of these provisions are severe, as under law service providers are held to a double-edged sword, where on one hand they are held criminally liable if they do not comply with governmental requests for interception, and on the other hand they are held responsible for violations pertaining to secrecy, confidentiality, and unauthorized interception.

C. Health Legislation

Broad disclosure of health-related information has implications for both private and public institutions. The rationale for proactive disclosure in the health sector, unlike banking or telecommunications, has primarily to do with public safety, order, and health as in the case of tracking epidemics. The Epidemic Diseases Act of 1947 requires that the government be informed if any part of the state is "visited by, or threatened with, an outbreak of any dangerous epidemic disease." In order to prevent the outbreak of a disease the government authorizes authorities to inspect persons traveling within the country or across a national border and inform the government of the findings of such inspections.

Proactive disclosure is also being enforced by the government through real-time monitoring of health patients. For example, launched on March 8, 2009, the Save The Baby Girl (STBG) Project was created with the objective of curbing female feticide and enhancing the sex ratio.[7] The STBG system is implemented in

6. Guidelines for Cyber Café Rules § 5(3). The log register must contain the user's name, address, gender, contact number, type and detail of identification document, date, computer terminal identification, log-in time, and log-out time.

7. www.savethebabygirl.com.

two phases: an online portal and the installation of a video-capture device called Silent Observer (SIOB) to the ultrasound machines. The SIOB, also known as the "active tracker," monitors ultrasound tests and records sonography images of each sonography conducted. The sonography video is accessible to doctors and a few government and company officials.

In 2006, the Indian Council of Medical Research (ICMR) published the Ethical Guidelines for Biomedical Research on Human Subjects. The guidelines outline general principles that should be followed when conducting research on human participants. Principles that protect patient privacy include: principle of informed consent, principle of privacy and confidentiality, principle of accountability and transparency, and principle of compliance. Under the guidelines, proactive disclosure is facilitated through government-initiated surveillance studies. Surveillance studies require ongoing, systematic collection, analysis, interpretation, and dissemination of data regarding a health-related event or to measure the burden of a disease.

VI. CATEGORIES OF DATA

Indian law does not make specific distinctions on the role of the court for access to different categories of communication data. For example, the interception of communications can be carried out through a court order, but security agencies are not required to explicitly obtain an order for certain types of data.

The clearest distinction between categories of data and the standards required for access to information by the government is from the 1997 case *PUCL v. Union of India*. The Supreme Court of India held that the interception of communications was an infraction of the constitutionally guaranteed right to life and personal liberty, unless permitted under the procedure established by law. Subsequently, the Supreme Court framed guidelines to be followed when intercepting telephone lines. The Central Government subsequently notified the Supreme Court's procedural safeguards as rules under the Telegraph Act. The rules state that: only a home secretary from the central or state government can authorize a wiretap; requests for interception must specify how the information will be used; each order unless canceled earlier will be valid for 60 days and can be extended to a maximum of 180 days; a review committee at the central/state level will validate the legality of the wiretap; before an interception order can be approved, all other possibilities of acquiring the information must be considered; the committee can revoke orders and destroy the data intercepted; records pertaining to an interception order will be destroyed every six months, unless required for functional purposes; and records pertaining to an interception maintained by the service provider will be destroyed every two months.

In the case of an emergency, immediate interception is permitted to be authorized by the Joint Secretary or any official above, provided that that the Union Home Secretary is informed within three days, and receives confirmation within seven days. However, according to some security experts based in Delhi and in Mumbai: (1) all phone calls in sensitive cities such as Mumbai are recorded for

two or three days, these records are reviewed by the police, and specific numbers are then retained for longer durations; and (2) all international voice traffic is retained for two or three days. However, representatives of Indian telecos speaking under conditions of anonymity assured us that such blanket voice retention measures were neither technically nor economically possible. The truth however lies somewhere in-between.

Telecos engage in data retention of voice and Internet traffic and metadata, but have rolled out legal interception equipment based upon the big data opportunity and the frequency of intercept or information requests. By examining media coverage of crime one can make an informed guess about the scope and nature of data retention. During the investigation of Arushi's murder it was clear that Internet traffic logs detailing search engine queries and details of when the modem was turned on and switched off could be recovered weeks after the incident. In contrast during the investigation of Sister Valsa John's murder it was not possible to recover her call records without finding the device.

VII. STANDARDS FOR USE

Standards for governmental use of accessed information vary across sectors, and in most cases are nonexistent. Apart from these safeguards for telephonic interception, which can be extrapolated to proactive disclosure, no other explicit standards for use or safeguards against abuse are mentioned in sectoral law. One of the six safeguards notified in the Telegraph Act rules as a result of the Supreme Court's verdict in *PUCL v. Union of India* impacts use of intercepted information: "all copies of the intercepted material must be destroyed as soon as their retention is not necessary under the terms of the Act."[8] The ITA Interception Rules prescribe maintenance of records by the designated officer to include "the name and other particulars of the officer or the authority to whom the intercepted or monitored or decrypted information has been disclosed, the number of copies, including corresponding electronic records of the intercepted or monitored or decrypted information made and the mode or method by which such copies, including corresponding electronic record are made, the date of destruction of the copies." However, in contrast, the "Guidelines for anti-money laundering measures" issued by Sebi do not mention any similar privacy safeguards under the sections dealing with "record keeping" and "retention of records."

VIII. CROSS-BORDER AND MULTI-JURISDICTIONAL ISSUES

The ITA 2008 in its preliminary chapter clarifies that it does not only apply to India's jurisdiction; it says it "applies also to any offense or contravention

8. "FAQs on Telephone Tapping," *PRS Blog* (Apr. 27, 2010), http://www.prsindia.org/theprsblog/?tag=telephone-tapping.

thereunder committed outside India by any person."[9] This is in contrast with the Telegraph Act, which only "extends to the whole of India."

IX. RECENT CONTROVERSIES AND/OR PENDING UNRESOLVED ISSUES

A. Blackberry

The four years of negotiations between the Indian government and Research in Motion (RIM) demonstrate how the Indian government includes an element of proactive disclosure outside of the legislative sphere. Since March 2008, India has threatened to place a ban on RIM's Blackberry services, unless given real-time and direct access to communication traffic. The Indian government during negotiations has proposed six solutions to allow for direct access to the BlackBerry network. The solutions involve: (1) physically locating the servers (Network Operating Centres) within India, thus giving the government clear jurisdiction; (2) enforcing a blanket data retention of all Internet data and email for a minimum period of six months; (3) lowering RIM's encryption to 40 bit from the current 256 bit to allow easy interception of communications; (4) encryption key escrow for both BIS and BES with the Indian government; (5) negotiate a "Government to Government" solution where legal interception orders will be routed through the US or Canadian governments, who will then comply and carry out interception on behalf of the Indian government; or (6) complying with the requirements of the Central Monitoring System (CMS), an interception network that allows security agencies to intercept emails, cyber chats, monitor voice calls, SMS, MMS, GPRS, fax communications on landlines, and CDMA and GSM networks—all in real time.[10]

If enforced, the CMS will create a system where the government will not need to require disclosure of information from the private sector, but instead will be able to access this information on its own. Solutions 4 and 6 proposed by the Indian government explicitly fall into the category of proactive disclosure, allowing the government to bypass the private actor and legal safeguards. This will also subvert the legal protections and safeguards found in confidentiality clauses, and take away an accountability and transparency mechanism that is typically in place when private entities protect information under contract. The policy and practice emerging from the standoff between RIM and the Indian government is commonly understood within and outside government to set the standard for data access and interception for other private-sector companies offering similar cloud-based encrypted communication services such as Google

9. ITA Interception Rules § 16 (2009).

10. John Ribeiro, "India to Set Up Automatic Monitoring of Communications," *PC World* (November 26, 2009), http://www.pcworld.com/article/183229/india_to_set_up_automatic_monitoring_of_communications.html.

Mail and Skype. RIM made several counteroffers to the Indian government often without directly responding to their demands. However, most recently RIM has opened a NOC in Mumbai that would subject it to the terms and conditions of the Unified Access Service License. This arrangement would allow for interception of PIN messages, and BIS traffic but not BES traffic, and would also resolve the government's anxiety over domestic traffic being routed to foreign NOCs. It is unclear from media reports whether key escrow for BIS users has been implemented. The Indian government however continues to demand interception of corporate or BES traffic. This could only be resolved via proactive disclosure or key escrow as mandated in the UASL (though never implemented).

B. NATGRID

In 2011, the National Intelligence Grid (NATGRID) was established as an attached office of the Ministry of Home Affairs; it facilitates governmental systematic access by providing security agencies with a license to go through and link 21 databases from government and private-sector organizations such as an tax records; air, train, and bus travel; Internet; and phone telecom records.[11] NATGRID complicates the picture of governmental access to information, because it does not operate via legislation, and claims only to connect databases. Thus, regulations and procedures do not exist. For the private sector this means that NATGRID could override any safeguards in place.

C. Corruption

Though the ITA rules do not comprehensively protect against systematic access, they do establish certain safeguards to prevent systematic access by the government. However, in practice the government often ignores these safeguards. Recently, in Mumbai, two city assistant police commissioners were accused of selling call details from conversations of high-profile individuals.[12] The police commissioners allegedly used their position to gain access to the communication records from telecos. Only one of the telcos responded when the investigating police officers approached seeking the names of the officers to whom details had been disclosed. This incident reveals that law enforcement officials abuse their positions to dilute data access safeguards. This demonstrates the loose implementation of the interception safeguard. In addition, it is clear that service providers are not transparent about data access either, because it is illegal or because

11. Vibhuti Agarwal, "Q&A: NATGRID Chief Raghu Raman," *Wall Street Journal* (June 29, 2011), http://blogs.wsj.com/indiarealtime/2011/06/29/qa-natgrid-chief-raghu-raman/.

12. "Two Delhi Cops May Land in the Dock for Selling Cell Call Records," *Times of India* (March 11, 2012), http://articles.timesofindia.indiatimes.com/2012-03-11/mumbai/31144815_1_delhi-officers-delhi-cops-service-providers.

they are afraid of consequences demonstrating the lack of redress and protection for service providers that is given if there is abuse by government entities.

D. CCTV

There are no specific laws governing the use of CCTV (closed circuit television) cameras in shops, offices, colleges, hostels, and other private-sector establishments. However, in New Delhi, other metro cities, and state capitals, the police have been strongly advocating the installation of CCTV cameras in private-sector establishments. Hotels are asked to install CCTV cameras at reception desks, front entrances, car parks, and all lobbies of the hotel until the guests enter their private rooms. The police have also been encouraging private establishments to make CCTV camera feeds available in real time by using web-streaming technologies. Most recently, the Delhi police called for mandatory real-time feeds of bars and pubs in Noida following the gang rape of an ex-employee. CCTV camera footage has been successfully used by the police to secure convictions for a wide variety of crimes. For example, CCTV cameras have been installed in response to terror attacks, such as the German bakery blast that took place in Pune. After the attacks that took place in 2010, the city amended the development control rules and made it mandatory for 24/7 cameras to be installed in public areas.[13] CCTVs are an example of an area where systematic access of private-sector data is growing rapidly in the absence of any regulatory framework.

X. CONCLUDING OBSERVATIONS

The practices around systematic access of private-sector data in India are difficult to understand clearly as very few members of the private sector are willing to speak about it even under conditions of anonymity. When it comes to policy, in many cases there is no explicit policy; where policy does exist it is unclear and lacking sufficient safeguards, allowing for a wide range of interpretations. When data retention is prescribed there are usually very few safeguards—no breach notification, no transparency requirements, usually not even internal record-keeping is required, no mandatory deletion/obfuscation policy, no requirement to publish a data-retention policy.

Given unclear policy and the cost of data retention, private-sector practices vary across the different organizations, across geographic regions, across market segments, and also across sectors. No indigenous private-sector organization publishes a data retention policy or is transparent about government access. No indigenous private-sector organization appears to publicly resist data access or surveillance demands of the government. In its annual report, Bharati Airtel says "In the lawful interception domain, we received 422 appreciation letters

13. Radheshyam Jadhav, "CCTV Cameras in Public Places Will Need Govt's Go-Ahead," *Times of India* (February 9, 2011), http://articles.timesofindia.indiatimes.com/2011-02-09/pune/28545041_1_cctv-cameras-fire-stations-pmc.

from various law enforcement agencies in the last one year alone."[14] The report is not clear about the total number of interceptions facilitated.

Surveillance and systematic access is usually permitted under law during a "public emergency" on when "public safety or tranquility," "sovereignty and integrity of India," "security of the state," "friendly relations with foreign states," or "public order" is undermined or to "prevent incitement to the commission of any offense." Over time the standards for surveillance and systematic access have been diluted from a "public emergency" to "prevent incitement to the commission of any offense." This is a pretty significant dilution given that the ITA has placed what some consider unconstitutional limits of freedom of expression by criminalizing acts such as "sending, by means of a computer resource or a communication device, any content that is grossly offensive or has menacing character; or any content which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will." Given this lowering of the threshold on free speech, the government could order surveillance or systematic access to private-sector data using different provisions of the law involving trivial reasons.

The government of India does not seem to exercise a scientific temper or adopt principles of natural justice when it comes to surveillance and systematic access to private-sector data. It appears to be sold on a techno-utopian vision of "surveillance for surveillance's sake" or very little appreciation of "privacy by design principles" or "privacy as a prerequisite for security" or "excessive surveillance compromising security." Massive surveillance projects are being rolled out without waiting for enabling legislation. This attitude of government is best understood via the design and implementation of projects such as the Baby Girl project, NATGRID, and CMS.

Given the policy vacuum, the lack of clarity in policy, and the distance between policy and implementation, the impact on the private sector has four dimensions: (1) unclear liability when personal data fall into the wrong hands, (2) lack of redress system available to the private sector in case of abuse by a government official, (3) a tendency for collusion between government actors and private-sector actors that can result in tampering of cyber-evidence, and (4) the likelihood that without transparency and access to recourse this will result in a private surveillance and censorship regime.

14. Bharati Airtel Annual Report, 2010–2011.

13

Systematic Government Access to Private-Sector Data in Japan

MOTOHIRO TSUCHIYA

I. ABSTRACT

The Japanese legal system has been based on the German legal system since the mid-nineteenth century, but the American legal system was grafted on to it following Japan's defeat in World War II in 1945. The postwar Constitution contained an article regarding the secrecy of communication and protected privacy in terms of respect of individuals. As of 2015, the Japanese government had 64,632 record files containing personal/privacy information of Japanese and foreign persons. Now, as the Personal Information Protection Law in the Executive Branch, which was enacted in 1988, and the Personal Information Protection Law, which was enacted in 2003, strictly regulate privacy, there have been fewer problematic cases regarding governmental access to private-sector data. Data gathering for law enforcement or intelligence activities has also been weaker following World War II. Private-sector corporations/organizations might share data with government agencies, but this is based on voluntary arrangements, not by any mandatory system. More focus is being cast not on governmental access to private-sector data, but on citizen's access to data, which government agencies are holding, as well as the establishment of a national ID system.

II. NATIONAL LEGAL CONTEXT AND FUNDAMENTAL PRINCIPLES

After the Meiji Restoration in 1867, Japan started adopting Western-style legal systems, especially from Germany, or Prussia. Japan needed to place the reins of government back in the hands of the Emperor from the rule of the Shoguns of the Tokugawas from the seventeenth century to mid-nineteenth century. However, the Emperor was not to become an absolute ruler but the head of a constitutional monarchy comprising independent legislative, executive, and judicial branches.

Leaders of the Meiji Restoration needed the Emperor as a symbol of a new political system, but tried to retain actual power in their own hands. Prussia was an example of such a system. Other social systems were mixtures of other Western traditions. For example, the road system was adopted from the United Kingdom. Japan still drives on the left.

The attempt of the Empire of Japan to become a regional hegemon was defeated by Japan's losing of World War II, which ended in 1945. The General Headquarters (GHQ) of the Allied Forces occupied the main four islands of Japan until 1952, while Okinawa was kept under the military administration of the United States until 1972. GHQ broke down many of the extant political, economic, and social systems in order to transform Japan into a more peaceful and democratic state. However, GHQ did not abolish the imperial system. This means that Japan's current legal system retains elements of the prewar systems.

At first, GHQ tried to allow the Japanese to redesign a new constitution themselves, but their first draft was considered too conservative. Then, General Douglas MacArthur ordered his GHQ staff to draft a constitution, and it was handed to the Japanese drafters. As there were many New Dealers in GHQ, the new Constitution is imbued with idealism. For example, Article 9 abolished the use of armed forces to solve international disputes. But it became one of the core problems regarding Japanese postwar diplomacy and national security policy. Later administrations in the United States requested Japanese rearmament, and the Japan Self-Defence Forces was established under the Japan-US Security Treaty.

Although the Constitution introduced American idealism, many of the statutory laws inherited from the prewar systems were still influenced by the German legal system. That is, the American legal system was grafted on the previous system after Japan lost World War II. For 70 years after its promulgation, many people have tried or proposed modification of the Constitution, but such attempts have been unsuccessful as the procedure to do so is so difficult. In July 2016 House of Councilors election the Liberal Democratic Party, New Komeito, and other parties, which were in favor of revising the Constitution, won two-thirds of the House. It is one step further for the revision, but Prime Minister Shinzo Abe posed a cautious position, though the revision is his long-time ambition.

The Japanese Constitution does not have any specific stipulations regarding protecting privacy, but Article 13, that people be respected as individuals, is said to protect rights of privacy. And Article 21, "nor shall the secrecy of communication be violated," clearly guarantees the secrecy of communication in writing. However, despite these articles in the Constitution, statutory laws were not enacted even after Japan regained its independence in 1952. The Personal Information Protection Law in the Executive Branch was enacted in 1988 and the Personal Information Protection Law covering the private sector was enacted in 2003. The 2003 Law was a direct response to the EU Data Protection Directive. Before the 2003 Law, there were privacy protection guidelines in each economic/social sector. There was no omnibus act covering public and private sectors on the same basis. Most of those guidelines were made by each sector or industry to cope with its own problems without statutory laws. The 2003 Law overrode

these guidelines and started regulating information gathering, storage, and dissemination in an excessive way. This has served to stifle government, business, and social activities. For example, in schools, parents cannot share their contact information, as school managers don't want to take the risks of storing such "sensitive" information. The law doesn't punish a thief who steals privacy information, but punishes an administrator who lets it be stolen. People, businesses, and even government agencies started avoiding holding privacy information.

Even before the 2003 Law, the Japanese government had hesitated to systematically access private-sector data. Based on bitter prewar and wartime experiences regarding the invasion of privacy and other human rights violations, Japan's mass media strongly opposes the presence of any government hand in private-sector information. Therefore, formal access to such information is not favored in Japan. The government relies on weaker, informal access to private-sector data. The private sector has set up its own guidelines and the government requested reports from it based on business laws regulating each sector.

Governmental data collection is also limited in law enforcement and intelligence activities. There is no corresponding law to the IPA (Investigatory Powers Act) in the United Kingdom and the USA FREEDOM Act in the United States. Interception of communications, or wiretapping, is not a popular tool among Japanese law enforcement/intelligence agencies. This is a deep-seated taboo after World War II, based on the widely shared repentance that spy agencies and military police powers abused wiretapping during the war. Nonetheless, the Interception Law for law enforcement purposes was enacted in 1999 while loud oppositions were heard against the enactment, but executive wiretapping is not clearly authorized. There is no strong power to seek wider wiretapping in the Japanese society.

In these contexts, there seems to be very few cases of systematic access to private-sector data by the Japanese government, as far as the author finds.

III. STATUTORY AND REGULATORY OVERVIEW

A. Freedom to Collect and Store Information

In principle, there is freedom to collect information for the government or the private sector in Japan.[1] However, in cases of invading others' rights or of clearly violating the social order, such activities might be prohibited. Among others, in cases involving specific and sensitive information, invasion of privacy is recognized.[2] However, there is no clear definition in the laws of what is "sensitive"

1. Taro Komukai, *Introduction to Information Law (Joho Ho Nyumon)* (Tokyo: NTT Publishing, 2008), p. 82 (in Japanese).

2. Hisamichi Okamura and Fumio Shimpo, *Electronic Networks and Personal Information Protection (Denshi Network to Kojin Joho Hogo)* (Tokyo: Keizai Sangyo Chosakai, 2002), p. 79 (in Japanese).

information. Section 4.4.2.3 of the Japanese Industrial Standards (JIS) Q 15001 defines it as follows:

1. Issues of thought, creed and religion
2. Race, nation, birthplace, domicile of origin, physical handicap, mental disability, criminal record, and other factors of social discrimination
3. Participatory status in a labor union
4. Participatory status in political activity
5. Medical and sexual life

Article 133 of the Criminal Law prohibits the opening of private mail. Articles 4 and 179 of the Telecommunications Business Law protect secrecy of communications. Article 3 of the Secrecy Protection Law regarding Japan-US Mutual Defense Aid Arrangements protects defense secrets connected to American military forces, but general defense secrets are not covered in full. A security clearance system has not been introduced to cover both the public and private sectors. One covers parts of the Ministry of Defence and the Self-Defence Forces.

Private-sector trade secrets are partially protected by Articles 3 and 4 of the Unfair Competition Prevention Law. It was revised in November 2005 to add penalties. Trade secrets must be kept secret and not be revealed to the public (Article 2).

Under the current laws, it is not necessarily illegal to steal information in Japan. If you take out confidential information from a stored place, you will be punished for stealing paper sheets or digital disks, not for stealing the information itself. However, the Unauthorised Access Prevention Law dissuades information theft in a sense. It was enacted in 1999 to respond to the rapid increase of computer-related crimes.

There is freedom to store information as well as collect information for the government and the private sector under the current laws in Japan.[3] Usually it is not requested for any party to disclose what kinds of information are kept. However, if personal/private information is kept in one way or another, the Personal Information Protection Law can be applied to maintain such information securely.

It is possible for government to collect, store, or access information using its public powers. But such information can be regarded as public property. More people are claiming that government information activities be checked under citizens' eyes.

B. Personal Information Protection Law

The most powerful law influencing governmental and private information activities is the Personal Information Protection Law enacted in 2003. The law strictly regulates the purpose of information collection and mandates strong protection of stored data. As a result of this law, collection and storage of personal/privacy data have stagnated in Japan. Incidental leaks of such data impose a high price for administrators in terms of compensation and reputation. It is also true for

3. Komukai, above note 1, pp. 83–84.

government. Government agencies avoid unnecessary gathering of private data because of fear of being blamed following any leak of citizens' privacy.

The law demands the definition of the purpose of data collection in each case to be as clear as possible (Article 20), and nobody can deal with data beyond defined purposes (Article 21). It is also forbidden to share data with a third party without consent (Article 28).[4]

As of 2015, the Japanese government has 64,632 record computer and manual (paper) files containing personal information of Japanese and foreign persons (Appendix 1).[5] This number doesn't include data on businesses corporations and other private organizations. Such files contain identifiers of more than 1,000 persons. If they contain fewer, they are not counted in this number. This number was reduced from 85,822 in 2011.

Table 13.1 shows examples of record systems containing personal information held by the Japanese government. The biggest owner of personal information among Japanese government agencies is the National Tax Agency, which gathers financial information on residents in Japan. Chapter 4 of the Establishment Law of the Ministry of Finance describes the mandates of the National Tax Agency. But it does not tell us how the agency is collecting data.

Table 13.1. Examples of Record Systems Containing Personal Information Held by the Japanese Government

Ministry/Agency	**Examples of Record Systems**
National Tax Agency	Personal tax ledger; List of mandatory tax collector at the source; List of class attendants for alcohol selling; and others
Ministry of Justice	List of prisoners; Data on persons who enter and exit Japanese border (Japanese and foreigners); and others
National Police Agency	Drivers' license information and others
Ministry of Foreign Affairs	List of foreign residents; Passport control file; List of foreign media; and others
Ministry of Health, Labour and Welfare	List of health care recipients; List of pension recipients; Public nursing care insurance recipients; List of money transfer to foreign countries; and others
Ministry of Defence	List of land owners for US bases
Ministry of Land, Infrastructure, Transport and Tourism	List of first-class architect; List of airline service employees; and others

source: http://www.soumu.go.jp/main_sosiki/gyoukan/kanri/pdf/shikojyokyo_h22/shikojyokyo_h22_12.pdf.

4. Okamura and Shimpo, above note 2, p. 194.

5. http://www.soumu.go.jp/main_content/000413445.pdf.

The government ministries, departments, and agencies are collecting these data based on (1) establishment laws of each government sector, and (2) business laws regulating each economic sector. The details of data collection methods are usually defined in ministry orders.

C. Law Enforcement and Intelligence Agencies

In Japanese society, government intelligence agencies are weaker as compared with other societies. The leader of the Japanese intelligence community is the Cabinet Intelligence Research Office (CIRO), and the community includes departments and agencies of the National Police Agency, the Ministry of Foreign Affairs, the Public Security Intelligence Agency, and the Ministry of Defence. But none of them holds big powers to access private-sector data. No cases of such agencies systematically accessing private-sector data have been found in the research process of this chapter. There is no question about these agencies collecting data on targets, but such activities are case-by-case and not systematic and regular. The National Police Agency and prefectural police departments all over Japan collect data especially on crime organizations such as cults and "yakuzas (mafias)" for law enforcement purposes. In order to stop money laundering, financial institutions are requested to report "doubtful" transactions to law enforcement agencies based on the Narcotics and Psychotropic Control Law and others, but this report is not mandatory. The government cannot access financial information without proper warrants.

Most cases involve accessing financial records for tax collection based on Article 141 of National Tax Collection Act (See Table 13.2). In other cases the Ministry of Justice is gathering data on persons who enter and exit Japanese borders based on the Emigration and Immigration Management and Refugee Recognition Law. As Japan is an island country, it is necessary to use vessels on the sea or airplanes to cross the border.

Table 13.2. Access to Personal Record Files Beyond Original Purposes in Fiscal Year 2014

	Administrative Agencies	**Independent Administrative Legal Entities and Others**
Cases based on Laws	2,698	293
Cases for Public Interests or Cases with First Person's Consent [a]	279	232

[a] For example, the Imperial Household Agency discloses records of people who receive medals.

SOURCE: http://www.soumu.go.jp/main_content/000413445.pdf.

So far, there are fewer cases of the use of communications interception, or wiretapping, for law enforcement or other purposes.[6] The Interception Law for law enforcement purposes was enacted in 1999, and it mandates annual disclosure of the number of interceptions done by police agencies all over Japan (Table 13.3). However, executive wiretapping to prevent future terrorism attacks or crimes is not authorized under the Japanese laws.

The Interception Law does not exclude computer communications. However, as Table 13.2 shows, all of the authorized interceptions in 2011 were mobile calls, because usually criminals prefer prepaid or illegally obtained mobile phones. Interception of Internet traffic is said to be legal under the current laws, but has not been used yet. The National Police Agency is still cautious about using the method. But it will be considered in the future. Of course, stored digital records in computers and other devices are searched with warrants.

The tradition of strict protection of communications secrecy dissuades telecommunications/Internet service providers from stopping apparently harmful traffic. They are allowed to access neither content nor corresponding communications data such as traffic data, service use data, and subscriber data. They only use such data to manage the quality and security of their networks with special reasons.[7]

Table 13.3. Number of Authorized Communications Interception in Japan in 2013

Case Number	Requests	Authorized	Communication Method	Number of Arrested Persons
1	8	8	Mobile	9
2	6	6	Mobile	4
3	12	12	Mobile	8
4	2	2	Mobile	12
5	4	4	Mobile	0
6	3	3	Mobile	3
7	3	3	Mobile	0
8	5	5	Mobile	3
9	6	6	Mobile	14
10	3	3	Mobile	12
11	7	7	Mobile	14
12	5	5	Mobile	0

source: http://www.moj.go.jp/content/000118702.pdf.

6. Fumio Shimpo, *Birth and Development of Rights of Privacy (Privacy no Kenri no Seisei to Tenkai)* (Tokyo: Seibundo, 2000), pp. 250–278 (in Japanese).

7. Ikuo Takahashi, Koichiro Hayashi, Makoto Funahashi, and Kazuo Yoshida, "Strange Destiny of Secrecy of Communications (Statutory Law)," *Joho Network Law Review*, vol. 8 (2009), pp. 1–26 (in Japanese).

Table 13.4. Examples of Business Sectors and Business Laws in Japan

Business Sector	Business Law	Supervisory Authority
Telecommunications	Telecommunications Business Act	Ministry of Internal Affairs and Communications
Banking	Banking Act	Financial Services Agency
Electric Power	Electricity Business Act	Ministry of Economy, Trade and Industry
Railways	Railway Business Act	Ministry of Land, Infrastructure, Transport and Tourism

D. Business Laws

In Japan there are various business laws corresponding to each economic (sometimes social) sector, and supervisory authorities in the government can request or mandate reports mainly on financial data from participants in each sector. Most of such reports are on an on-demand basis, but usually businesses and persons submit reports without reluctance. This is an important and useful way for the Japanese government to understand the situation of each industry (Table 13.4).

IV. RECENT CONTROVERSIES AND/OR PENDING UNRESOLVED ISSUES CONCERNING SYSTEMATIC GOVERNMENT ACCESS TO PRIVATE-SECTOR DATA

As cloud services on the Internet are becoming popular, the problem of data jurisdiction is being discussed here and there. If we put data in the United States, the US government could access the data under the USA FREEDOM Act and other laws. If we put data in the EU area, the EU Data Protection Directive would influence the data. Or, we might not be able to retrieve the data once we sent it to the EU if the EU or a Member State prohibits data transfer for any reason.[8] Furthermore, it is said that data stored in servers in China might be accessed without legal reason. Therefore, it is not the governmental access to private-sector data that matters in Japan, but the way the government uses such services.

On the other hand, there is no statue in Japan to regulate data transfer overseas. However, there are semiformal guidelines clarifying the details of handling data, which prohibits international data transfer. Article 25 of the Foreign Exchange and Foreign Trade Law does not authorize international data transfer in some cases.[9]

However, this debate was drastically changed after the Great East Japan Earthquake and tsunami of March 11, 2011. The City of Takada in Iwate Prefecture

8. Hiroshi Kondo and Kei Matsumoto, *Cloud and Law (Cloud to Hou)* (Tokyo: Kinyu Zaisei Jijo Kenkyukai, 2011), pp. 117–22 (in Japanese).

9. Kazuaki Yoshii, "Legal Risks in Cloud Service," *Joho Network Law Review*, vol. 10 (2011), pp. 159–74, footnote 47 (in Japanese).

and three other cities and towns lost critical servers containing the basic data of their residents. The local governments could not issue certificates and other official documents. Following this, it is now being discussed whether or not critical data and information should be kept on-site. Data should be stored in remote sites in multiple locations. Cloud services can be insurance against such risks.

Japan maintains a domiciliary register system. Every citizen must be registered with the local government following birth. Family trees are also kept in government servers. The system used to be paper-based, but it was digitized and networked in 2000. Servers of local governments in Japan were interconnected to exchange traffic. This change raised a lot of privacy concerns, and several local governments refused to connect to the system.

However, in a networked society, it is critical to have digital data and a unique personal ID. Japanese residents have several unique IDs, for the domiciliary register system, for the tax ID system, for the pension system, the health insurance system, the driver's license system, and others. More and more people want one-stop service with one ID. A national ID system is now on the political agenda.

In October 2015 "My Number" system started and all residents (citizens and foreigners living in Japan) started to be given their own 12-digit numbers (artificial persons get 13-digit numbers). This new system is for (1) realization of fair society, (2) effective government, and (3) advancement of people's convenience. These numbers are used for social security services, tax collection, and disaster countermeasures. They are similar to Social Security Numbers in the United States, but they should not be shared for other services in private sectors. There are growing concerns about data breach, but the government claims this system will make related systems more transparent and efficient.

Related to the "My Number" system, the Personal Information Protection Commission (PPC) was established on January 1, 2016, by reorganizing the Specific Personal Information Protection Commission. The PPC is an independent body from government structures, and supervises private and government entities, which deal with personal information.[10]

V. CONCLUDING OBSERVATIONS

In general, there have been no serious problems reported regarding systematic access to private-sector data by the Japanese government so far. This does not mean that there is actually no problem. Real problems might be just hidden from the public eye.

At any rate, the present political atmosphere does not allow such systematic access. And the impact of the Personal Information Protection Law in 2003 has suppressant effects over data gathering by government and business actors.

On-demand reports from the private sector to the government are a more common practice in Japan. This is not systematic and regular access, but works well between the business sector and the Japanese government.

10. http://www.ppc.go.jp/en/.

APPENDIX 1: NUMBER OF RECORD SYSTEMS CONTAINING PERSONAL INFORMATION HELD BY THE JAPANESE GOVERNMENT

Ministry/ Agency	Number of Record Systems Containing Personal Information														
		Breakdown		Breakdown according to Number of Records											
				Less than 10,000			More than 10,000 and less than 100,000			More than 100,000 and less than 1 million			More than 1 million		
		Computer	Manual		Computer	Manual		Computer	Manual		Computer	Manual		Computer	Manual
National Tax Agency	57,807	51,893	5,914	29,962	25,219	4,743	20,815	19,775	1,040	6,955	6,824	131	75	75	0
Ministry of Justice	4,569	1,678	2,891	3,857	1,105	2,752	264	126	138	368	367	1	80	80	0
Ministry of Agriculture, Forestry and Fisheries	527	524	3	416	415	1	97	95	2	12	12	0	2	2	0
Ministry of Health, Labour and Welfare	404	219	185	277	114	163	56	42	14	25	20	5	46	43	3
Ministry of Internal Affairs and Communications	268	268	0	175	175	0	49	49	0	43	43	0	1	1	0

Ministry of Finance	265	265	0	149	149	0	71	71	0	30	30	0	15	15	0
Ministry of Defence	184	111	73	79	51	28	90	48	42	15	12	3	0	0	0
Financial Services Agency	21	12	8	10	3	7	10	8	2	1	1	0	0	0	0
Imperial Household Agency	119	2	117	96	2	94	23	0	23	0	0	0	0	0	0
Ministry of Land, Infra-structure, Transport and Tourism	101	88	13	34	32	2	35	27	8	22	19	3	10	10	0
Others	367	247	121	210	130	80	116	82	34	29	24	5	12	11	1
Total	64,632	55,307	9,325	35,265	27,395	7,870	21,626	20,323	1,303	7,500	7,352	148	241	237	4

SOURCE: http://www.soumu.go.jp/main_content/000413319.pdf.

14

Systematic Government Access to Private-Sector Data in the Republic of Korea

SANG JO JONG*

I. ABSTRACT

This chapter examines the statutory grounds for governmental access to private-sector data in Korea. It focuses on issues such as the circumstances under which access is allowed without a warrant and how unjustified government access can take place in practice.

II. INTRODUCTION AND OVERVIEW

In 2011, the Cultural Minister Yu In-chon was attending a welcoming ceremony held at Incheon International Airport to greet the 2010 Vancouver Winter Olympic champion skater Kim Yu-Na. During the ceremony, the minister stretched out his arms toward Kim's shoulders as a gesture of welcome, but the scene was captured and slightly edited to look as if the minister tried to hug Kim as she reluctantly avoided him. This video clip was posted on a website for funny pictures/video clips, and the humiliated minister sued for libel the Internet users who uploaded it.[1] Upon the filing of the complaint, the police requested the Internet users' names, resident registration numbers, cell phone numbers, and date of subscription, which the ISP provided two days later. Then, one of the accused whose personal information was given to the police sued the ISP for disclosing his personal information in breach of the ISP's terms of use. The case

* The author expresses his gratitude to Ms. Hanhee Yang for her help in translating this chapter.

1. Kwon Mee-yoo, "Culture Minister Yu Upset at Yu-na Video," *The Korea Times* (Seoul, March 17, 2010), http://www.koreatimes.co.kr/www/news/nation/2010/03/117_62548.html.

generated a heated controversy over whether such governmental access without proper warrants was an infringement on privacy or the right of personal information. Six years later, the Supreme Court of Korea came to a conclusion[2] that illustrates some of the realities and statutory limits of governmental access to private-sector data in the Republic of Korea.

Systematic government access to private-sector data can take place in a variety of ways. Under some circumstances, access requires warrants issued by a court, whereas in other situations it does not. Notably, due to the unique truce situation, under which the Republic of Korea is technically still at war with North Korea, Korean authorities are sometimes allowed to obtain private-sector data without warrants, for national security purposes.[3]

This chapter will examine the statutory grounds for governmental access to private-sector data in Korea, focusing specifically on issues such as the circumstances under which access is allowed without a warrant and how unjustified government access can take place in practice.

III. NATIONAL LEGAL CONTEXT AND FUNDAMENTAL PRINCIPLES

Article 17 of the Constitution of the Republic of Korea states, "The privacy of no citizen shall be infringed," and Article 18 states, "The privacy of correspondence of no citizen shall be infringed." The Constitution does not explicitly mention a fundamental right of personal information or data protection. However, based on Article 37, which reads, "freedoms and rights of citizens shall not be neglected on the ground that they are not enumerated in the Constitution," and in light of Article 10 (which recognizes the human worth and dignity of all citizens) and Article 21 (which protects freedom of expression), plus Articles 17 and 18, it is reasonable to conclude that personal information privacy is a fundamental right. Indeed, Korean courts have held that the rights to privacy and the pursuit of happiness in these Articles provide the ideological basis for acknowledging a so-called "right to self-determination of personal information" as a separate constitutional right.[4] This "right to self-determination of personal information" is in turn embodied and delineated in various statutes, including the "Personal Information Protection Act."

Previously, the obligations of government bodies with regard to personal information protection were regulated by the "Act on Personal Information Protection of Public Agencies" (APIPPA). On September 30, 2011, the APIPPA was replaced by and incorporated into the "Personal Information Protection

2. Supreme Court of Korea Decision 2012 da 105482 (S Korea, March 10, 2016).

3. Government Organization Act, art 29; Personal Information Protection Act [hereinafter PIPA], art 18; Communication Privacy Act [hereinafter CPA], art 8.

4. Supreme Court of Korea Decision 96 da 42789 (S Korea, July 24. 1998); Constitutional Court of Korea Decision 99 hun-ma 513, 2004 hun-ma 190 (S Korea, May 26, 2005).

Act," which covers both the public and private sectors. Further regulations applicable to the private sector are also found in a variety of industry-specific statutes, including the Act on Promotion of Information and Communications Network Utilisation and Information Protection (Communications Network Act), the Act on Use and Protection of Credit Information (Credit Information Act), the Communication Privacy Act (Communication Privacy Act), the Act on Real Name Financial Transactions and Guarantee of Secrecy (Real Name Financial Transactions Act), the Act on Report and Use of Specific Financial Transaction Information (Financial Transaction Information Act), and the Act on Use and Protection of Location Information (Location Information Act).

Enacted in 2011, the Personal Information Protection Act (PIPA) is a comprehensive statute that imposes obligations on entities dealing with personal information ("processors"), both in the public sector and the private sector. PIPA establishes basic principles regarding the collection, use, and disclosure of personal information. It is notable that PIPA explicitly requires, as a general rule, that processors obtain consent from the data subject; in the case of a disclosure, the data subject must be informed as to the recipient of the personal information, what personal information will be transferred, the purpose for which the information will be used, and the period for which it will be retained. These requirements also apply when providing personal information to a third party overseas.[5] Moreover, PIPA requires the government to "work out policy measures necessary to enhance the personal information protection standard in the international environment."[6]

As for the obligations of the state, PIPA provides that the government "shall devise policy measures to prevent any harmful effect from collecting personal information for any purpose other than the intended purpose, misusing, abusing, or excessively monitoring and tracking, etc. personal information, thereby protecting human dignity and personal privacy."[7] Article 15 permits collection and use not only with consent but also "where special provisions exist in laws" and "where it is unavoidable so that the public institution may carry out such work under its jurisdiction as stated by laws and regulations."[8] Apart from these basic principles, PIPA does not say much about the scope and procedures regarding government access to third-party private-sector data. Instead, the standards for government access to personal information must be found elsewhere. Personal information is acquired by public authorities using the existing warrant system or under numerous administrative procedures. In addition, data that does not fit within the PIPA definition of personal information can always be submitted to the government voluntarily and informally.

5. PIPA, above note 3, art 17(3).

6. PIPA, above note 3, art 14.

7. PIPA, above note 3, art 5.

8. PIPA, above note 4, arts 15(1)2 and 15(1)3.

IV. STATUTORY OVERVIEW AND ANALYSIS

A. Laws regarding Governmental Access to Private-Sector Data

This section will examine PIPA and other statutes in greater detail.

As a preliminary point, it should be emphasized that private-sector data can be divided into two categories: personal information data and everything else. Statutes on privacy including PIPA define personal information as "the information pertaining to any living person that makes it possible to identify such individual by his/her name, resident registration number, image, etc. (including the information which, if not by itself, makes it possible to identify any specific individual if combined with other information)." However, Internet log records (the date, frequency, and length of connections) and telephone calling records (the originating and called numbers, with time and duration) do not normally fall within the scope of the definition of personal information unless they are put together with name or personal identification number. Internet logs and dialed number records, sometimes referred to as "transactional data," are considered to be personal information if and only if the service provider collecting the logs or records has another database containing users' names and/or personal ID numbers and if the company is technically capable of easily putting those databases together.

PIPA Article 15 states as a basic principle that personal information must be collected only with consent of the subject of such information.[9] However, the government can obtain personal information without consent where it is necessary for a public institution to carry out its official duties under its jurisdiction as stated by other laws and regulations that supersede PIPA, or where it is deemed necessary explicitly to protect the data subject or any third party from impending danger to his/her life, body, or property. The phrase "official duties under its jurisdiction as stated by laws and regulation" refers to the obligations and authorities of public bodies prescribed in the Government Organisation Act, the Resident Registration Act, the National Taxation Act, the Medical Service Act, the Infectious Disease Control and Prevention Act, and the National Health Insurance Act, as well as relevant regulations enacted by local governments. For example, the Ministry of Public Administration and Security collects data on public officers for the purpose of personnel, ethics, services, and pension management.[10] It also operates the "National Human Resource Database," which accumulates large amounts of personal information. Medical records are collected and used by the National Health Insurance Corporation in the ordinary course of insurance benefits management.[11]

9. PIPA, above note 3, art 15.

10. Government Organization Act, art 29.

11. National Health Insurance Act, art 13.

In principle, the processors of personal information can disclose personal information only with the consent of the data subject, and only within the scope of the initial purpose of collection.[12] There is an exception in the PIPA, however, that the government and public agencies can disclose personal information for the purpose of law enforcement "where it is necessary for the investigation of crimes, indictment and prosecution, or for the court to process the case or for punishment and enforcement of care and custody."[13]

PIPA establishes specific rules for what is referred to as "sensitive information," which includes information on ideology, belief, admission/exit to and from trade unions or political parties, political mindset, and health and sexual life.[14] Yet there are some exceptions in the Act: The government is allowed to acquire genetic information or criminal records when necessary.[15] PIPA also limits the collection and use of resident registration numbers unless it comes under exceptions specified by the Act. PIPA also requires the government to provide a means for Internet users to subscribe to its websites without submitting their resident registration numbers. In response to the ongoing digitalization of governmental functions, with the result that personal information is stored and managed in the interlinked systems of public agencies, placing at risk information privacy in the public sector, PIPA requires public institutions in specified circumstances to conduct privacy impact assessments.[16]

Whereas PIPA acts as a comprehensive and basic statute on personal information protection, the Telecommunication Business Act (TBA) specially regulates telecommunication service providers. Basically, the Act states that telecommunication service providers must obtain consent from the data subject before providing personal information to a third party, and the third party can use the information only in accordance with the purpose for which it was provided.[17] However, when submitting information to law enforcement authorities who possess a warrant issued by a court pursuant to the Criminal Procedure Act, consent of the data subject is not necessary.[18]

Apart from PIPA and TBA, a number of other statutes, including the Credit Information Act, the Communication Privacy Act, the Real Name Finance Act, and the Act on Use and Protection of DNA Identification Information (DNA Identification Act), provide for data seizure by warrant or other means.

12. PIPA, above note 3, art 17.

13. Ibid., art 18.

14. Ibid., art 23.

15. Ibid., art 23.

16. Ibid., art 33.

17. Act on Communications Network Promotion and Personal Information Protection, art 24-2 [hereinafter Comm Network Act].

18. Huh Soon-Chol, "Internet Search and the Right to Informational Self-Determination," 10:2 *Korean Public LJ* 157 (Korean Comparative Public Law Association, 2009).

In scholarly discourses in Korea, there is a controversy over whether electronic data is subject to seizure and search. According to the Criminal Procedure Act, "the court may seize any *articles* which it believes may be used as evidence or liable to confiscation." In addition, "A person, effects, dwellings . . . may be searched only when there are circumstances which warrant the belief that there are *articles liable to seize* therein."[19] It is argued that, under the express language of these provisions, only tangible articles are eligible to be seized or searched and therefore the provisions of the Act are not applicable to the seizure and search of intangible data. Although the seizure and subsequent search of hard discs, laptops, and other physical media containing data is one action, demanding the disclosure of data stored on such devices is quite different. This distinction raises a question as to the legitimacy of the search and seizure provisions of the Criminal Procedure Act when applied to searches of stored data. Moreover, it is not clear under existing statutes whether the data subject must be notified of the execution of a warrant for data pertaining to that person. In the case of so-called transactional data, the Communication Privacy Act requires the law enforcement authorities to notify the data subjects in writing within 30 days after obtaining records for the purpose of investigation.[20] However, the Criminal Procedure Act imposes no such obligation when seizing and searching articles from a third party, so under that Act enforcement authorities are not required to give any notice when seizing and searching personal information held by a telecommunication service provider.

A warrant issued by a court is not the only means by which the government can obtain personal information. As will be explained below, there are other explicit provisions scattered in various statutes allowing the government to request personal information from the private sector without any warrant.

19. Criminal Procedure Act, art 106, 109.

20. CPA, above note 3, art 13-3, 9-2. The phrase used in the English version of the Communication Privacy Act is not "transactional data" but rather "communication confirmation data," which the Act defines as follow:

> "The term "communication confirmation data" means the data on the records of telecommunications falling under any one of the following items:
>
> (a) The date of telecommunications by subscribers;
> (b) The time that the telecommunications commence and end;
> (c) The communications number of outgoing and incoming call, etc. and the subscriber's number of the other party;
> (d) The frequency of use;
> (e) The computer communications or internet log-records relating to facts of using the telecommunications services by the users of computer communications or internet;
> (f) The data on tracing a location of information communications apparatus connecting to the information communications networks; and
> (g) The data on tracing a location of connectors capable of confirming the location of information communications apparatus to be used by the users of computer communications or internet for connecting with the information communications networks.

B. Law Enforcement Access, Regulatory Access, and/or National Security Access

1. Law Enforcement Access without Court Permission

Regarding public sector data, the government and public agencies may disclose personal information for the purpose of law enforcement without any court permission under the PIPA.[21] Regarding private-sector data, however, government access is only made possible by consent of the data subject, statutory provision, or court permission. There are some exceptions: first, the TBA provides a telecommunication service provider may comply with a request for provision of communications data from a court, a prosecutor, the head of an investigative authority, or the head of an intelligence agency, when necessary for a trial, a crime investigation, the execution of a sentence, or national security. The TBA specifically provides that telecommunication service providers "may" provide to law enforcement agencies communications data such as names of their users, resident registration numbers of users, addresses of users, phone numbers of users, identification codes used to identify the rightful users of communications networks, and dates on which users commence or terminate their subscriptions.[22]

However, such governmental access without a judicial warrant was challenged in the lawsuit described at the beginning of this chapter, which questioned the legitimacy of an ISP's providing the police with users' personal information. The Seoul Central District Court held that the ISP was not responsible for any mental stress experienced by the data subject, because the TBA allows ISPs to provide personal information for trials, crime investigation, or national security reasons.[23] On appeal, however, the Seoul High Court found that the ISP has no obligation to disclose information upon the mere request of law enforcement authorities. Rather, the Seoul High Court held, an ISP is responsible for deciding whether it should provide the requested personal data based upon a careful examination of specific factors such as the seriousness and urgency of the crime, the importance of the public interest, and the degree of infringement on the personal information rights of the data subjects. Accordingly, the High Court held the ISP in this case breached its responsibility and infringed the users' rights of self-determination and to anonymous speech, and ordered the ISP to compensate the users.[24]

2. The Supreme Court Decision on Law Enforcement Access

The case was appealed to the Supreme Court, raising issues as to the availability and scope of the government's authority to access private-sector data and any responsibility of ISPs when presented with government requests. At the end of

21. PIPA, above note 3, art 18.

22. Telecommunication Business Act, art 83.

23. Seoul Central District Court Decision 2010 gahap 72873 (S Korea Jan. 13, 2011).

24. Seoul High Court Decision 2011 na 19012 (S Korea, Oct. 18, 2012).

the court hearing, which took several years, the Supreme Court reversed and remanded the decision of the Seoul High Court.[25] Regarding the availability and scope of government access, the Supreme Court distinguished between mere "contact information" such as name, address, phone number, resident registration number, and user identification codes on the one hand and "telecommunication confirmation data" such as when and how long users communicated, with whom they communicated, and their location information on the other. The Supreme Court found that the Communication Privacy Act clearly provides that the police and other investigative authorities need court permission to get access to telecommunications confirmation data held by the private sector and also to intercept "telecommunication contents."[26] It was held by the Supreme Court, however, that the TBA allowed ISPs to voluntarily provide "contact information" without court permission for the purpose of facilitating law enforcement. The constitutional issue relating to such government access to private-sector data without a court's permission had already been addressed in 2012, when the Constitutional Court of Korea decided that the statutory provision of the TBA does not violate the fundamental right of privacy under the Constitution of Korea as long as it does not impose a mandatory obligation on ISPs to provide contact information to law enforcement authorities.[27]

As the voluntary mechanism of governmental access to private-sector data was interpreted as being constitutional, the Supreme Court of Korea moved forward to deny the responsibility of ISPs: ISPs are themselves not the police nor judicial institutes and, accordingly, ISPs are not expected to bear any responsibility for making case-by-case decisions about how to respond to requests for personal information by investigative authorities.[28] Although ISPs are not under a mandatory obligation under the TBA to provide contact information unless there is court permission, in reality they do not have any alternative but to provide the data in accordance with formal requests of law enforcement authorities. In the case of abusive requests by law enforcement authorities, there may be infringement of personal information rights, but liability for that, the Supreme Court held, must not be borne by ISPs but by the abusive authorities themselves.

As our national security is threatened not only by military attacks from North Korea but also by terrorist attacks from the Islamic State, the Act on Anti-Terrorism for the Protection of Citizens and Public Security (Anti-Terrorism Act)[29] was recently enacted. To have access to communication contents, entry/departure information, and financial information, the National Intelligence Agency

25. Supreme Court of Korea Decision 2012 da 105482 (S Korea, Mar. 10, 2016).

26. CPA, above note 3, art 13.

27. Constitutional Court of Korea Decision 2010 hun-ma 439 (S Korea, March 23, 2012).

28. Supreme Court of Korea Decision 2012 da 105482 (S Korea, March 10, 2016).

29. Act on Anti-Terrorism for the Protection of Citizens and Public Security (law no 14071, enacted on March 3, 2016).

(NIA) of Korea will have to follow the procedure under the Communication Privacy Act, the Immigration Control Act, and the Act on Reporting and Using Specified Financial Transaction Information. According to the Anti-Terrorism Act, however, the NIA will be able without a court warrant to ask ISPs to provide contact information, location information, and other relevant personal information regarding terrorist suspects.[30] Following the Supreme Court decision, ISPs are not responsible to data subjects for disclosure of their personal information unless the requested data clearly do not relate to terrorist suspects.

3. Wire-Tapping and Other Communication-Restricting Measures

The Communication Privacy Act allows "communication-restricting measures" for the investigation of crimes prescribed in the Criminal Act, the National Security Act, or the Military Secret Protection Act, or for other national security purposes, subject to court permission.[31] The term "communication-restricting measures" means "censoring any mail, wire-tapping any telecommunications, providing the communication confirmation data and recording or listening to conversations between others that are not made public." These measures are permitted only when there is a substantial reason to suspect that a crime is being planned or committed or has been committed and it is otherwise difficult to prevent the commission of the crime, to arrest the criminal, or to collect the evidence. The heads of certain intelligence and investigative authorities may also take these measures, when they expect the national security is at risk and the collection of intelligence is required to prevent such danger.[32] When the communication-restricting measures are to be taken against a Korean national, permission must be obtained from a senior chief judge of the high court. With respect to communications of countries hostile to the Republic of Korea, foreign agents, or groups or persons suspected of engaging in antinational activities or in intelligence collection activities for a foreign power, approval must be obtained in

30. Ibid., art 9.

31. CPA, above note 3, arts 5–7.

32. CPA, above note 3, art 7. This Act further provides that heads of Intelligence can use such measures without court permission, when the following conditions are met:

(1) It must be an urgent situation in which an act of conspiracy exists that threatens the national security or an imminent planning/carrying out of any serious or organized crimes that may cause death or serious injury.
(2) There must be a substantial reason to suspect that such conspiracy or crime is being planned or committed or has been committed.
(3) There must be emergency grounds that make it impossible to go through normal procedures to obtain court permission.

However, the heads must apply to the court for ex post facto approval as soon as possible, and if they fail to obtain the approval within 36 hours from the commencement of the measure, the measure must be terminated immediately.

writing from the president of the Republic of Korea. Communication-restricting measures undertaken for the investigation of crime shall not last more than two months and, for national security purposes, four months.

In the event of urgent situations involving an act of conspiracy that threatens the national security, or the planning or committing of any serious or organized crime that may cause death or serious injuries, the public prosecutor, police officer, or any of the heads of the intelligence and investigative agencies may take a communication-restricting measure without permission from the court,[33] provided an application for permission is filed with the court immediately thereafter. If the court does not issue permission within 36 hours from the commencement of the measure, the prosecutor, police officer, or agency head must halt the execution of the measure.

As wiretapping and other communication-restricting measures involve disclosure of communication contents, the threat to privacy becomes serious and could have an enormous chilling effect on freedom of expression if abused by the government. When the Korea National Intelligence Agency had access to certain data packets by wiretapping the Internet under the permission of the Seoul Central District Court, the alleged suspect brought a constitutional suit arguing that the statutory provision allowing for data packet wiretapping was in violation of the fundamental right of privacy under the Constitution. Although the constitutional suit was dismissed because the alleged suspect died,[34] the case highlighted the serious tension between privacy and national security and the possibility of abuse by the government.

4. Regulatory Access

The government may also obtain access to privately held information for regulatory or administrative purposes. When the government collects personal information from the private sector, it is not always clear whether the purpose is for law enforcement or administrative management. One example is the personal information concerning copyright infringers submitted to the Minister of Culture, Sports and Tourism. In the name of enhancing copyright protection, the Copyright Act of Korea gave the minister the authority to demand that Internet Service Providers (ISPs) delete or stop transmitting illegal reproductions or to suspend the infringer's account for online service for a limited period.[35] Furthermore, upon the request of a copyright holder seeking data for lawsuits, the minister may order an ISP to provide the list of people who are suspected of having copies of or transmitting illegal reproductions.[36] Although such governmental seizure of personal information without any control by the court

33. CPA, above note 3, art 8.

34. Constitutional Court of Korea Decision 2011 hun-ma 165 (S Korea, February 25, 2016).

35. Copyright Act of 1957, art 133-2.

36. Ibid., art 103-3.

may promote copyright protection, it has been criticized for unduly infringing the privacy of Internet users.[37]

5. Transparency Report

Given the difficulty of achieving a good balance between the public interest and privacy, and also given the growing concern among Internet users about their personal information, ISPs in Korea such as Naver and Kakao have begun publishing transparency reports.[38] These transparency reports have been made voluntarily. There is no statutory provision requiring government agencies or companies to issue transparency reports. Unlike ISPs, telecommunication companies such as KT, SK Telecom, and LG U+ have not published transparency reports yet. It was reported in the *New York Times* that those three companies had provided law enforcement agencies with subscriber information such as names, addresses, resident registration numbers and other customer information pertaining to more than 6 million phone numbers in the first half of 2014 alone.[39] They provided the information whenever a request was made, without demanding a warrant or informing affected customers.

After the decision of the Seoul High Court in 2012 described above, ISPs such as Naver and Kakao had stopped providing any contact information of their users to government authorities without court warrants or court orders. In 2014, however, there was a news report that government authorities were scrutinizing the data of users of Kakao's messaging app, Kakao Talk. Because court warrants or orders should be strictly limited to criminal investigations or national security, overbroad court warrants or orders might have raised serious privacy concerns among Kakao users. Due to the news report, an estimated 610,000 South Korean smartphone users visited a German competitor Telegram on the same day, a fortyfold increase over the previous day.[40] South Korean users posted reviews on Telegram saying they left Kakao to seek "a Cyber-asylum." As in the FBI-Apple encryption dispute,[41] the government and ISPs in Korea are facing the

37. Sang Jo Jong, "Development and Regulation of Internet Industry," *Justice* (Issue 115, September 2011) 766–87; Sang Jo Jong, "Telecommunication and Intellectual Property: Interaction of Technology, Market and Law," 10:2 *Journal of Korean Law* (Seoul National University Law Research Institute, October 2011) 277–301.

38. Transparency Reporting Index, Access Now http://www.accessnow.org/pages/transparency-reporting-index.

39. Se-Woong Koo, "South Korea's Invasion of Privacy," *The New York Times* (April 2, 2015), http://www.nytimes.com/2015/04/03/opinion/south-koreas-invasion-of-privacy.html?_r=0.

40. "Kakaotalk, Telegram, and the South Korean Government," *Omona They Didn't!* (October 10, 2014), http://omonatheydidnt.livejournal.com/14318239.html.

41. "Apple vs the FBI: A Complete Timeline of the War over Tech Encryption," *Digital Trends* (April 3, 2016), http://www.digitaltrends.com/mobile/apple-encryption-court-order-news/.

most difficult task of balancing the conflicting interests of national security and personal information.

C. Reporting Financial Data and/or Passenger Records

Generally, there are a number of circumstances in which that the government can obtain private-sector data without a warrant. For example, the Korea Communications Commission can demand data from ISPs when a breach of the Communications Network Act occurs or becomes known to the Commission, or when necessary to protect Internet users.[42] The Board of Audit and Inspection, which is empowered to audit the conduct of officials of the national and local governments, can order third parties including ISPs to submit information pertaining to an inspection.[43]

Governmental access to private-sector financial data occurs in two ways: one is when the government requests financial data from credit information companies, and the other is when the government collects the financial data itself in the course of administering a government program.

The first method of government access has a statutory basis. According to the Credit Information Act, when the head of a public institution requests in writing credit information for a purpose allowed by related Acts and subordinate statutes, the credit information company shall provide such information.[44] Although in principle financial information on loans and guarantees may be disclosed only with the prior consent of the data subject, the Act lists a number of exceptions: when the information is sought in accordance with a court order or a warrant, or in an emergency where a person's life is endangered. Also, a credit information company must submit information to the government without obtaining any prior consent when the information is sought under the statutes relating to taxation.[45] The government also might obtain some financial information from credit information companies in connection with the supervision of such companies by the Financial Services Commission. The Commission is authorized to inspect the business and financial standing of credit information companies and demand related information or summon related personnel.[46]

42. Comm Network Act, above note 17, art 64. Although the Korea Communications Commission can demand personal information under this authority, there is a certain limit to the Commission's discretion. Moreover, ISPs have a responsibility to protect personal information by not providing data in excess of such limit. In this sense, although PIPA is not directly applied to the Commission's authority, the basic concepts of PIPA provide criteria that are useful in defining the limits of the Commission's discretion and the responsibility of ISPs, respectively.

43. Board of Audit and Inspection Act, art 27.

44. Use and Protection of Credit Information Act, art 23(7) (Credit Info Act).

45. Ibid., art 32.

46. Ibid., art 45.

The government also has access to information from financial institutions in connection with its anti-money laundering program.[47] More specifically, financial institutions are required to report to the Commissioner of the Korea Financial Intelligence Unit any transaction exceeding US $5,000 (or the equivalent in foreign currency) or 10 million Korean won when the financial institution has reasonable grounds to suspect that the transaction is in relation to money laundering, terrorist activities, or other crime. Financial institutions also must report payments or receipts of cash exceeding 20 million Korean won, subject to some exceptions, within 30 days.

Some financial information is gathered by the government in the course of the government's own credit activities. For instance, the Korea Credit Guarantee Fund (KCGF) and Korea Technology Finance Corporation (KTFC) are established by the government and collect financial information from customers as they carry out their activities. They can request resident registration numbers from the Minister of Administration and Security or personally identifiable information from financial institutions with the consent of the data subject.[48]

When collecting and investigating credit information, credit information companies need to specify the purpose of such collection and investigation and they may use only reasonable and fair measures to the extent required to serve the specified purpose.[49] KCGF and KTFC bear the same liability and are subject to the same limits as ordinary credit information companies with regard to collection and investigation of credit information. Also, credit information companies are not allowed to collect or investigate information that is related to certain sensitive matters, including national security, trade secrets, R&D results, and political beliefs.[50]

Passenger records are also submitted to the government for administrative use. For example, the Director of Customs may request shipping or airline companies to allow inspection of passenger reservation data on the network of the company or to submit such data to the government for the purpose of detecting counterfeit goods, narcotics, firearms and explosives, and other illegal goods.[51] Upon request, the companies must provide nationality, name, date of birth, passport number, reservation number, address, telephone number, itinerary, and travel agency.

Immigration officers also have access to passenger records in certain circumstances. For example, immigration officers may request passenger records from transportation and shipping companies for the purpose of identifying any passenger with an invalid passport or false identity guarantee or invitation, or who is

47. Act on Report and Use of Specific Financial Transaction Information, art 4, 4-2.

48. Credit Info Act, above note 44, arts 24, 34.

49. Ibid., art 15.

50. Ibid., art 16.

51. Customs Act, art 137-2.

carrying firearms or explosives or is otherwise harmful to the general public (e.g., drug addicts).[52] The specific items of information that immigration officers may obtain include are nationality, name, date of birth, passport number, reservation number, address, telephone number, itinerary of journey, and travel agency.

The government may also order individuals, entities, and private-sector organizations, as well as other public agencies, to submit data that the government determines are necessary for statistical purposes.[53]

D. Voluntary Broad Access to Data

As far as personal information is concerned, PIPA and a number of other relevant statutes regulate government access. These statutes prescribe quite clearly the scope of government access and thus provide statutory protection for personal information. On the other hand, in the case of information that is not "personal information" as defined in these statutes or any information that is beyond the scope of these statutes, informal and voluntary disclosure by an entity in the private sector to the government can readily occur without any legal process. As explained above, personal information includes information that when combined with other information makes it possible to identify an individual. It is extremely difficult, however, to make clear distinctions between information that could, in combination with other information, be used to identify an individual and information that could never be used in that way, for it would depend on how the data are structured or treated technically.[54] For example, non-content communication data, such as searched keywords, online behavior records, purchase records, or terminal location records that do not reveal identifiable information by themselves are likely to be regarded as non-personal information, which could be disclosed to the government without any legal responsibility. Therefore, when investigatory authorities request such non-personal information, the third-party entity would lack any statutory grounds for rejecting the request.[55]

To evade possible legal liability, private-sector telecommunication providers and Internet service providers tend to obtain comprehensive prior consent from their subscribers. For example, Apple's privacy policy, which is made a part of the Terms of Use for Apple's website, states as follows:

> It may be necessary—by law, legal process, litigation, and/or requests from public and governmental authorities within or outside your country of

52. Immigration Control Act, art 73-2.

53. Statistics Act, art 25.

54. Korea Communications Commission, *Personal Information Protection Guideline for ISP* (December 2009) 8–10.

55. Na Jon Youn for Korea Internet & Security Agency (KISA), *Use and Protection of Personal Information in Ubiquitous Computing Environment* (2009) 44–45 [hereinafter Youn, 'Use'].

> residence—for Apple to disclose your personal information. We may also disclose information about you if we determine that for purposes of national security, law enforcement, or other issues of public importance, disclosure is necessary or appropriate.[56]

Whether a court would nullify such unlimited and unfair prior consent in favor of the users is not yet clear. There are opinions that such broad prior consent should be accepted at least in practice to protect the service providers, considering the fact that the government exercises substantive power over private-sector entities.[57]

E. The Role of the Courts

In summary, PIPA, the Communications Network Act, the Communication Privacy Act, the Credit Information Act, the DNA Identification Act, and other statutes addressing personal information require the consent of the data subjects for disclosure of personal information held by a third party. As a general rule, the provision of data without consent is allowed only when a court grants a warrant in connection with a criminal investigation or for similar reasons. Therefore, the court is in the position to judge whether the data in question is really necessary and to determine if the investigation is beyond the legitimate scope of the relevant authorities.

In many cases, however, the statues allow the government to access data without a court warrant in the name of law enforcement or administrative functions. For example, the Credit Information Act, the Customs Act, the Immigration Control Act, and the Copyright Act authorize government access to private-sector information for efficient execution of those statutes. In some cases, for example with regards to credit information and traveler records, disclosure without a warrant is permitted in emergency situations. In the case of information related to copyright infringement, which ISPs must submit to the government without judicial review or a court warrant, commentators have criticized the relevant statute as imbalanced because it offers too much protection to copyright holder while neglecting to protect the privacy of those suspected of infringement.

Where there are statutory grounds for government access without a warrant, the courts do have a role in that they must determine ex post whether the governmental access was within the scope of the statute and satisfied all the relevant substantive and procedural requirements. A good example is the court's review of the case involving the poster of a video clip who sued the ISP for deleting his posting based solely on the copyright holder's infringement claim.[58] However, as explained above, in the recent Supreme Court case involving the government

56. Privacy Policy, Apple Korea http://www.apple.com/kr/privacy/.

57. Kim Ki Chang for National Assembly Research Service (NARS), *Cloud Service and Personal Information Protection* (Policy Research Report, December 2011).

58. *Lenz v. Universal Music Corp*, 572 F. Supp. 2d 1150, 88 USPQ 2d 1629 (N.D. Cal. 2008); Seoul High Court 2010 na 35260 (S Korea, October 13, 2010).

minister and the Olympic skater, where the ISP, without a court order, handed over personal information of a suspect accused of libel, it was found extremely difficult to hold an ISP liable for disclosing information to the government in the absence of a clear responsibility on the ISP to examine and balance the conflicting interests of the data subject and law enforcement.[59]

In general, PIPA and other statutes related to personal information specify the conditions and procedures for governmental access to data held by the private sector. Private information that does not fall into the exact definition of personal information has little chance of being protected by laws or judicial oversight. Thus, it is important that the private sector itself endeavors to protect such personally non-identifiable information through a privacy policy or other voluntary mechanisms. Equally, the government needs to seek to expand the protection of the laws by legislating more specific and transparent procedures for government access.[60]

F. Standards for Use, Access, Retention, and/or Destruction

PIPA, the principle statute for personal information protection, explicitly limits the use of information by data processors (including public agencies) to the initial purpose of collection.[61] In addition, the Act requires the immediate deletion of information after the specified retention period prescribed or if the information is no longer needed.[62] Such removal or deletion of data must be accomplished in a way that does not allow it to be recovered or restored.

Most legislation related to personal information contains provisions on usage and retention similar to those in PIPA. For example, the Communications Network Act,[63] the Credit Information Act,[64] the Communication Privacy Act,[65] the DNA Identification Act,[66] the Customs Act,[67] and the Immigration Control Act[68] all have articles addressing purpose specification, use limitation, and data retention.

59. Supreme Court of Korea Decision 2012 da 105482 (S Korea, March 10, 2016).

60. Sang Jo Jong for Korea Communications Commission, *Legal Review on Protection and Use of Personally Non-identifiable Information* (2010) 106–15.

61. PIPA, above note 3, art 15.

62. Ibid., art 21.

63. Comm Network Act, above note 17, arts 24, 29, 64, 64-2.

64. Credit Info Act, above note 44, arts 15, 19.

65. CPA, above note 3, arts 12, 13.

66. Act on Use and Protection of DNA Identification Information, arts 12, 13, 15.

67. Customs Act, art 137-2; Customs Act, presidential decree, art 158-2.

68. Immigration Control Act, arts 12-2, 38, 73-2.

G. Cross-Border and Multi-jurisdictional Issues

PIPA states that when information processors (including public agencies) provide personal information to a third party overseas, they shall inform the data subjects of the purpose for which the information will be disclosed and obtain their consent.[69] However, consent is not required with respect to personal information handled by the government according to the Statistics Act or received for analysis in relation to national security.

A recently proposed statute on Internet cloud services, entitled the "Act on Promotion of Cloud Computing and User Protection (draft)," includes a provision stating that when a user's data will be stored overseas, the cloud computing service provider shall disclose the name, privacy policy, and legal procedures of that country where the data will be located.[70] Also, the provider shall take necessary measures to safeguard the data stored overseas.

V. CURRENT LEGISLATIVE ISSUES AND CONCLUSION

To summarize, there are quite a number of statutes regarding personal information protection in Korea, and some of them provide relatively detailed regulatory measures. Some commentators criticize these laws as too burdensome for data controllers while offering too little protection of personal information.[71] On the other hand, existing legislation fails to address many issues regarding personal information protection.[72] These omissions include information related to browsing history, online behavior, online purchase records, and location information generated by devices such as cell phones, all of which are easily combined with other types of information to produce identifiable information on specific individuals. Accordingly, there are calls for regulations or guidelines defining the limit of governmental access to such information.[73]

69. PIPA, above note 3, art 17.

70. Act on Promotion of Clouding Computing and User Protection (draft) art 27 (Korea Communication Commission Public Notice 2012-79).

71. Sang-Jo Jong, "Developments in Advertising Technologies and Their Challenge to Information Privacy," *Justice* (Issue 106, September 2008) 601–23; Sang-Jo Jong and Young-Joon Kwon, "The Protection of Personal Information and Its Civil Remedies," *BupJo* (Vol 58:3, March 2009) 5–73.

72. Korea Communications Commission, *Personal Information Protection Guideline for ISP* (December 2009) 8–10.

73. Youn, 'Use', above note 55, 44–45.

PART TWO

Governance and Oversight

15

Organizational Accountability, Government Use of Private-Sector Data, National Security, and Individual Privacy

JAMES X. DEMPSEY, FRED H. CATE, AND MARTIN ABRAMS*

I. ABSTRACT

Companies that collect personal data in the course of their business must be accountable for the safe and fair management of that data. The accountability of companies as data stewards extends both to their own processing of data and to processing by their vendors and partners to whom data is disclosed, thus prompting companies to use contract and other means to ensure that entities to whom they disclose data will likewise be responsible, in a chain of accountability that can extend through multiple links. This accountability principle has now been widely incorporated into national and international data protection standards. However, when a government entity demands that a company disclose data in its possession or control, the chain of accountability can be broken if government itself, shielded by secrecy, is not accountable. This chapter examines what companies can do to remain accountable in the face of government disclosure demands. In addition, it concludes that the principles and practices of accountability that have been developed around corporate handling of personal information collected in commercial contexts are directly applicable to data governance within police and intelligence agencies and are especially relevant when those agencies demand disclosure of data held by the private sector.

* Jennifer Stoddart, Privacy Commissioner of Canada from 2003 to 2013, participated in the systematic access project and chaired meetings in Montreal and London that focused on the concept and practice of accountability. The authors gratefully acknowledge her guidance and insight.

II. THE TENSION BETWEEN CORPORATE ACCOUNTABILITY AND GOVERNMENT ACCESS

Under the now well-accepted principle of information accountability, companies that collect personal data in the course of their business must be accountable for the safe and fair management of that data. The accountability of companies as data stewards extends both to their own processing of data and to processing by their vendors and partners to whom data is disclosed. A commitment to the concept of accountability leads companies both to carefully structure their own data collection, use, and retention practices and to use contract and other means to ensure that the entities to which they disclose data will likewise be responsible, in a chain of accountability that can extend through multiple links.

What happens, however, to accountability when a government entity demands that a company disclose data in its possession or control? How can a company follow through on its accountability commitments when the fact of the government's demands and the government's uses of data are cloaked in secrecy? Before the Snowden leaks and other related disclosures, there was a quiet concern among many private-sector entities that government demands were growing.[1] After the Snowden leaks, it became apparent that many countries around the world were demanding disclosure of large quantities of data directly from companies or were seizing it as it moved over communications links between data centers.[2]

In 2015, in *Schrems v. Data Protection Commissioner*, the issue came to a head. For years, the EU-US Safe Harbor agreement had allowed companies to transfer data to the United States if they promised to adhere to privacy standards at least equivalent to those that would have applied to the data had it remained in Europe. However, the data stored in the United States became subject to US government disclosure demands. In *Schrems*, the Court of Justice of the European Union declared the Safe Harbor invalid because it had been adopted without sufficient findings about the rules limiting those US government demands or the availability of any redress for abuse. In essence, the Court found, the accountability chain was broken: companies transferring data to the United States were required to comply with government demands with no assurance that such demands were appropriately limited in purpose and scope.

1. We recognize that there is a difference between an enforceable or compulsory "demand" and a "request" that could, under applicable law, be complied with on a permissive or voluntary basis. This chapter concerns both mandatory and permissive disclosures, and we use the words "demand" and "request" interchangeably.

2. For example, a study for the European Parliament found that "[p]ractices of so-called 'upstreaming' (tapping directly into the communications infrastructure as a means to intercept data) characterize the surveillance programmes" of four out of five of the EU Member States selected for the study. "National Programmes for Mass Surveillance of Personal Data in EU Member States and Their Compatibility with EU Law," a study for the Directorate General for Internal Policies (2013), http://info.publicintelligence.net/EU-MassSurveillance.pdf.

While invalidating the Safe Harbor, the *Schrems* decision left key questions unanswered: What are the minimum standards for government demands? What is the responsibility of the accountable corporation when data is requested by government entities? But as *Schrems* confirmed the threat that government access poses to the accountability framework, its disruption of trans-Atlantic data flows created an urgent need for solutions. And it appears that the accountability framework itself offers part of that solution: elements of the accountability framework can be extended to governmental demands for and uses of data. In approving the Privacy Shield as a suitable improvement over the Safe Harbor, the EU gave some initial indication of what types of internal and external oversight are sufficient to extend the chain of accountability to the government agency demanding access to data held by the private sector. It also indicated how the transparency element of accountability could be satisfied when both the fact of disclosure and the government's uses of the data once obtained must be kept secret.

Accountability in the face of government demands implicates the interests of at least four sets of stakeholders: the companies that collect and process data in the course of providing the vast range of services that characterize the information society; the data protection regulators that enforce privacy laws; the law enforcement and national security agencies that require information about individuals and that rely on the cooperation of the private sector to carry out their vital responsibilities; and consumers, represented by policymakers, regulators, and civil society organizations.

Accountability is inextricably linked to, but nevertheless distinct from, the substantive criteria for data processing. In *Schrems*, the CJEU was concerned both with the criteria limiting government access and use and with the mechanisms by which "persons whose personal data is concerned have sufficient guarantees enabling their data to be sufficiently protected against the risk of abuse." Other chapters in this volume discuss the substantive criteria for access, centered on the principles of necessity and proportionality. These include rules as to permissible purposes of data collection and other processing, the factual threshold that must be met to initiate such actions, the scope and duration of surveillance, and retention periods. Accountability focuses on the question of how, once those rules are established, an entity can ensure that they are followed. In the context of governmental access, accountability turns on the question of how a corporation can assure itself that a government entity demanding data is accountable for the further processing of that data.

III. THE INFORMATION ACCOUNTABILITY FRAMEWORK

The effort to develop accountability principles for data governance began in 2009 as a dialogue among privacy enforcement agencies, governments, civil society, and business, co-facilitated by the Office of the Privacy Commissioner of Ireland and the Centre for Information Policy Leadership at Hunton & Williams LLP. The project published "Data Protection Accountability: The Essential Elements"

in October 2009, describing five essential elements that are the structural building blocks for accountability-based privacy governance.[3] The five elements are:

1. Organizational commitment to accountability and adoption of internal policies consistent with external criteria.
2. Mechanisms to put privacy policies into effect, including tools, training, and education.
3. Systems for internal ongoing oversight and assurance reviews and external verification.
4. Transparency and mechanisms for individual participation.
5. Means for remediation and external enforcement.

These essential elements articulate the conditions that must exist in order for an organization to establish, demonstrate, and test its accountability with respect to the personal data that it processes. One has to look at all five essential elements of accountability to determine whether an organization is fully accountable. For private-sector organizations to be fully accountable, they must have mechanisms to assure the obligations that are attached to data (no matter the application) travel with the data. This requires different mechanisms in different situations. Sometimes contracts are enough. In other situations, there needs to be assurance reviews or audits. No matter the due diligence a company might do, a company cannot be fully accountable unless the entities it provides data to are accountable as well.

The principle of accountability was featured prominently in the Madrid Resolution, adopted by the International Conference of Data Protection and Privacy Commissioners in October 2009. Another important milestone was reached in July 2010 when the Article 29 Working Party issued an Opinion on the principle of accountability, proposing a requirement that data controllers put in place appropriate and effective measures to ensure that privacy rules are complied with and to demonstrate compliance to supervisory authorities. In 2012, the Federal Privacy Commissioner of Canada and the Information Commissioners of Alberta and British Columbia released a document articulating what data protection authorities would expect of organizations under an accountability approach.[4] In 2013, when the Organisation for Economic Co-operation and

3. http://tiaf01.ipower.com/wp-content/uploads/2013/09/The-Essential-Elements-of-Accountability.pdf. The elements of accountability have been fleshed out in a series of guides and tools. See http://www.huntonfiles.com/files/webupload/CIPL_Accountability_Phase_II_Paris_Project.PDF and http://www.informationpolicycentre.com/files/Uploads/Documents/Centre/Accountability_Chart_Phase_IV.pdf. Additional materials on accountability are complied at: http://www.informationpolicycentre.com/resources/.

4. Office of the Privacy Commissioner of Canada (OPC) and Offices of the Information and Privacy Commissioners (OIPCs) of Alberta and British Columbia, *Getting Accountability Right with a Privacy Management Program* (2012), https://www.priv.gc.ca/information/guide/2012/gl_acc_201204_e.asp.

Development revised its highly influential privacy framework, it noted that "the principle of accountability [has] received renewed attention as a means to promote and define organisational responsibility for privacy protection." Building on this experience, the new Part Three of the OECD Guidelines ("Implementing Accountability") introduced the concept of a privacy management program and articulated its essential elements.[5] The Asia-Pacific Economic Cooperation forum's Cross-Border Privacy Rules adopted an accountability-based code of conduct.

Since then, the concept has increasingly come to be incorporated in national data protection systems. In January 2015, for example, the French data protection authority (CNIL) issued a data governance standard that specified 25 requirements for an accountable organization, starting with the existence of both internal and outward-facing privacy policies defining the various permitted uses of data within the company.[6] Ten elements of the French standard focus specifically on the appointment and role of a chief privacy officer inside a company, whereas others address the need for a compliance assessment process and the establishment of procedures by which data subjects can exercise their rights. In 2015, the Colombian Data Protection Authority issued its own accountability guidelines, as did Hong Kong and Australia.

With the 2016 adoption of the European Union's new General Data Protection Regulation, accountability has reached its fullest implementation in law. Article 5 of the GDPR expressly states that "the controller shall be responsible for, and be able to demonstrate compliance with," the core principles relating to the processing of personal information (an obligation that the Regulation expressly refers to as "accountability"). Article 24 further specifies the controller's responsibility:

> Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.

Essentially identical language appears in the equally important but often overlooked directive on personal data processing in the police and judicial area, also adopted in 2016, thereby expressly extending the accountability principle to law enforcement agencies.[7]

5. *The OECD Privacy Framework* (2013), http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

6. CNIL, *Privacy Seals on Privacy Governance Procedures* (2014), https://www.cnil.fr/sites/default/files/typo/document/CNIL_Privacy_Seal-Governance-EN.pdf.

7. *Directive (EU) 2016/680 of the European Parliament and of the Council of 27 Apr. 2016 on the protection of natural persons with regard to the processing of personal data by competent*

As the European Data Protection Supervisor has noted, although accountability is not a new concept, "[w]ith the GPDR, however, comes a quantum shift in emphasis: controllers are responsible." Accountability, the EDPS emphasizes, "goes beyond compliance with the rules—it implies culture change."[8]

IV. RECONCILING ACCOUNTABILITY AND GOVERNMENT ACCESS

This brings us, then, to our challenge: if a national security agency obtaining data from a private-sector company is itself not accountable, the company providing the data has a gap in its accountability framework, even if the company provides the data under compulsion. What steps can be taken to fill this gap by companies, regulators, and agencies demanding data from the private sector?

The issue of accountability and government access to private-sector data has at least four elements:

- How should accountable companies review and limit requests for disclosure?
- How might those requests be parsed beyond what is legal to what is appropriate?
- How might accountable companies be transparent about both requests for data and how they are parsed?
- How might the concept of accountability extend to the governmental entities that are the recipients of the data?

The first three of these questions have been explored by individual companies and on a multi-stakeholder basis by the Global Network Initiative (GNI) and

authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, Article 19, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0680&from=en.

8. EDPS, "EDPS launches Accountability Initiative" (2016), https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Accountability/16-06-07_Accountability_factsheet_EN.pdf. The EDPS uses the following formulation of accountability:

> Accountability in personal data processing involves:
>
> 1. Transparent internal data protection and privacy policies, approved and endorsed by the highest level of the organisation's management;
> 2. Informing and training all people in the organisation on how to implement the policies;
> 3. Responsibility at the highest level for monitoring this implementation, assessing and demonstrating to external stakeholders and supervisory authorities the quality of the implementation;
> 4. Procedures for redressing poor compliance and data breaches.

others.[9] The fourth question—how to extend the principles of accountability to the practices of government itself—is receiving increasing attention as some governments bring their surveillance practices into the light and strengthen their oversight mechanisms. The Privacy Shield agreement between the United States and the EU provided some answers to the fourth question, although it remains to be seen whether the agreement survives the inevitable challenges it will face.

V. WHAT CAN COMPANIES DO TO REMAIN ACCOUNTABLE IN THE FACE OF GOVERNMENT DEMANDS?

Major companies have addressed some aspects of this challenge, committing to review requests from government agencies, including national security agencies, and challenge overbroad ones. Under the GNI implementation guidelines, it is not sufficient for companies merely to say, "We only comply with lawful demands."[10] The GNI implementation guidelines specify that companies should have in place procedures to carefully assess not only whether a government demand is lawful but also whether it is overbroad or inconsistent with international human rights standards. The guidelines specifiy that, when required to provide personal information to governmental authorities, participating companies will:

- Narrowly interpret and implement government demands that compromise privacy.
- Seek clarification or modification from authorized officials when government demands appear overbroad, unlawful, not required by applicable law or inconsistent with international human rights laws and standards on privacy.
- Request clear communications, preferably in writing, that explain the legal basis for government demands for personal information, including the name of the requesting government entity and the name, title and signature of the authorized official.
- Require that governments follow established domestic legal processes when they are seeking access to personal information.
- Adopt policies and procedures to address how the company will respond when government demands do not include a written directive or fail to adhere to established legal procedure. These policies and

9. The Global Network Initiative is a multi-stakeholder collaboration of companies, human rights advocates, investors, and others, working to help Internet companies meet their human rights obligations with respect to privacy and free expression when responding to government demands to disclose customer information or take down or block content. https://www.globalnetworkinitiative.org/.

10. Global Network Initiative, *Implementation Guidelines for the Principles on Freedom of Expression and Privacy*, http://globalnetworkinitiative.org/implementationguidelines/index.php (last visited on April 27, 2017).

procedures shall include a consideration of when to challenge such government demands.
- Narrowly interpret the governmental authority's jurisdiction to access personal information, such as limiting compliance to users within that country.
- Challenge the government in domestic courts or seek the assistance of relevant authorities, international human rights bodies or non-governmental organizations when faced with a government demand that appears inconsistent with domestic law or procedures or international human rights laws and standards on privacy.[11]

Some companies have sought to increase transparency around government requests as another key aspect of accountability. Transparency in this context concerns both legal authorities and the scope of the government's exercise of those authorities: What types of information are being disclosed to government agencies, and under what legal authorities and for what purposes; and how much data, affecting how many customers, is disclosed? Companies are largely at the mercy of national laws and government policy in terms of what they can disclose, but some have pushed to the full extent of those boundaries. Even before the Snowden leaks, companies in the United States, starting first with Google, began issuing transparency reports in which they publish statistical information about the number of government disclosure demands they receive and/or the number of accounts affected. Since 2013, this practice has expanded in the United States. The USA FREEDOM Act, adopted by Congress in 2015, clarified and expanded the ability of companies to disclose information about the number of government demands they had received and the number of customer accounts that were specifically targeted by those demands.[12] Still, US companies remain constrained by some government-imposed limits.

Outside the United States, there has also been movement toward corporate transparency. A 2015 report found that, for the first time a small handful of Canadian carriers had begun issuing their own Transparency Reports.[13] There have also been some positive changes, especially in Europe. A major

11. Ibid., pp. 8–10.

12. The law does not permit companies to disclose the number of customers affected by demands, so if a company receives one request affecting millions of customers, it cannot use the numbers to indicate that. Other parts of the USA FREEDOM Act prohibited the issuance of bulk demands.

13. Andrew Clement & Jonathan A. Obar, *Keeping Internet Users in the Know or in the Dark: A Report on the Data Privacy Transparency of Canadian Internet Carriers* (March 12, 2015) at p. 5, https://ixmaps.ca/docs/DataPrivacyTransparencyofCanadianCarriers-2014.pdf. The report went on to state, "While the details in these reports are typically scanty, and not up to the standards being established by large US service providers, this is a good sign that Canadian carriers are beginning to respond to public pressure for greater transparency." Ibid.

development occurred in 2014, when Vodafone issued a transparency report on law enforcement demands it faced in 29 countries.[14]

Other European-based companies followed suit, including Orange, Deutsche Telekom, and Teliasonera, as did the Australian Telstra. These reports are limited to law enforcement requests. Vodafone's reports are by far the most detailed outside the United States. As Deniz Duru Aydin of Access Now noted in July 2015, "Whole continents, such as Latin America and Asia, remain dark, as neither telecoms nor governments reveal their handover of user data."

A third component of corporate accountability with respect to government access concerns whether the company maintains control over its own network. Vodafone's 2014 report contained an extraordinary acknowledgment that in some countries authorities had unmediated access to the company's communications network:

> However, in a small number of countries the law dictates that specific agencies and authorities must have direct access to an operator's network, bypassing any form of operational control over lawful interception on the part of the operator. In those countries, Vodafone will not receive any form of demand for lawful interception access as the relevant agencies and authorities already have permanent access to customer communications via their own direct link.

Vodafone made it clear that it was opposed to these requirements of direct access and that it preferred instead to follow the lawful interception technical standards set down by the European Telecommunications Standards Institute (ETSI), which define the separation required between a government monitoring center and the operator's network. As Vodafone explained:

> The ETSI standards are globally applicable across fixed-line, mobile, broadcast and internet technologies, and include a formal handover interface to ensure that agencies and authorities do not have direct or uncontrolled access to the operators' networks as a whole. We continuously encourage agencies and authorities in our countries of operation to allow operators to conform to ETSI technical standards when mandating the implementation of lawful interception functionality within operators' networks.

VI. WHAT CAN GOVERNMENTS DO TO RESPECT ACCOUNTABILITY?

Although the GNI principles encourage companies to challenge government demands that appear inconsistent with domestic law or procedures or international human rights laws and standards on privacy, companies are limited

14. Vodafone, *Law Enforcement Disclosure Report* (last visited April 27, 2017), https://www.vodafone.com/content/sustainabilityreport/2014/index/operating_responsibly/privacy_and_security/law_enforcement.html#csctag.

in what they can do. Prior to the Snowden leaks, there had been some attention to the principle of government accountability with respect to acquisition of private-sector data, especially in the jurisprudence of the European Court of Human Rights (in cases such as *Weber and Saravia v. Germany* and *Liberty v. UK*), as well as in the prescient report of Frank La Rue, the UN special rapporteur. In the United States, intense debates around the PATRIOT Act and related governmental powers led to the creation of the independent Privacy and Civil Liberties Oversight Board and to the creation of Privacy Officers within federal law enforcement and intelligence agencies. Following the Snowden leaks, there were extensive calls on both sides of the Atlantic for greater governmental accountability. The *Schrems* decision, in striking down the Safe Harbor, affirmed those calls and prompted a more granular focus on US practices.

In 2014, in response to the Snowden leaks, the Article 29 Working Party adopted an opinion on surveillance[15] in which it made specific recommendations for governments that map to two key components of accountability: transparency and oversight. On transparency, the Working Party said that Member States should be "transparent to the greatest extent possible about their involvement in intelligence data collection and sharing programmes, preferably in public, but if necessary at least with their national parliaments and the competent supervisory authorities."[16] This includes transparency as to legal authorities: "these programmes have to be based in clear, specific, and accessible legislation." Effective and independent oversight of the intelligence services is of the "highest importance," the Working Party said. It identified specific elements of oversight that it found to be best practices drawn from the mechanisms in place in Member States:

- Strong internal checks for compliance with the national legal framework;
- Effective parliamentary scrutiny; and
- Effective, robust, and independent external oversight, "performed either by a dedicated body with the involvement of the data protection authorities or by the data protection authority itself."[17]

In June 2014, the Office of the High Commissioner for Human Rights (OHCHR) issued a report on the right to privacy in the digital age. The OHCHR specifically noted the importance of procedural safeguards and effective oversight, stating that the right to the protection of the law against unlawful or arbitrary

15. Article 29 Data Protection Working Party, *Opinion 04/2014 on Surveillance of Electronic Communications for Intelligence and National Security Purposes* (adopted on April 10, 2014), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp215_en.pdf.

16. Ibid., p. 12.

17. Ibid., p. 13.

interference or attacks on privacy "must be given life through effective procedural safeguards, including effective, adequately resourced institutional arrangements."[18] The OHCHR went on to state:

> Internal safeguards without independent, external monitoring in particular have proven ineffective against unlawful or arbitrary surveillance methods. While these safeguards may take a variety of forms, the involvement of all branches of government in the oversight of surveillance programmes, as well as of an independent civilian oversight agency, is essential to ensure the effective protection of the law.[19]

And the OHCHR called out the right to an effective remedy, noting that Article 2 of the ICCPR states in paragraph 3 (b) that States parties to the Covenant undertake "to ensure that any person claiming such a remedy shall have his right thereto determined by competent judicial, administrative or legislative authorities, or by any other competent authority provided for by the legal system of the State, and to develop the possibilities of judicial remedy."[20] Effective remedies, the OHCHR stated, can come in a variety of judicial, legislative, or administrative forms, but they typically share certain characteristics. First, those remedies must be known and accessible to anyone with an arguable claim that his or her rights have been violated. Notice (that either a general surveillance regime or specific surveillance measures are in place) and standing (to challenge such measures) thus become critical issues in determining access to an effective remedy. Second, effective remedies will involve prompt, thorough, and impartial investigation of alleged violations. Third, for remedies to be effective, they must be capable of ending ongoing violations. Fourth, he stated, where human rights violations rise to the level of gross violations, nonjudicial remedies will not be adequate, as criminal prosecution will be required.

Companies, too, in the wake of the Snowden revelations called for greater governmental accountability, to restore trust. Under the banner of "Reform Government Surveillance," a group of US-based companies recommended that accountability elements be built into government surveillance practices, including those of the US government. The companies' recommendations specifically highlighted transparency and oversight.[21]

Individual companies also called for greater government transparency. For example, when Verizon released its 2014 transparency report, in which it published data on National Security Letters, the company noted that it was still

18. Office of the United Nations High Commissioner for Human Rights, *The Right to Privacy in the Digital Age* (June 30, 2014) at 12 http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf.

19. Ibid., pp. 12–13.

20. Ibid., p. 13.

21. https://www.reformgovernmentsurveillance.com/.

limited in what it could publish, and it called on the US government to itself be more open: "We once again call on all governments to make public the number of demands they make for customer data from such companies, because that is the only way to provide the public with an accurate data set."[22]

Although several chapters in this volume find that national governments have in recent years extended their surveillance powers, some national governments have at the same time improved their accountability mechanisms.

It is undeniable, for example, that the United States is more transparent than it was before the Snowden leaks. The 2015 USA FREEDOM Act, as noted above, expanded somewhat the ability of companies to disclose information about government requests they received. The Office of the Director of National Intelligence has a website, IC on the Record,[23] which publishes information of a scope and depth that would have been inconceivable before the Snowden leaks, including opinions of the special court that authorizes surveillance inside the United States, procedures for exercising various authorities, statistics on the use of those authorities, and compliance reports. The National Security Agency and the Central Intelligence Agency have both appointed senior officials devoted solely to the privacy and civil liberties portfolio. Likewise, the UK in 2015 published what it promised would be an annual transparency report on investigatory powers.[24] Also in the UK, an independent Interception of Communications Commissioner publishes detailed reports on the authorities exercised by the government, including both descriptions of the legal standards and statistical data on the frequency of their use. (In both the United States and the UK, the statistics provide only a partial picture of the scope of government surveillance.)

In 2014, US president Barack Obama issued a policy directive making certain commitments as to how the US government will handle data collected through signals intelligence in the national security context.[25] Substantively, the directive specified that signal intelligence activities of the United States "shall be as tailored as feasible," but it went on to acknowledge that the US government did

22. Verizon, "Updates to Our 2013 Transparency Report," *Verizon News* (March 3, 2014), https://www.verizon.com/about/news/updates-to-our-2013-transparency-report. Verizon provides service in 18 countries in addition to the United States. In all but Germany, it is prohibited from reporting information about the interception of content. See Verizon, *International Report* http://www.verizon.com/about/portal/transparency-report/international-report/ (last visited April 27, 2017).

23. https://icontherecord.tumblr.com/.

24. *HM Government Transparency Report 2015: Disruptive and Investigatory Powers*, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473603/51973_Cm_9151_Transparency_Accessible.pdf.

25. Presidential Policy Directive 28—Signals Intelligence Activities (January 17, 2014), http://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.

engage in bulk collection of communications and information about communications. The directive spoke specifically to accountability:

> [T]he policies and procedures of IC [Intelligence Community] elements, and departments and agencies containing IC elements, shall include appropriate measures to facilitate oversight over the implementation of safeguards protecting personal information, to include periodic auditing . . . .
>
> The policies and procedures shall also recognize and facilitate the performance of oversight by the Inspectors General of IC elements . . . and other relevant oversight entities, as appropriate and consistent with their responsibilities.

As Sarah St.Vincent notes in her chapter in this volume, cases pending before the European Court of Human Rights challenging the UK's surveillance practices may produce further limits on government data collection and use, as did the recent CJEU case on data retention. Already, the cases of the ECtHR constitute perhaps the fullest body of international law on government surveillance, analyzed by Ira Rubinstein, Greg Nojeim, and Ron Lee in their chapter in this volume. Certain basic criteria that the ECtHR has articulated in assessing government access programs provide reference points in assessing government accountability:

- "In accordance with law." Under the jurisprudence of the ECtHR, surveillance standards must be spelled out in a public law or regulation precisely enough to protect against arbitrary application and to inform the public of which entities can conduct surveillance and under what criteria. Such laws must specify not only the standards for collecting data but also the limits on examining, using, and storing it.
- Oversight by independent entity. An independent body (judicial, executive, legislative) must oversee the actual implementation of surveillance procedures to protect against abuse.
- Redress (remedy). Individuals must be able to obtain redress for violations of the established standards.[26]

One of the fullest discussions to date of government accountability can be found in the decision of the European Commission on the adequacy of the US commitments that constitute the Privacy Shield.[27] The Commission focused on both

26. See D. Korff, "Note on European and International Law on Transnational Surveillance prepared for the Civil Liberties Committee of the European Parliament" (August 23, 2013), http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/note_korff_/note_korff_en.pdf.

27. European Commission, *Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield*, available at http://ec.europa.eu/justice/data-protection/international-transfers/eu-us-privacy-shield/index_en.htm.

the substantive rules limiting US surveillance as well as on the accountability mechanisms intended to assure compliance with those rules. The Commission found that the US intelligence agencies are subject to oversight by both internal and external bodies, congressional committees, and, to some extent, judicial supervision. Within the executive branch, the Commission found that "[m]ultiple oversight layers have been put in place, including civil liberties or privacy officers, Inspector Generals, the ODNI [Office of the Director of National Intelligence] Civil Liberties and Privacy Office, the PCLOB [Privacy and Civil Liberties Oversight Board], and the President's Intelligence Oversight Board."[28] These oversight entities are supported, the Commission said, by compliance staff in all the agencies. The Commission further noted that intelligence agencies are encouraged (but not required) to design information systems to allow for auditing of queries or other searches of personal information.There are extensive reporting requirements, the Commission stated, with respect to noncompliance. In addition to oversight mechanisms within the executive branch, the Commission noted, congressional committees have oversight responsibilities regarding all US foreign intelligence activities. Third, the Commission noted, data acquisition in the United States is overseen by a Foreign Intelligence Surveillance Court, an independent tribunal.

The Commission stated that a number of avenues were available under US law to EU data subjects concerned about whether their personal data had been processed by the US intelligence community. However, the Commission noted these avenues were limited by exceptions, including doctrines restricting judicial access. In order to address these concerns, the US government committed to creating a new oversight mechanism, the Privacy Shield Ombudsman, independent of the intelligence agencies, to receive and investigate complaints. Moreover, the United States agreed that, unlike plaintiffs in ordinary judicial cases in the United States, an individual complaining to the Ombudsman would not have to demonstrate that his/her personal data have in fact been accessed by the US government in order to have a complaint heard. The US government made a commitment that individuals will receive from the Ombudsman independent confirmation that US laws have been complied with or, in a case of violation, the noncompliance has been remedied.

It remains to be seen whether the Privacy Shield commitments of the US government are borne out in practice and whether they are upheld against the seemingly inevitable challenges they will face at the national and EU level. But they represent perhaps the fullest commitment to date of any country to establish a system of accountability for data acquired from the private sector.

28. Ibid., para. 95.

VII. CONCLUSION: MAPPING THE ACCOUNTABILITY FRAMEWORK TO GOVERNMENT ACCESS PROGRAMS

Applying the broad concept of accountability to intelligence services is not new.[29] Government officials, institutions such as the Geneva Centre for the Democratic Control of Armed Forces (DCAF), human rights advocates, and scholars around the world have for decades been developing and commenting upon best practices for intelligence oversight.[30] The special insight we are proposing here is that the principles and practices of accountability that have been developed around corporate handling of personal information collected in commercial contexts are directly applicable to data governance within police and intelligence agencies and are especially relevant when those agencies demand disclosure of data held by the private sector.

As expressed elsewhere in the volume, governments and human rights institutions are continuing to define the standards for government demands of access to data held by the private sector. Our point in this chapter is that the protection of privacy does not end when data is transferred pursuant to criteria meeting human rights standards. The transfer of private-sector data to the government for law enforcement or national security purposes starts a new accountability chain.

Accountability, especially in the national security context, is difficult to maintain. Any and all of the elements of an effective oversight system may fail or be frustrated, at least for a time. In the United States, from 2006 through 2013, the Foreign Intelligence Surveillance Court repeatedly, without written analysis, stretched a statute beyond recognition to authorize a bulk telephone metadata program (now ended). In 2016, in Germany, the Data Protection Commissioner found that the foreign intelligence agency had illegally and massively restricted her supervision authority on several occasions, "making comprehensive and efficient control not possible."[31] Moreover, accountability, as noted above, is only as effective in protecting rights as the substantive rules that the system enforces.[32] Nevertheless, it is increasingly apparent that the five essential elements of

29. See, for example, Hans Born and Ian Leigh, *Making Intelligence Accountable: Legal Standards and Best Practice for Oversight of Intelligence Agencies* (2005).

30. See Zachary K. Goldman and Samuel J. Rascoff, *Global Intelligence Oversight: Governing Security in the Twenty-First Century* (2016).

31. Andre Meister, "Secret Report: German Federal Intelligence Service BND Violates Laws and Constitution by the Dozen," *Netzpolitik.org* (September 2, 2016), at https://netzpolitik.org/2016/secret-report-german-federal-intelligence-service-bnd-violates-laws-by-the-dozen/.

32. "Even if perfect compliance could be achieved, however, it is too paltry a goal. A good oversight system needs its institutions not just to support and enforce compliance but to design good rules." Margo Schlanger, "Intelligence Legalism and the National Security Agency's Civil Liberties Gap," 6 *Harvard National Security Journal* 112 (2015).

accountability can and must be transposed into the governmental context. We conclude with the following observations:

A. Organization Commitment to Accountability and Adoption of Internal Policies Consistent with External Criteria

Accountability for any surveillance program begins with the criteria laid down in a public law. The ECtHR has made it clear that a law must describe a governmental power precisely enough to protect against arbitrary application and to inform the public of which entities can conduct surveillance and under what criteria. However, translating the necessarily broad and often generic criteria of statue into internal operating procedures is not easy, especially in more complex systems where multiple kinds of data may be collected through various means. Nevertheless, the externally stated rules and the internal practices must be consistent.

B. Mechanisms to Put Privacy Policies into Effect, including Tools, Training and Education

"Tools" may include audit trails, documentation, and permissioning systems for internal access and query. Tools may also include privacy impact assessments, formal internal processes that assess the risks to individuals associated with new processing (including collection). Of course, to make the assessment process meaningful, mitigating those risks must be part of the final processing plan. Such privacy by design practices should be part of an agency's comprehensive privacy program. Training should start with an understanding of privacy and data protection, since the terms, although widely used, are often misunderstood.

C. Systems for Internal Ongoing Oversight and Assurance Reviews and External Verification

Nico van Eijk, in his chapter in this volume, identifies the seven key characteristics of effective oversight:

- Oversight must be comprehensive, in three respects: (a) The government (the executive branch), the legislature, the judiciary, and a specialized (non-parliamentary, independent) commission should all play a role. (b) Oversight should include prior oversight, ongoing oversight, and oversight after the fact. (c) The oversight bodies' mandate should encompass review of both lawfulness and effectiveness.
- Oversight should encompass all stages of the intelligence cycle, including collection, storage, querying, and analysis of data.

- Some of the oversight bodies must be independent of the intelligence services and the government. Judicial oversight offers the best guarantees of independence.
- Oversight should take place prior to the imposition of a measure. Although prior judicial oversight is strongly preferred, van Eijk states that a system of ministerial orders combined with prior oversight by an independent, specialized commission; after-the-fact oversight on the overall functioning of the system of surveillance by a parliamentary committee; and the possibility for individuals to complain before an independent body could also be compliant with human rights standards.
- Oversight bodies should be able to declare a measure unlawful and to provide for redress.
- Oversight should incorporate the adversary principle.
- Oversight bodies should have sufficient resources to perform effectively.

D. Transparency and Mechanisms for Individual Participation

Transparency means both public awareness of what the law actually authorizes as well as numerical reporting to indicate the scope of government access. As the Article 29 Working Party stated: "Some form of general reporting on surveillance activities should be in place."[33] The systems of the United States and the UK, although not perfect, offer important templates for transparency. Individual participation, on the other hand, remains the most underdeveloped element of the accountability system.[34]

E. Means for Remediation and External Enforcement

In its most robust form, remediation is normally equated to judicial redress. However, in approving the Privacy Shield, the EU Commission found that a "composite structure" that included the Ombudsman Mechanism guaranteed individual redress. The key point is that some independent entity must have the ability to insist on remedial action, and the security services must commit to respect that judgment.

33. The Working Party cited the decision of the ECtHR in *Youth Initiative for Human Rights v. Serbia* (June 25, 2013).

34. See Rebecca Richards, Civil Liberties and Privacy Office, NSA, "Defining Privacy" (November 12, 2014), https://www.nsa.gov/about/civil-liberties/resources/assets/files/PCLOB_Remarks_20141112.pdf.

16

Surveillance and Privacy Protection in Latin America

Examples, Principles, and Suggestions

EDUARDO BERTONI AND COLLIN KURRE

I. ABSTRACT

This chapter covers surveillance and privacy protection in Latin America providing examples, principles, and suggestions. The first part offers an overview of governmental surveillance regulation through an analysis of existing legislation in four Latin American countries: Argentina, Colombia, Mexico and Peru. It should be noted that this analysis merely seeks to identify trends in legal frameworks, rather than provide a comprehensive account of existing laws. Regulating state surveillance and creating a precedent of rights protection both off- and online is critical. To provide a more nuanced and updated understanding of how human rights should be protected online, the second part of this chapter examines several sets of principles that have been created by civil society actors, technical experts, and human rights specialists. The chapter compares those principles with the actual legislation in the four countries surveyed, and concludes with some suggestions for future policymaking concerning communications interceptions and surveillance in Latin America.

II. INTRODUCTION

Debates concerning the protection of personal privacy and freedom of expression certainly predate Edward Snowden's 2013 revelation of massive national and international surveillance operations in the United States and beyond. In recent years, however, three interrelated factors have made discussions of privacy protection more salient: the permeation of Internet use across all facets of modern life, the resulting ease of data collection on an unprecedented scale, and the demonstrated existence of governmental programs to collect and store such

Bulk Collection. Fred H. Cate and James X. Dempsey.

data on a massive basis. To be clear: governmental surveillance might be justifiable in certain cases—for example, for the prosecution of serious crimes or human rights abuses. However, permitting any government unfettered access to citizens' private communications violates fundamental rights, jeopardizes democratic institutions, creates a culture of fear or self-censorship, and has proven ineffective in preventing future crimes.

In Latin America, historical context is important for discussions of privacy protection and judicial restrictions on governmental surveillance. In many cases, the most egregious violations of human rights under Latin American dictatorial governments were fundamentally linked to surveillance operations conducted by intelligence agencies. Such surveillance operations typically targeted dissident groups, journalists, students, and trade unions,[1] even though the right to privacy was and is included in the constitutions of these countries.

The first part of this chapter provides an overview of governmental surveillance regulation through an analysis of existing legislation in four Latin American countries: Argentina, Colombia, Mexico, and Peru. These countries represent a diverse sample group geographically and institutionally, and in terms of Internet penetration.[2] It should be noted that this analysis merely seeks to identify trends in legal frameworks, rather than provide a comprehensive account of existing laws.

Regulating state surveillance and creating a precedent of rights protection both off- and online is critical. To provide a more nuanced and updated understanding of how human rights should be protected online, the second part of this chapter examines several sets of principles that have been created by civil society actors, technical experts, and human rights specialists. The chapter compares those principles with the actual legislation in the four countries surveyed.[3]

Finally, the chapter concludes with some suggestions for future policymaking concerning communications interceptions and surveillance in Latin America.

1. R.A. Ugarte & E. Villa, *Who's Watching the Watchers?: A Comparative Study of Intelligence Organizations Oversight Mechanisms in Latin America*, Privacy International, Asociación por los Derechos Civiles (2014). See https://www.privacyinternational.org/node/351.

2. According to the Internet Society (ISOC), the rate of Internet penetration in Latin America hovers around 30 percent (see http://www.internetsociety.org/what-we-do/where-we-work/latin-america-caribbean). Within the sample group, Argentina and Colombia have higher-than-average penetration rates, whereas Mexico and Peru have lower (see http://www.internetworldstats.com/stats10.htm). In all cases, the growth in the rate of penetration shows no signs of slowing—on the contrary, the Latin American Internet audience grew 23 percent in 2014 alone.

3. Principles that are included in the analysis are: Necessary and Proportionate, Tshwane, Manila, and OAS Inter-American Juridical Committee.

III. FOUR EXAMPLES OF SURVEILLANCE LEGISLATION IN LATIN AMERICA

In Latin America, surveillance legislation is frequently taken as a suggestion instead of a firm rule, and the reality of government activities frequently oversteps legislated constraints. However, understanding the legal frameworks remains important for making valid and practical policy recommendations. In Latin America, two commonalities can be identified among intelligence activities: first, partisan abuse of surveillance techniques to monitor the opposition; and second, habitual attempts of police and intelligence forces to increase autonomy and limit checks on authority. Although the implications of such will be further explored later on, it is important to acknowledge that governments' simultaneous obligations to safeguard individual rights while addressing threats to public safety are neither aligned nor mutually exclusive. Instead, these two imperatives are manifested as a balancing act for which there is no universal solution. In the following subsections, the legal frameworks for Argentina, Colombia, Mexico, and Peru are briefly explored.

A. Argentina

Though government surveillance capabilities are abundant and well known in Argentina, the right to privacy in personal communications is specifically defined in the Argentine Constitution.[4] In terms of legislation for data protection and the right to privacy, the pendulum has swung in both directions. In addition to the requirement for judicial authorization and other specific protocols for communications interceptions specified in the Federal Criminal Procedure Code,[5] the Personal Data Protection Law, passed in 2000, addressed the administration of public and private databases with provisions for user consent and its revocation,[6] the mandatory destruction of irrelevant data,[7] and the requirement for legal authorization when releasing personal data.[8] Four years later, the Mobile Communications Services Law 25.891 mandated that telecommunications companies maintain databases of personal data (name, address, etc.) to enable the

4. Constitution of the Argentine Nation. (1953, reinstated 1983). Art. 18: "The residence is inviolable, as are letters and private papers; and a law shall determine in what cases and for what reasons their search and seizure shall be allowed." See https://www.constituteproject.org/constitution/Argentina_1994.pdf.

5. Argentine Criminal Procedure Code. (August 21, 1991). Art. 236. See http://www.infoleg.gov.ar/infolegInternet/anexos/0-4999/383/texact.htm.

6. Personal Data Protection Law, Law 25.326, art. 11, §§ 1–4. (October 30, 2000). See http://www1.hcdn.gov.ar/dependencias/dip/textos%20actualizados/25326.010408.pdf.

7. Ibid., art. 4, § 11.

8. Ibid., art. 7, § 2.

clear identification of their customers,[9] which many considered an unnecessary violation of privacy.[10] Most recently, the 2014 Argentina Digital Law reiterated the inviolability of communications and granted all communications, electronic or otherwise, protection equal to that previously granted to postal services, permitting interception only with authorization from a competent judge.[11]

Other limits and safeguards for surveillance and intelligence gathering exist on the books. For example, the 1991 Domestic Security Law established the Bicameral Auditing Committee to monitor domestic security and intelligence activities.[12] The first oversight mechanism of its kind in Latin America, the Committee had one widely publicized success case when it identified illegal state surveillance of unions and student organizations in 1993. However, its oversight and enforcement powers were limited.[13]

In 2001, the National Intelligence Law expanded the aforementioned committee, renaming it the Bicameral Committee for the Oversight of Intelligence and Internal Security Bodies and Activities.[14] This Committee is now charged with the task of supervising all communications interceptions and has been granted the power to investigate intelligence activities on its own initiative.[15] By law, all parts of the National Intelligence System must honor any of the Committee's requests for information or documentation and must submit to it annual reports.[16] The reports are approved by the Intelligence Secretariat's Directorate of Judicial Surveillance, which is also the sole overseer for judicial authorizations for communications interceptions.

These oversight mechanisms are frequently criticized by advocacy groups, on several grounds. First, the Intelligence Secretariat reports directly to the executive, effectively giving the president power over the subsidiary branches dealing with criminal and military strategic intelligence.[17] Some suggest that under

9. Mobile Communications Services Law, Law 25.891, art. 2. (April 28, 2004). See http://servicios.infoleg.gob.ar/infolegInternet/anexos/95000-99999/95221/norma.htm.

10. V. Ferrari & D. Schnidrig, *Vigilancia de las Comunicaciones por la Autoridad y Protección de los Derechos Digitales en Argentina*, CELE, EFF (October 2015). See https://www.eff.org/files/2015/11/24/argentina-es-final.pdf.

11. Argentina Digital Law, Law 27.078, art. 5. (December 16, 2014). See http://www.infoleg.gob.ar/infolegInternet/anexos/235000-239999/239771/norma.htm.

12. Domestic Security Law, Law 24.059, art. 33. (December 18, 1991). See http://servicios.infoleg.gob.ar/infolegInternet/anexos/0-4999/458/texact.htm.

13. Ugarte & Villa, above note 1, p. 12.

14. National Intelligence Law, Law 25.520, art. 32. (2001, Nov 27). See http://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70496/norma.htm.

15. Ibid., art. 32.

16. Ibid., art. 33, § 4.

17. Ibid., art. 7.

the control of the executive, the Secretariat has been used for political ends.[18] Moreover, the NGO Asociación por los Derechos Civiles (ADC) has found that none of the deputies from Congress has ever received an annual report from the oversight Committee, meaning the check exists only in theory.[19] Third, the Regulatory Decree 950 makes the Bicameral Committee's capacity to access classified information dependent on the Secretariat's authorization—effectively subjecting the oversight mechanism to the will of the institution being monitored.[20]

In January 2015, following the controversial death of federal prosecutor Alberto Nisman, President Cristina Fernandez de Kirchner held a televised address to present a bill to dissolve the Intelligence Secretariat. That bill became the Federal Intelligence Agency Law, transferring the "personnel, assets, current budget, and equity" of the Intelligence Secretariat to a new entity, the Federal Intelligence Agency (AFI).[21] Responding to criticisms, one improvement is that the executive-designated Director and Subdirector of the AFI must be approved by the Senate, providing a legislative check.[22] Despite these changes, there is ongoing concern that surveillance and intelligence activities in Argentina remain convoluted, politically charged, and, in practice, free of oversight from the public or independent bodies.

As the most technologically advanced country of those in question, Argentina's state and intelligence activities boast access to sophisticated techniques for data collection. One such measure is the new federal biometric system for the identification of citizens, SIBIOS, which was introduced by President Cristina Fernandez de Kirchner in 2011 and uses physical traits such as fingerprints and face scans to uniquely identify nationals and foreigners alike.

B. Colombia

In terms of codified law, Colombia has clearly-defined processes and oversight mechanisms for data interception. Under the Criminal Procedure Code, requests for communications interceptions must be approved by the attorney general's office.[23] Such requests must have a stated investigative purpose and must specify the data subjects, the type of data to be collected, and the duration of the

18. J.M. Ugarte, "Sistema de inteligencia nacional argentino: ¡Cambiar ya!," Latin American Studies Association (2000) p 13. See http://lasa.international.pitt.edu/Lasa2000/Ugarte.PDF.

19. Ibid.

20. National Intelligence Law, Decree 950, art. 2. (June 5, 2002). See http://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/74896/norma.htm.

21. Federal Intelligence Agency Law, Law 27.126, art. 24. (February 25, 2015). See http://www.infoleg.gob.ar/infolegInternet/anexos/240000-244999/243821/norma.htm.

22. Ibid., art. 8.

23. Colombian Criminal Procedure Code, art. 114, § 3. (August 31, 2004). See https://www.oas.org/juridico/mla/sp/col/sp_col-int-text-cpp-2005.html.

surveillance.[24] Furthermore, communications interceptions must be authorized by a competent judicial authority (although retroactive approval is permitted),[25] and the Penal Code specifies that illegal interception of data without judicial order carries criminal penalties of 36 to 72 months in prison.[26]

In addition to the protocols and safeguards for data collection indicated in the penal and criminal procedural codes, there are several laws that deal directly with governmental surveillance and personal data. Expanding upon The Telecommunications Law of 2009 and the Citizen Security Law, which expanded investigatory powers in 2011.[27] Decree 1704 mandated that service providers must maintain accurate subscriber details such as identity, address, and connection information for a period of five years.[28] Although there is no specific provision for the companies to retain other communications metadata, the law specifies that if any additional metadata is retained for business purposes, the government can request it for up to five years.[29]

Colombia's Data Protection Law, passed in 2012, was intended to expand the constitutional "Right to Know" as applied to personal information stored in public or private databases.[30] Under the law, the data subject must always give prior, express, and informed consent for all activities pertaining to the collection, use, and transfer of personal data—except those specifically exempted from the law, such as credit data.[31] The Data Protection Law established the National Register of Databases as a public directory of all databases in the country to be consulted by any citizen.[32] However, personal data acquired by the various law enforcement agencies' mass data collection platforms do not appear in these registers.

24. Colombian Penal Code, art. 269, § C. (July 24, 2000). See http://perso.unifr.ch/derechopenal/assets/files/legislacion/l_20130808_01.pdf.

25. J.C. Rivera & K. Rodriguez, "Vigilancia de las Comunicaciones por la Autoridad y Protección de los Derechos Fundamentales en Colombia," EFF (May 2015). See https://www.eff.org/files/2015/05/19/colombia-principios-may-14.pdf.

26. Ibid.

27. The Telecommunications Law, Law 1341, art 4, § 10. (July 30, 2009). See http://www.mintic.gov.co/portal/604/articles-3707_documento.pdf. Citizen Security Law, Law 1453, arts. 52 and 53. (June 24, 2011). See http://www.mintic.gov.co/portal/604/articles-3709_documento.pdf.

28. Decree 1704, art. 4. (August 15, 2012). See http://www.mintic.gov.co/portal/604/articles-3559_documento.pdf.

29. Rivera & Rodriguez, above note 25, p 20.

30. Data Protection Law, Law 1581. (October 17, 2012). See http://www.sic.gov.co/drupal/sites/default/files/normatividad/Ley_1581_2012.pdf.

31. As specified in the Habeas Data and Database Management Law, Law 1266. (December 31, 2008). See https://www.bancoldex.com/documentos/1291_Ley_1266_de_2008_(Habeas_Data).pdf.

32. Data Protection Law, art. 14.

In 2013, the government attempted to increase the checks on intelligence activities with the Intelligence and Counterintelligence Bill, which became Law 1621. The law created the Legal Commission for Monitoring the Activities of Intelligence and Counterintelligence, as well as an advisory committee for data and archive management.[33] However, these committees may only scrutinize documents provided by the agencies themselves, resulting in no direct supervision from independent organizations.[34] In addition, the intelligence bodies must submit an annual report to Congress. However, as in the case of Argentina, the entity being monitored determines which information to submit for review. Moreover, such checks have proved to be largely irrelevant as the Directorate of Criminal Investigation and Interpol (DIJIN)'s highly contested phone and Internet monitoring system, PUMA, was advanced in 2014, the same year that the government carried out the widely-publicized Andrómeda surveillance operation, which is further discussed below.

C. Mexico

Mexico's Constitution clearly enshrines the inviolability of private communications and further specifies that only designated federal authorities may employ surveillance methods, and then only with judicial authorization and under threat of criminal prosecution for noncompliance.[35] Yet the Law Against Organised Crime of 1996 expanded investigative and prosecutorial tools including electronic surveillance, undercover operations, and the prosecution for criminal association.[36] Although some criticized the law as a violation of the right to privacy or even a case of constitutionally-sanctioned espionage,[37] the text of the law does provide safeguards. Requests for communications interceptions, for example, must be made in writing to a district judge and must state the objective and necessity of the intervention as well as a detailed plan of investigation, including specific people, places, and type of communication to be intercepted and the duration of the operation.[38] The Mexican Supreme Court has further established the precedent that the phrase "private communications" in the Constitution

33. Intelligence and Counterintelligence Law, Law 1621, arts. 19–26. (April 17, 2013). See http://wsp.presidencia.gov.co/Normativa/Leyes/Documents/2013/LEY%201621%20DEL%2017%20DE%20ABRIL%20DE%202013.pdf.

34. Rivera & Rodriguez, above note 25, p. 29.

35. Constitution of the Mexican States of American. (1917; last revision December 20, 2010). Art. 16. See http://www.te.gob.mx/gobernadores/edomex/data/legisloc/constitucion.pdf.

36. Federal Law Against Organized Crime, arts. 15–28. (1996, Nov 7). See http://www.diputados.gob.mx/LeyesBiblio/pdf/101_070417.pdf.

37. See E. Gallegos, "Con la Reforma Anticrimen, el Espionaje Entrará a la Constitución," *La Jornada* (April 28, 1996). http://www.jornada.unam.mx/1996/04/28/LEY00-2704.html.

38. Federal Law Against Organized Crime, art. 16.

encompasses any extant technologies and those that may evolve in the future, including communications via the Internet.[39]

Mexico is a federation like the United States or Argentina, but until recently, there were separate and inconsistent penal codes for each of Mexico's 32 states. With the implementation of the Federal Penal Processing Code in 2014, the country's judicial proceedings were streamlined and made uniform nationwide.[40] In terms of communications surveillance, the Code designates the attorney general as the governmental authority that may carry out surveillance activities for the purpose of criminal proceedings. The Code also establishes penalties for those who misuse data obtained during the interception of private communications or conduct such interventions without authorization from the attorney general's office and a competent judge.[41] However, the Penal Procedural Code lists "the placement of tracking and surveillance devices" as a recognized security tool,[42] and Article 178 requires that any person "required by the Attorney General or competent authority [shall] collaborate or provide information to geo-locate communication devices in real time."[43]

This stipulation is based on the 2014 Federal Telecommunications and Broadcasting Law, which significantly increased the state's capacity to surveil private communications. Although the Telecommunications Law lists "the protection of personal data" as a user right,[44] Article 190 establishes an ample list of obligations for telecommunications service providers to comply with law enforcement activities. In addition to providing real-time location data upon request, the service provider must maintain a registry of communications made from any of its lines, identifying the following data: names, corporate name, and address of subscriber; types of communication or of services used; origins and destinations of communications; the date, hour, and length of the communications; and the activation and localizations tags, among others.[45]

39. Suprema Corte de Justicia de la Nación. Primera Sala. Amparo en Revisión 1621/2010 y Contradicción de Tesis 194/2012.

40. Mexican Penal Procedural Code, art. 211, § 1. (August 30, 1934). See http://www.diputados.gob.mx/LeyesBiblio/pdf/9_120315.pdf. Code updated and applied nationwide via DOF Decree, (March 5, 2014). See www.dof.gob.mx/nota_detalle.php?codigo=5334903&fecha=05/03/2014.

41. Ibid., art. 177.

42. Ibid., art. 24, §§ 15, 19.

43. "A la persona física o en su caso al representante de la persona moral que sea requerida por el Ministerio Público o por la autoridad competente para colaborar o aportar información para la localización geográfica, en tiempo real de los dispositivos de comunicación en términos de lo dispuesto por la Ley Federal de Telecomunicaciones y Radiodifusión . . ." Ibid., art. 178 bis.

44. Federal Telecommunications and Radiodiffusion Law, art. 191. (July 14, 2014). See http://www.dof.gob.mx/nota_detalle.php?codigo=5352323&fecha=14/07/2014.

45. Ibid., art. 190, § 2, A-G.

Despite the mandate for companies to collect and store massive quantities of personal information ex ante, the lengthy Article 190 concludes with a reiteration of the inviolability of private communications and the affirmation that only requests made by specific authorities will be honored, and only if they are authorized by a federal judge. Regardless, the mandatory retention of metadata opens the door for breaches or unlawful transfers of information. It also has a chilling effect on freedom of expression. Considering Mexico's current National Digital Strategy, which has the stated goal of incorporating "information communication technologies into every aspect of the everyday lives of people, organisations, and government,"[46] the potential for misuse becomes all the more critical.

D. Peru

Peru has a similarly solid legal base for personal data protection. In the 1993 Political Constitution, there are numerous provisions that pertain directly to data privacy. In addition to specifying the Freedom of Expression, Right to Privacy, and reputation protection,[47] the Peruvian Constitution explicitly specifies the Right to Communications Privacy in Section 10 of the Bill of Rights.[48]

The 2011 Personal Data Protection Law expanded upon these rights.[49] After giving a broad definition of data as any information on an individual that identifies him or makes him identifiable, the Law continues with a series of articles that directly require Legality, Consent, Purpose, Proportionality, Quality, Security, Recourse, and Protection in the interception, transfer, management, or processing of data. The law also includes a provision stating that these principles will be the guiding force in future decision-making.[50] Furthermore, the protocol for processing data requires authorization by a judge for data interception, and requires that any data obtained in violation of the Law be destroyed.[51]

46. National Digital Strategy del Gobierno de la República. (November 2013), p 7. See http://cdn.mexicodigital.gob.mx/EstrategiaDigital.pdf.

47. Political Constitution of Peru. (1993). Art. 2, § 4, 6, 7, respectively. See http://portal.jne.gob.pe/informacionlegal/Constitucin%20y%20Leyes1/CONSTITUCION%20POLITICA%20DEL%20PERU.pdf.

48. Ibid., art. 10: "Al secreto y a la inviolabilidad de sus comunicaciones y documentos privados. / Las comunicaciones, telecomunicaciones o sus instrumentos sólo pueden ser abiertos, incautados, interceptados o intervenidos por mandamiento motivado del juez, con las garantías previstas en la ley. Se guarda secreto de los asuntos ajenos al hecho que motiva su examen. / Los documentos privados obtenidos con violación de este precepto no tienen efecto legal. . . ."

49. Personal Data Protection Law, Law 29733. (July 3, 2011). See http://www.leyes.congreso.gob.pe/Documentos/Leyes/29733.pdf.

50. Ibid., arts. 4, 5, 6, 7, 8, 9, 10, 11, and 12, respectively.

51. Ibid., art. 38.

Similarly, the Protocol on the Interception and Recording of Communications, enacted in 2014, clearly plots the procedure for communications interception in seven stages, including an opportunity for control or reexamination at the request of the affected.[52] Permission for surveillance may be requested only by specific authorities (the criminal prosecutor, attorney general, or national prosecutor), must receive authorization from a federal judge, and may only be used in investigations concerning 15 serious crimes, which are specified within the text. Additionally, those under surveillance must be notified upon completion, and data that is outside the pre-specified scope of an approved investigation must be destroyed.

Despite the clarity of this communications interception regulation, the Legislative Decree 1182, or "Stalker Law," has been flagged by many as an unwarranted expansion of police power. The Decree states that service providers are immediately required to provide to authorities real-time location information about suspects of a serious crime, and no prior authorization from a judge or the prosecutor's office is necessary provided the information is vital to the investigation of a blatant crime for which the penalty would be more than four years in prison.[53] Although there is a liability regime in place for those who use the system maliciously, compliance with the limited requirements set out is assessed retroactively, and the system entirely removes the check of judicial authorization. Furthermore, the Decree requires all public telecommunications licensees (fixed and mobile) to retain data for 36 months minimum and up to three years in special storage systems that are easily accessible by authorities.[54]

Decree 1182 was passed in July 2015, months after the DINI (National Intelligence Directorate) was shut down after allegations of misconduct, but in September 2015 Bill 4809 was introduced to repeal it.[55] Bill 4809 maintains many of the articles from the Decree, but requires authorization by a criminal judge on duty in advance of, or within 24 hours after, requesting information from a service provider. It also restores the central role of the attorney general in investigations, as Decree 1182 refers to the police force in general.[56] As evident by the legislative volleying and coinciding closure of the Intelligence Directorate, Peru remains equally mired in conflict and scandal concerning surveillance operations, despite its comprehensive legal framework for communications interceptions.

52. Miguel Morachimo, "Vigilancia Estatal de las Comunicaciones y Derechos Fundamentales en Perú," EFF, Hiperderecho (Dec. 2015). See https://www.eff.org/country-reports/Peru-ES-final.

53. Legislative Decree 1182, art. 3. (July 27, 2015). See https://www.hiperderecho.org/wp-content/uploads/2015/07/DL_1182.pdf.

54. Ibid., "disposiciones complementarias finales," § 2.

55. Projected Law of Coordination for Use of Derived Data. (Rec. September 10, 2015). See http://www2.congreso.gob.pe/Sicr/TraDocEstProc/Contdoc03_2011.nsf/0/210d4d53cb946e-2b05257ebc0082aaa9/$FILE/PL0480920150910.pdf.

56. Ibid., art. 3.

IV. HUMAN RIGHTS PRINCIPLES

Massive governmental surveillance operations capitalizing on modern technologies are a phenomenon not limited to Latin America, and generally speaking legislation intended to regulate surveillance lags behind the pace of innovation in most countries. The protection of human rights and civil liberties in the digital realm is therefore an ever-evolving endeavor requiring participation and cooperation from states, the private sector, civil society, and beyond. Given the incomparable power that states maintain over safeguarding—or violating—the human rights of their citizens, regulating state surveillance and creating a precedent of rights protection online is critical.

To provide a more nuanced and updated understanding of how human rights should be protected online, several sets of principles have been adopted by groups of civil society actors, technical experts, and human rights specialists. Below, brief overviews of four of these sets of principles are included to indicate their general directions and, more important, to highlight the ways in which many of the aforementioned national laws are similar. The principles under review are: the Necessary and Proportionate Principles, the Tshwane Principles, the Manila Principles, and the OAS Juridical Committee Principles.

A. The Necessary and Proportionate Principles

The most directly applicable of the principles mentioned above are the International Principles on the Application of Human Rights to Communications Surveillance (2014), alternately referred to as the Necessary and Proportionate (NP) Principles.[57] The Principles include four key elements:

- Any limitations to privacy must be explicitly provided for by law.
- Communications interceptions must be necessary for a legitimate aim and must be undertaken only after the exhaustion of alternative, less intrusive courses of action.
- Interceptions must be proportional to their intended aim, and must never exceed their stated purposes.
- Checks and safeguards against surveillance abuse must be established, legally and systematically, to ensure the continued protection of human rights.

The NP Principles gained many signatories from organizations based in Argentina, Colombia, Mexico, and Peru.[58] Indeed, language employed in the Principles appears nearly verbatim in some legislation, such as Peru's 2011

57. International Principles on the Application of Human Rights to Communications Surveillance. "Necessary and Proportionate Principles." (2014). See https://necessaryandproportionate.org/principles.

58. In total: 9 organizations from Argentina, 9 from Colombia, 17 from Mexico, and 6 from Peru. See https://en.necessaryandproportionate.org/signatories.

Personal Data Protection Law. Overall, each of the countries in question has legislation specifying the processes for authorizing and carrying out surveillance, as well as criminal penalties for noncompliance or the misuse of personal data—all elements of a sound surveillance system called for in the NP Principles. Yet despite the specified processes for communications interceptions, illegal surveillance persists in criminal proceedings and intelligence gathering. Moreover, the patchwork of oversight mechanisms involving the judiciary and/or legislature is often crippled because the overseers obtain only official information from the bodies that they seek to monitor, and there are virtually no provisions for public or independent oversight.

B. The Tshwane Principles

The Tshwane Principles on National Security and the Right to Information (2013) acknowledge this deficiency, further recognizing that within police and intelligence departments "illegal, corrupt, and fraudulent conduct may occur and may not be uncovered, and violations of privacy and other individual rights often occur under the cloak of national security secrecy."[59] As evident in the aforementioned cases where surveillance is suspected, assumed, or even documented but rarely confirmed or curtailed, the public has very little knowledge about systems of surveillance and the procedures for authorizing them.[60] For example, although habeas data is an established right in Latin America and many countries have comprehensive databases so that citizens may seek information gathered about them, governmental operations are often hidden from such registries.

The Tshwane Principles acknowledge that some level of secrecy is expected in pursuing the legitimate end of national security. However, the Principles stress that burden of establishing the legitimacy of any restriction falls squarely on the state. They specify that citizens' access to information should be interpreted broadly and state restrictions narrowly.[61] Furthermore, information should be withheld on national security grounds for only as long as necessary to protect a legitimate national security interest, and no public authority, including the intelligence agencies, the armed forces, police, and other security agencies, should be exempt from disclosure requirements to the general public and for independent oversight.[62]

59. *The Global Principles on National Security and the Right to Information (Tshwane Principles)*, New York: Open Society Foundations (June 12, 2013) p. 9. See https://www.opensocietyfoundations.org/sites/default/files/global-principles-national-security-10232013.pdf.

60. Ibid., Principle 10e.

61. Ibid., Principle 4.

62. Ibid., Principle 16, 5, and 10c, respectively.

C. The Manila Principles

The Manila Principles on Intermediary Liability, released in 2015, advocate that technical intermediaries such as Internet Service Providers (ISPs), social networks, and search engines should be shielded from liability for the third-party content.[63] These principles, which also count numerous signatories from the countries surveyed here, mandate that requests to intermediaries for the disclosure of personally identifiable information be made only via an order by a judicial authority.[64] Although the Manila Principles focus mainly on content restrictions and freedom of expression, they state that intermediaries should not be required to ensure that they have the capacity to identify users.[65] This is highly relevant to the direct obligation on telecommunications companies to conserve personal information and metadata for government retrieval, clearly seen in Mexico and Peru.

D. The OAS Inter-American Juridical Committee Principles

Perhaps a bit less idealistic in nature, the Inter-American Juridical Committee (IAJC) of the Organisation of American States created a set of Principles for Privacy and Personal Data Protection in the Americas in 2012,[66] and a Legislative Guide on Privacy and the Protection of Personal Data in 2015.[67] According to the IAJC, the Principles:

> aim at encouraging Member States of the Organisation to adopt measures ensuring respect for people's privacy, reputations, and dignity. They were intended to provide the basis for Member States to consider formulating and adopting legislation to protect the personal information and privacy interests of individuals throughout our hemisphere.

The goal of the Guide is "to expand upon the Principles by giving additional context and guidance to Member States to assist in their preparation of national legislation."

63. *Manila Principles on Intermediary Liability*, Electronic Frontier Foundation (2015). See https://www.manilaprinciples.org/.

64. Ibid., Principle 5e.

65. Ibid., Principle 3d.

66. Inter-American Juridical Committee. (March 9, 2012). Statement of Principles for Privacy and Personal Data Protection in the Americas. 80th Regular Session. Mexico City: Organization of American States. See https://www.oas.org/en/sla/iajc/docs/ijc_current_agenda_privacy_personal_data_protection.pdf.

67. Inter-American Juridical Committee. (2015). Legislative Guide on Privacy and the Protection of Personal Data. 86th Regular Session. Rio de Janeiro: Organization of American States. See https://www.oas.org/en/sla/dil/docs/CJI-doc_474-15_rev2.pdf.

One key difference between this document and the NP Principles is its overt recognition of the exceptions and limitations to the public's right to access information about themselves, specifically in the case of criminal investigations.[68] Although the recommendations set forth in the Legislative Guide are often paired with a deference to extant national legislation, it is consistent with the NP and Tshwane documents in its assertion that communications interceptions must have a demonstrated necessity and legitimate ends and that only the citizenry, "physical people" as opposed to government operations, have an interest in privacy.[69]

V. CONCLUSIONS AND SUGGESTIONS

A. The Disparity between Law and Practice

Perhaps the best example of the disconnect between law and principles, on the one hand, and actual practice, on the other hand, comes from Colombia. Although the right to privacy is cemented in the Colombian Constitution,[70] illegal phone tappings are so common that there is a colloquial word for them—"chuzadas." In recent decades, communications surveillance has played a large part in the ongoing armed conflict between the Colombian government and the rebel group Fuerzas Armadas Revolucionarias de Colombia, or FARC. In 2007, after years of bugging complaints from political opponents and journalists, then-president Alvaro Uribe's Defence Minister acknowledged the existence of illegal wiretapping operations—although he claimed that the government had no knowledge of the information being procured.[71] As a result, 12 members of Congress were jailed on charges of colluding with paramilitaries.

Indeed, nearly every legislative initiative in Colombia addressing privacy or surveillance has been preceded by a scandal. In one sensational incident, news came to light in 2009 that the Administrative Department of Security (DAS, now defunct) had illegally surveilled and actively harassed public figures. In 2014, the widely-circulated newspaper *Semana* revealed that a Colombian army unit had spied on the government's negotiating team during peace talks with

68. Ibid., Principle 8.

69. Ibid., "Definitions."

70. The Constitution of Colombia. (1991). Art 15: "All individuals have the right to personal and family privacy and to their good reputation, and the State has to respect them and to make others respect them. Similarly, individuals have the right to know, update, and rectify information collected about them in data banks and in the records of public and private entities." See https://www.constituteproject.org/constitution/Colombia_2005.pdf.

71. D. Crowe, "Colombia Admits Wiretapping Operation," *The Washington Post* (May 15, 2007). See http://www.washingtonpost.com/wp-dyn/content/article/2007/05/15/AR2007051501696.html.

FARC in Havana, Cuba, during an operation code named Andrómeda.[72] Perhaps most strikingly, it is common knowledge that the attorney general's office, the Directorate of Criminal Investigation, and the Police Intelligence Directorate each has its own separate mass data interception system—all of which are illegal according to Colombian law.[73]

Although provisions intended to ensure the necessity and proportionality of communications interception, judicial oversight, and penalties for illegal surveillance are present in Colombian law, there are clearly many shortcomings in the legal framework. For example, there is no way for individuals to know if they have been surveilled by the government, and there are no channels for recourse in the event that human rights abuses are discovered. Transparency is virtually nonexistent, and oversight bodies only have access to information provided by the same entities they seek to monitor. Furthermore, the government's possession and employment of multiple illegal data interception systems clearly indicates that laws need to specify in greater detail the exact capabilities and limitations of law enforcement bodies.

Illegal surveillance by the government is so common that it's expected and assumed, which has produced a strong culture of self-censorship, or at least technological guardedness. Looking forward, Colombia's widespread surveillance is especially troubling considering the government's aggressive policies to increase Internet and telecommunications access across the country.[74]

The situation in Mexico is not so different: in 1998, reports revealed that the Mexican government had been electronically eavesdropping on political opposition members, journalists, and human rights activists for nearly a decade.[75] In addition to thousands of pages of transcripts from bugged telephone lines, investigations revealed hidden microphones and cameras in government offices and receipts for the purchase of $1.2 million in Israeli surveillance equipment. "Everything I say and do, I assume that I am being spied on," Vicente Fox, the Guanajuato governor who became president in 2000, told the *Washington Post* after learning that he was targeted in the operation.[76]

Peru had a similarly complicated experience with government surveillance throughout the 1990s. Until 2000, surveillance activities in Peru were conducted

72. "Chuzadas: Así fue la Historia," *Semana* (August 2, 2014). See http://www.semana.com/nacion/articulo/chuzadas-asi-fue-la-historia/376548-3.

73. The Attorney General's office runs Esperanza, the DIJIN has PUMA, and the DIPOL manages IRS.

74. D.M. Vega, "Colombia's Digital Agenda: Successes and Challenges Ahead," in *The Global Information Technology Report*, Beñat Bilbao-Osorio et al., eds. (New York: World Economic Forum, 2013). See http://www3.weforum.org/docs/GITR/2013/GITR_Chapter2.1_2013.pdf.

75. M. Moore, "Spy Network Stuns Mexicans," *The Washington Post* (April 13, 1998). See http://www.washingtonpost.com/archive/politics/1998/04/13/spy-network-stuns-mexicans/a0314a5a-c22a-4802-a23a-c93fabbd64bc/.

76. Ibid.

mainly by the Peruvian National Intelligence Service (SIN), which President Fujimori dissolved in 2000 amidst reports of bribes and other illegal activities. At present, Peru's non-military National Intelligence System (SINA) is controlled by the DINI, which reports directly to the executive. In February 2015, the DINI was closed for reorganization for 180 days following the release of evidence indicating that President Ollanta Humala had committed espionage against critical political figures using DINI's capacities.[77] Although SINA has a legislative check in place, the congressional oversight committee charged with monitoring the intelligence agency's activities has little autonomy and relies exclusively on information provided by SINA itself to make its assessments.

Finally, Argentina has also followed these patterns. The SIBIOS biometric face- and finger-scanning system mentioned above led Julian Assange to refer to Argentina as having "the most aggressive surveillance regime in all of Latin America."[78] In 2012, shortly after implementing this new system, the Argentine gendarmerie cast doubts on its treatment of sensitive personal data when reports revealed that the government had committed espionage against political, labor, and social leaders, collecting the amassed data in a digital database ominously labeled "Project X."[79] Only months later, Argentina's federal tax collection agency, AFIP, revealed the three pillars of their auditing strategy as: the maximum use of available technology, centralized data mining, and the employment of both operational and ex-ante inspection,[80] further casting doubt on the government's prudence in dealing with personal data.

To summarize—in Latin America, two commonalities can be identified among intelligence activities: first, partisan abuse of surveillance techniques to monitor the opposition; and second, habitual attempts of police and intelligence forces to increase autonomy and limit checks on authority.

B. Policy Suggestions

It is clear that legal surveillance measures may be necessary under some circumstances, and for that reason they will continue. However, if the parameters defining what is "legal" are insufficiently executed, law enforcement agencies will be tempted to continue illegal ongoing practices or worse—even if surveillance is carried out in many circumstances in good faith or for fair purposes. For this

77. M. Morachimo (December 2015). See https://www.eff.org/country-reports/Peru-ES-final.

78. Infobae América. (June 26, 2013). "Infobae: Entrevista a Julian Assange." YouTube. See https://www.youtube.com/watch?v=If7MbOvuEbg.

79. "La Gendarmería en el Banquillo," Página 12 (February 7, 2012). See http://www.pagina12.com.ar/diario/elpais/1-187784-2012-02-17.html.

80. "AFIP Refuerza el Control 'en Línea' de las Operaciones Económicas," AFIP Gacetilla de Prensa (August 15, 2012). See http://www.afip.gob.ar/novedades/docsComunicados/com3369.htm.

reason, policy suggestions should be pursued on two axes: first, to strengthen accountability mechanisms within existing and future legal frameworks; and second, to increase human rights protection against governmental (understood in the broad sense) surveillance.

In terms of accountability, the first step would be pushing the existing oversight bodies, such as congressional committees, to better fulfill their assigned functions. This might involve granting them additional tools for monitoring the agencies under their control, or it might require the creation of third-party, independent oversight groups. A level of public oversight would not only increase accountability, but also serve to better inform civil society and reduce the chilling effect produced by covert and obfuscated mass surveillance activities.

Concerning the protection of human rights, it is clear that surveillance—which, as has been previously established in this chapter, may be necessary to certain ends—affects personal rights to privacy, among others. However, under national and international standards, the main problem is not surveillance per se, but the threat posed by abusive or arbitrary surveillance measures. The burden of proving the necessity and proportionality of surveillance measures should rest squarely on the agencies conducting such activities. In all cases, respecting human rights should be a foremost concern, integrally incorporated into the design of legislation and oversight regimes, and never circumvented via loopholes or reactive legislation in the wake of tragedy. In other words, "human rights by design" should be the rule for policymaking in this field.

At present, terrorist attacks plotted and carried out by ISIS and other extremist groups have drawn the issue of communications surveillance to center stage. Although increased access to wide arrays of personal data and communications may seem like a worthy exchange in the wake of mass and senseless violence, policymakers must resist the impulse toward hardline, tough-on-terror legislation that could easily transcend exceptional circumstances and become a new norm. At this moment in particular, policymakers must avoid perpetuating a dystopian culture of fear and guardedness, and governments around the world must not sacrifice the values of accountability, transparency, and human rights protection in the name of national security.

17

Trust but Verify

The Importance of Oversight and Transparency in the Pursuit of Public Safety and National Security

SCOTT CHARNEY*

I. ABSTRACT

This chapter addresses the elements of an oversight or governance system that should be applied to any government program seeking broad access to personal data held by the private sector, and for industry to responsibly respond to such requests or demands. If by "broad access" we mean "access not tied to any specific account or person," our view is that such access is not acceptable, and it cannot be made acceptable through oversight or governance mechanisms. The issue of broad access received attention after the disclosures by Edward Snowden. News reports regarding US government surveillance practices highlighted several programs but, for the purpose of examining the issue of broad access, this chapter focuses on the 215 Program. This bulk collection program, so named because it was authorized under Section 215 of the PATRIOT Act, involved a secret court order that required phone companies to provide metadata to the government.

II. ANALYSIS

We have been asked to address, in practical terms, the elements of an oversight or governance system that should be applied to any government program seeking broad access to personal data held by the private sector, and for industry to responsibly respond to such requests or demands. If by "broad access" we mean "access not tied to any specific account or person," our view is that such access is not acceptable, and it cannot be made acceptable through oversight or governance mechanisms.

* The author would like to thank John Frank for his contributions.

Bulk Collection. Fred H. Cate and James X. Dempsey.

The issue of broad access received attention after the disclosures by Edward Snowden. News reports regarding US government surveillance practices highlighted several programs but, for the purpose of examining the issue of broad access, we will focus on the 215 Program. This bulk collection program, so named because it was authorized under Section 215 of the PATRIOT Act, involved a secret court order that required phone companies to provide metadata (time, duration, and phone numbers, as opposed to content) to the government.

Following the Snowden disclosures, it is clear that reasonable minds can differ on the propriety of broad access and the bulk collection of records. Although one can debate the merits of individual bulk collection programs, it helps to have an overarching framework to decompose such programs into their component parts and identify what, if anything, gives cause for concern. Such a framework would look as follows:

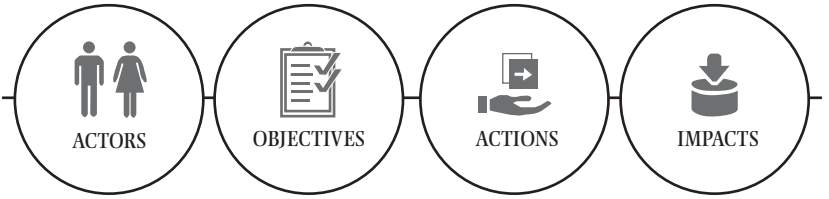

Figure 17.1 Impact Assessment Framework.

Before diving into the issue of broad access, it may be helpful to give an example of the framework in action, using a situation that is familiar to many: airport security. Over the past several years, there have been numerous attempts to improve the screening of passengers, particularly after law enforcement authorities interrupted assorted plots to blow up airplanes with liquid explosives or explosives hidden in shoes. In response to these events, a government actor (the US government), with the objective of protecting airplanes and their passengers, took the action of deploying backscatter X-ray scanners. The impact of this action included passenger exposure to radiation and graphic images of bodies. Notwithstanding government assertions that these machines were safe and appropriate, the public reaction suggested otherwise; that is, even if the right actor had the right objective, the actions taken produced unacceptable impacts. In response, the government moved to millimeter wave scanners (radio waves) and more opaque images. This change in action reduced the impacts of concern, and public opposition abated.

If we turn to the issue of broad access, the use of the framework highlights several concerns. The first element—the actor—is government. It is true that companies collect lots of data too, also raising privacy concerns.[1] This being true, it is fair to ask, "Are governments unique?" The answer is yes because (1) governments can compel the production of data, over the objections of the data holder

1. Microsoft is at the forefront of these discussions. See http://www.microsoft.com/en-us/twc/privacy/default.aspx.

and/or data subject; (2) governments can compel silence, by providing nondisclosure orders; and (3) methods of accountability differ. Although both governments and private parties can be castigated in the court of public opinion for their actions, private companies are accountable to government regulators and cannot avoid public scrutiny by saying their activities are "classified." Indeed, but for the disclosure of classified information by Edward Snowden, there would have been no public discussion on the propriety of the government-run program. Thus, the concern is that the power of the state—and the secrecy rules the state can leverage—are problematic when collecting data on people who have committed no crime or suspicious activity.

The second element relates to objective. Here the objective is to protect public safety and national security by combatting terrorism and, hopefully, preventing terrorist attacks. This is clearly a proper objective for governments. Some may be concerned that data collected for this purpose may be subject to secondary uses (i.e., used to achieve some other objective), with or even without appropriate authority. For that reason, there is prophylactic value in prohibiting collection in the first instance, as data never collected can neither be repurposed nor misused. But that does not change the fact that the objective of fighting terrorism remains valid.

The third and fourth elements—action and impacts—are closely related. As reflected in the example above on airport security, actors often have a range of options, and each of those options will have different impacts. In the scenario here, the "action" is the broad collection of data. The justification for such broad collection, according to the US government, is that "if you are looking for a needle, the haystack is relevant."[2] The problem with this argument is that it knows no bounds. Governments have always sought relevant evidence but relevancy, according to the dictionary, is defined as "connected with the matter at hand."[3] Prior to these broad collection programs, law enforcement agents would identify with specificity the person being investigated and/or the particular crime under investigation. An example might be "John Smith is planning to rob a bank" or "an unknown person is planning to bomb a subway in City X on June 3rd." In support of such an investigation, law enforcement agents would collect relevant evidence *specific to that person or crime*. But in an age where loosely affiliated individuals are constantly plotting unknown attacks, those responsible for protecting public safety decided it was appropriate to collect haystacks and search for needles.

One way to test this argument is to apply it in related contexts. For example, it has been written that a school shooter forecast his rampage three months

2. See Ellen Nakashima & Joby Warrick, "For NSA Chief, Terrorist Threat Drives Passion to 'Collect It All'," *Washington Post* (July 14, 2013), https://www.washingtonpost.com/world/national-security/for-nsa-chief-terrorist-threat-drives-passion-to-collect-it-all/2013/07/14/3d26ef80-ea49-11e2-a301-ea5a8116d211_story.html.

3. Merriam-Webster, "Relevant," (retrieved 2012), http://www.merriam-webster.com/dictionary/relevant.

before his attack.[4] One could argue that, to prevent the next school shooting, every diary in America should be collected, digitized, and stored so that this data store can be searched to prevent the next such attack. Of course, this is not possible: there are physical impracticalities (too many homes to search), as well as constitutional and legal prohibitions. But that misses the philosophical point. This is not just about the laws of physics and potential legal impediments; the deeper philosophical question is whether we should seize haystacks to create an ability to search for needles, knowing that most of that hay is lawful activity, engaged in by law-abiding citizens.

This is a particularly important question as new technologies and big data analytics change the way people can be profiled. As noted by the Supreme Court,

> GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations. See, *e.g., People* v. *Weaver*, 12 N. Y. 3d 433, 441–442, 909 N. E. 2d 1195, 1199 (2009) ("Disclosed in [GPS] data . . . will be trips the indisputably private nature of which takes little imagination to conjure: trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on").[5]

As in the case with X-ray machines at airports, an action may reveal "too much" and make people uncomfortable. This is often referred to as "the creepiness factor."

Our view that bulk collection is inappropriate is validated by recent congressional action, as Congress recently concluded that government agents can be effective without collecting haystacks.[6] That said, there are times when governments *should* be able to access data and, in fact, do so in secret. Microsoft believes—and there is no doubt our customers believe too—that people should be safe, both online and in the physical world. We should not create safe havens for criminals, and information, simply because it is digitized, should not be off limits to those responsible for preventing, investigating, and prosecuting crime. Even for specific, tailored access, however, governance models are important.

In this regard, it is important to appreciate that different types of investigations are subject to different levels of oversight, as "one size does not fit all" when it comes to governance models. For example, when surveillance is conducted for

4. Jordan Steffen, Zahira Torres & Jennifer Brown, "Report: Arapahoe High School Shooter Wrote in Diary of Coming Rampage," *Denver Post* (April 26, 2016), http://www.denverpost.com/news/ci_26702161/final-details-arapahoe-high-school-shooting-be-revealed.

5. *United States v. Jones*, 132 S. Ct. 945 (2012) (Sotomayer, J., concurring).

6. See USA Freedom Act, Public Law No. 114-23 (eliminating bulk collection of US phone records), https://www.congress.gov/114/plaws/publ23/PLAW-114publ23.pdf.

criminal investigative purposes, there is judicial supervision, followed by notification to the target when the investigation is complete[7] and, sometimes, production of that evidence in public court proceedings. This individualized notice is supplemented by broader public reports concerning the use of wiretapping as an investigative tool, and those reports are made public.[8] This is not to suggest that "after-the-fact" oversight is a substitution for "before-the-fact" relevancy requirements, but rigorous oversight is one way to ensure that rules have in fact been followed and to build trust in governance processes.

By contrast, when surveillance is conducted for intelligence purposes (e.g., to monitor a foreign spy operating on US soil), the goal may not be the bringing of public charges in open court, and notice to an intercepted party might never be appropriate. As such, there is no required notice to the parties intercepted unless evidence collected pursuant to a Foreign Intelligence Surveillance Act order is being offered in court.[9] Additionally, the reporting requirements require reporting to Congress (not the Administrative Office of US Courts), and the reports can be redacted to protect national security.[10]

Although these situations do vary and governance models need to be tailored appropriately, from the discussion above we can glean several important principles. First, there should be no broad or unfettered access; the requests should be specific. Second, the process for accessing data should include appropriate oversight, which means an appropriate segregation of duties (e.g., having courts approve legal requests for such access). Third, there should be transparency so that legislators and the public know the general scope of such surveillance activities. Indeed, a lawsuit filed by information technology companies led to just such transparency, as companies were granted the right to describe, in broad terms, the number of orders it receives, including those related to national security.[11]

Although there is no doubt that government access to data cannot always be completely transparent, having specific requests, oversight by an independent judiciary, and transparency to regulators and the public will permit governments to protect public safety and national security while deflating concerns that the government is acting in ways that may chill fundamental rights, including rights of freedom of association and freedom of expression. In sum, it will ensure that the right parties pursue the right objectives with the right actions and impacts.

Finally, in a globally connected world, it is important to think about the international implications of surveillance programs. The fact is, surveillance laws

7. 18 U.S.C. § 2518(8)(d) (2012). There are exceptions to this rule.

8. See 18 U.S.C. § 2519 (2012); http://www.uscourts.gov/statistics-reports/analysis-reports/wiretap-reports.

9. 50 U.S.C. § 1806(c) (2012).

10. 50 U.S.C. § 1871(d) (2012).

11. See http://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/.

often differentiate between citizens and foreigners, as well as between domestic and international surveillance. These distinctions are premised on the fact that a government's primary mission is to protect its own citizens' public safety and national security. But the Snowden disclosures certainly made clear that spying on allies can create tensions in important relationships, as well as undermine trust in information technology.[12] Unaddressed concerns about the security of the supply chain and communications networks can reduce the benefits offered by global innovation and connectivity.

This is not to suggest governments abdicate their responsibility to protect national security. But as the recent German SPD Report on oversight and regulation of signals intelligence makes clear, there are no international standards on intelligence collection that permit even friendly states to have a common code of conduct.[13] To the extent that citizens of one country may be concerned about surveillance by governments other than their own, creating international standards, at least between like-minded countries, might increase trust in surveillance programs, especially if those standards would prohibit, as the SPD would, "a ban on the creation of an NSA-style data haystack."[14]

12. See Simon Shuster, "German Mistrust of the U.S. Deepens amid Latest Spy Scandals," *Time* (July 7, 2014), http://time.com/2963472/spy-scandals-damage-us-german-alliance/; Claire Cain Miller, "Revelations of N.S.A. Spying Cost U.S. Tech Companies," *New York Times* (March 21, 2014), http://www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html?_r=0.

13. SPD Report, p. 8.

14. SPD Report, p. 3.

18

Regulating Foreign Surveillance through International Law

ASHLEY S. DEEKS*

I. ABSTRACT

Regulating how governments conduct *foreign* electronic surveillance against another state's citizens poses a complex challenge. In the wake of Edward Snowden's leaks in 2013, the extent to which governments conduct surveillance of foreign state leaders and citizens became strikingly clear. And the extent to which the subjects of that surveillance are discontent with the status quo also became apparent. This chapter argues that, although states traditionally have been loath to regulate their intelligence activities using international law, that body of law offers an important avenue by which states can reduce criticisms stemming from human rights and other groups, help set the agenda for the future of foreign surveillance, and respond to foreign and domestic fears that government surveillance is unconstrained. The chapter describes the variety of pressures states face to modulate their foreign surveillance, explains some of the benefits that states may accrue by doing so, and suggests six procedural norms around which certain Western democracies may be able to coalesce.

II. INTRODUCTION

Regulating how governments conduct electronic surveillance against their own citizens and in their own territory is a potent challenge, in view of the scope and speed of technological developments and the evolving nature of security threats. Regulating how governments conduct *foreign* electronic surveillance against another state's citizens poses an even more complex challenge—but a

* The arguments in this chapter are drawn from Ashley S. Deeks, "An International Legal Framework for Surveillance," 55 *Virginia Journal of International Law* 291 (2015).

Bulk Collection. Fred H. Cate and James X. Dempsey.

critical one.[1] In the wake of Edward Snowden's leaks in 2013, the extent to which governments—especially the United States but also states such as the United Kingdom, Germany, Australia, France, and Sweden—conduct surveillance of foreign state leaders and citizens became strikingly clear. And the extent to which the subjects of that surveillance are discontent with the status quo also became apparent.

This chapter argues that, although states traditionally have been loath to regulate their intelligence activities using international law, that body of law offers an important avenue by which states can reduce criticisms stemming from human rights and other groups, help set the agenda for the future of foreign surveillance, and respond to foreign and domestic fears that government surveillance is unconstrained. The chapter describes the variety of pressures states face to modulate their foreign surveillance, explains some of the benefits that states may accrue by doing so, and suggests six procedural norms around which certain Western democracies may be able to coalesce.

III. PRESSURES TO REGULATE

At least until recently, states have treated their spying activities as existing in an uneasy but stable relationship with international law. Most states and scholars seem to share the view that international law neither authorizes nor condemns spying by one state on another—or on the other's citizens. Some even believe that international law affirmatively permits spying. This group usually points to the widespread and long-standing practice of spying in support of the claim that international law does not purport to regulate this type of activity. Before the Snowden leaks, there was little pressure on states to revisit this approach.

A smaller group of actors criticizes spying as a violation of international law. Until recently, this was a minority view, but this approach has garnered some traction as ordinary citizens begin to realize the extent to which foreign states are able to monitor and collect their data. These actors argue that foreign surveillance implicates—and often runs afoul of—areas of international law such as human rights (and especially the right to privacy), diplomatic law, and customary rules about the sovereignty and territorial integrity of states. It remains unclear the extent to which states actually crafted these rules to reach surveillance, but some actors seek to "repurpose" these existing rules for today's foreign surveillance.

These demands on (Western, democratic) states to regulate their overseas surveillance come from disparate quarters, and arise against a contemporary backdrop characterized by three important conditions. First, many individuals

1. By "foreign surveillance," this chapter means to capture peacetime surveillance by one state of the communications of another state's officials or citizens who are located outside the surveilling state's territory, using electronic means such as Internet and cell phone monitoring or satellites. This type of surveillance currently faces the least amount of regulation in international law and in states' domestic laws.

around the globe have developed a personal understanding and concern about how foreign government surveillance affects them, because the government techniques involve accumulating large volumes of data of "ordinary" people. Second, the interests of corporations, foreign leaders, citizens, and elite opinion in the United States and Europe are aligning in a pro-regulation direction. Third, the very governments whose activities were most exposed by the documents revealed by Snowden are governments that are sensitive to public and elite pressures.

Specific examples of pressure to curtail foreign surveillance abound in political, economic, and rights-based forms. Once US surveillance policies came to light, for instance, the United States faced significant political pressure from the leaders of Germany, Brazil, and France to cease spying on their cell phones. (As a result of this pressure, the United States tightened its policies about when it would monitor the communications of heads of state of friendly governments.) In the economic sphere, US corporations such as Google, Facebook, and Microsoft fear the perception that they are facilitating NSA surveillance and worry about losing business abroad. As a result, they have pressured the US government to reduce the breadth of its foreign intelligence-gathering. Third, activities in the United Nations, the International Court of Justice, domestic European courts, and the European Court of Human Rights reflect efforts (by foreign states, nongovernmental organizations, and individuals) to more aggressively protect the right to privacy. Some of these rights-based pressures may produce legal changes, as when a court rules against a government's surveillance program. Other rights pressures may be less direct but persist over time, as actors urge states to adopt a more expansive definition of what the right to privacy of communications entails.

In short, new pressures on states to roll back some aspects of foreign surveillance abound. But given that states rarely have resorted to international law to collectively constrain their intelligence activities, why might some set of states wish to do so here? First and most obviously, they may agree to do so if the pressures just discussed continue to strengthen. That is, states may decide that it is worth adopting new norms to satisfy their domestic constituents. Second, each state presumably would prefer a world in which its officials and citizens were subject to less foreign surveillance, but the only way to achieve that is to establish agreed rules of cooperation among like-minded and trustworthy states. Third, the absence of agreed norms of foreign surveillance may force certain states to reduce their intelligence sharing with other states that they perceive to be acting in troubling ways. Establishing harmonious interpretations of joint international legal obligations could help sustain intelligence cooperation and data sharing.

IV. SIX NORMS

The first part of this chapter illustrated why the international landscape seems poised for change. If conditions and incentives stimulate states to develop international norms of foreign surveillance, what might those norms look like? The

best and most realistic place from which to draw inspiration is existing domestic surveillance laws. Many Western states have put in place domestic laws regulating how their governments may conduct surveillance of their own citizens (either at home or abroad) and how those governments may conduct surveillance of foreign actors who are communicating with those citizens. These laws have been tested in practice, have been developed in the crucible of public debates, and are, for the most part, publicly accessible. Although very few states currently regulate purely extraterritorial surveillance, the communications of some foreign nationals receive some incidental protections (particularly when the foreign actors are communicating with a state's nationals). There is little reason, therefore, not to accord those types of protections to all foreign nationals. Further, states are more likely to achieve inter-state agreement by focusing on procedural norms, rather than trying to achieve consensus about the substance of privacy rights.

I extracted the following six proposed norms from common principles found in the domestic laws of the United States, the United Kingdom, Australia, Canada, and Germany. Although not representative of all states' surveillance laws, these states have some of the most extensive laws regulating surveillance. That suggests that these states have paid careful attention to how to appropriately balance privacy and national security, how to monitor and counterbalance the government's surveillance power, and how to internally protect data once they collect it. In proffering these principles, the hope is that the norms will increase the accountability of state officials engaged in surveillance, reduce (though not eliminate) the disparity in treatment between citizens and foreigners, limit the ability of government actors to act in overly discretionary ways, and advance the transparency of the rules being applied.

The six principles that states should adopt are: (1) notice to the public of the applicable rules, (2) limits on the reasons that states may collect or query data, (3) a requirement for periodic reviews of surveillance authorizations, (4) limits on the length of time for which the state may hold the data, (5) a preference for action by the host state intelligence services (rather than foreign intelligence services) wherever reasonable, and (6) the existence of a neutral body that will authorize surveillance ex ante or review it ex post.

The first principle is one of legality. People should know how their own state and foreign states are empowered or constrained in conducting foreign surveillance. This includes knowledge about who may be subject to surveillance, which agencies are conducting the surveillance, and the use to which the collected communications may be put. It does not mean that in any particular case a person has the right to know whether the state is monitoring his activities. But adopting this principle would improve the status quo, under which most individuals do not know whether states generally are engaged in foreign surveillance and under what rules.

The second principle is that states should limit the reasons they collect or query data. Most of the five states examined currently have collection limits or use limits, though the content of those limits differs. The United States, for instance, may use the bulk metadata it has collected only to detect and counter espionage

and other activities directed by foreign powers against US interests, terrorist threats, proliferation of weapons of mass destruction, cyber threats, threats to US or allied forces, and transnational criminal threats. Germany may conduct strategic, warrantless surveillance of telephonic and Internet communications to avert the risk of an armed attack on Germany, the commission of international terrorist acts with a direct relation to Germany, international weapons or drug trafficking, or certain cases of counterfeiting and money laundering. These offer examples of types of collection limits that states might agree to adopt. States also could agree to take certain types of data or uses of data off the table, such as attorney-client communications or the sharing by states of intelligence about foreign businesses with their domestic companies.

Third, states should require that at least one government actor periodically reconsider an authorized surveillance activity. This would ensure that a state actor considers at fixed intervals whether continued surveillance is appropriate and thus would avoid indefinite surveillance of a target.

Fourth, states should agree to limit the length of time they may retain collected data—perhaps to a year or 18 months. Intelligence officials have acknowledged that older data is less important. This norm therefore should not pose a significant operational challenge, but would offer an important check on intentional or accidental abuse or release of swaths of collected information.

Fifth, states should adopt a preference for surveillance by the state in which the suspicious activities are taking place. Assuming that the territorial state has the capacity to conduct surveillance and a positive relationship with the state seeking the information, collection by the territorial state is likely to be more rights-protective because domestic laws regulating surveillance tend to be more restrictive when a state is collecting on its own soil.

Finally, states should agree to a norm that requires neutral oversight—ex ante, ex post, or both—of the executive's conduct of foreign surveillance. The laws of each state I examined provide at least one, and often multiple, forms of oversight. Those oversight bodies include courts, parliamentary committees, and inspectors general. States might even accept a norm that allows foreign nationals to submit allegations of unlawful surveillance to an adjudicatory body, though this is somewhat less common.

Creating international law takes time. One route is via a negotiated multilateral treaty, but it is unlikely that states engaged in the most extensive surveillance (including the United States, United Kingdom, China, and Russia) would be able to reach agreement on appropriate rules for foreign surveillance. It seems more likely that states will develop international norms as a matter of customary practice. The actual formation of customary international law is slow and requires widespread and consistent state practice followed out of a sense of legal obligation. In the shorter term, states could signal their support for these types of surveillance-related norms in several ways. A core group of Western states might make a public commitment to a set of foreign surveillance principles, including through the use of a political memorandum of understanding. Or they might issue parallel unilateral declarations that a certain set of norms

reflects internationally acceptable behavior. For now, the form is less important than the fact of a meeting of the minds among high-profile states engaged in foreign surveillance.

A final caveat: not all states will be attracted to these norms. One can sort states into three basic categories regarding surveillance regulation: Western and other democratic states; technologically powerful non-democracies or quasi-democracies, such as China and Russia; and states that lack robust surveillance capabilities. States in the third category have good reasons to push for extensive regulations because they will bear limited costs and obtain benefits for themselves and their nationals if such regulations are adopted. States in the second category seem unlikely to adopt new norms because they face little internal or external pressure to do so. States in the first category have stronger incentives to adopt international surveillance norms, but also have more at stake than states in the third category. Indeed, it seems likely that Western democracies will form the core group of states to consider these norms. States such as South Korea, Japan, and Israel might also seek to participate in developing these principles. And any state that adopts this set of international norms presumably would only apply those norms to the citizens of other states that have, correspondingly, adopted the norms themselves.

V. CONCLUSION

The approach set forth in this chapter attempts to navigate between two shoals: a deeply cynical approach to foreign surveillance—which submits that states will never agree to modify their foreign spying—and an excessively optimistic approach that believes that states soon will be able to arrive at a shared interpretation of robust privacy protections. One might think of this chapter's approach as an intermediate step that preserves the possibility of a future substantive consensus about the essence of privacy rights, but provides certain nearer-term protections to the many private actors exposed to foreign electronic surveillance. Government programs that seek and obtain broad access to personal data of a large number of foreign citizens should embrace the six procedural constraints detailed herein: doing so would alleviate the sense that states are engaged in unfettered foreign surveillance, while imposing costs that states realistically can bear.

19

Preventing the Police State

International Human Rights Laws Concerning Systematic Government Access to Communications Held or Transmitted by the Private Sector

SARAH ST.VINCENT*

> *The maintenance of . . . dossiers about citizens who have never been charged with any violation of law and who have no means of refuting misinformation that may have been collected concerning them is an invitation to abuses of the gravest sort. Secret dossiers are paraphernalia of a police state. They are not proper instruments of a democratic government . . .*
>
> *It does not matter that these invasions of what were once deemed inalienable rights have been adopted for the sake of national security . . . Dictatorship always has its origin in the assumption that men supposed to be benevolent may be entrusted with arbitrary authority.*
>
> Alan Barth, *critiquing the United States government's Employees Loyalty Program, 1951*[1]

* I am grateful to James X. Dempsey for inviting me to contribute a chapter to this volume and to Lara Ballard, Tamir Israel, Maria McFarland Sánchez-Moreno, Dinah PoKempner, Amie Stepanovich, Amos Toh, and Cynthia Wong for reviewing the draft. The views expressed herein are my own and do not necessarily reflect those of Human Rights Watch or the individuals acknowledged above.

Sections of this chapter closely track, and at times draw directly from, a brief guide I created in the early days of my acquaintance with the subject as a fellow at the Center for Democracy & Technology: Sarah St.Vincent, *International Law and Secret Surveillance: Binding Restrictions upon State Monitoring of Telephone and Internet Activity*, (September 4, 2014), https://cdt.org/files/2014/09/CDT-IL-surveillance.pdf.

1. Alan Barth, *The Loyalty of Free Men* (1951), pp. 129–30 (quoted in Jay Feldman, *Manufacturing Hysteria: A History of Scapegoating, Surveillance, and Secrecy in Modern America* (2011), p. 197).

> *Powers of secret surveillance of citizens, characterising as they do the police state, are tolerable under the Convention only in so far as strictly necessary for safeguarding the democratic institutions.*
>
> *European Court of Human Rights*[2]

I. ABSTRACT

This chapter is intended as a basic reference guide for lawyers, legislators, and advocates approaching the issue of mass surveillance—or surveillance more generally—through the lens of international human rights law for the first time. It focuses on the International Covenant on Civil and Political Rights and the human rights treaties that apply in Europe and the Americas, with a particular emphasis on the rights to privacy, freedom of expression and opinion, and an effective remedy for violations. Although the exact parameters of the right to privacy are still being decided, it appears increasingly clear that state interferences with any kind of communications data will generally be subject to a standard of strict necessity applied on an individualized basis, and there is presently a trend toward finding that mass surveillance—including systematic state access to data held or transmitted by the private sector—violates the human rights treaties.

II. INTRODUCTION

In an era when fears of deadly public violence are running high in many parts of the world, some political leaders have made little secret of their belief that one crucial means of preventing destruction and disorder is the state's systematic access to individuals' communications and related data—colloquially, mass surveillance.[3] However, despite the apparent enthusiasm for these practices in a number of powerful states, international human rights laws and jurisprudence currently suggest that this type of activity is permissible only in a vanishingly

2. *Klass and others v. Germany*, Application no. 5029/71, Judgment (Plenary) (September 6, 1978) ¶ 42. The same or similar language appears in, for example, *Rotaru v. Romania*, Application no. 28341/95, Judgment (Grand Chamber)(May 4, 2000), ¶ 47; *Segerstedt-Wiberg and others v. Sweden*, Application no. 62332/00, Judgment (June 6, 2006), ¶ 88; *Szabó and Vissy v. Hungary*, Application no. 37138/14, Judgment (January 12, 2016), ¶ 54.

3. See, for example, Theresa May, *Oral Statement to Parliament: Publication of Draft Investigatory Powers Bill* (November 4, 2015), https://www.gov.uk/government/speeches/home-secretary-publication-of-draft-investigatory-powers-bill (asserting that the state requires the powers to intercept communications and acquire communications data in bulk

small set of circumstances, if at all. Moreover, the case law and commentary appear to be evolving toward a conclusion that state interferences with private communications and/or related data on a systematic and indefinite basis will always violate the human rights treaties in the absence of a valid derogation[4] from those instruments.

The discussion below is intended as a basic reference guide for lawyers, legislators, and advocates who are approaching the issue of mass surveillance—or surveillance more generally—through the lens of international human rights law for the first time. It focuses on the International Covenant on Civil and Political Rights (ICCPR) and the human rights treaties that apply in Europe and the Americas, as the regional courts in those parts of the globe have been the most active in addressing surveillance-related matters. The chapter's concern is with legal rather than policy considerations, and it adopts a relatively formalist approach, treating the various human rights instruments (and the jurisprudence of the regional courts) as strictly binding only upon the relevant states parties, although otherwise constituting persuasive authority. Similarly, it treats the views of the UN treaty bodies and Special Rapporteurs as persuasive but not conclusive. Additionally, it assumes that a state's treaty obligations are binding

in order to address terrorism and other crimes); "Tony Abbott National Security Statement to Parliament," *Sydney Morning Herald* (September 22, 2014), http://www.smh.com.au/federal-politics/political-news/tony-abbott-national-security-statement-to-parliament-20140922-10kccx.html (depicting data-retention mandates as necessary to countering terrorism).

Although "mass surveillance" remains an informal term rather than a legal one at the international level, this chapter uses it as shorthand for state interferences with communications and related data to which privacy rights attach under the applicable treaties, where those interferences are or may be carried out on a large scale without being based on an individualized suspicion of wrongdoing. As there is broad agreement among the human rights courts and experts mentioned herein that the retention of data constitutes an interference with the right to privacy (see below), this chapter treats blanket data-retention mandates—that is, obligations on Internet or telecommunications companies to retain certain data describing communications, such as the dates, times, senders, and recipients of emails—as one form of mass surveillance. Others include, for example, the indiscriminate and large-scale interception of the content of communications.

4. A derogation is a state's temporary suspension of one or more of its commitments under a treaty. The human rights instruments typically provide that states are only permitted to derogate from their obligations under those instruments during an emergency so severe that it poses a threat to "the life of the nation." See, for example, International Covenant on Civil and Political Rights, 999 U.N.T.S. 171 (1966), art. 4 (hereinafter ICCPR); Convention for the Protection of Human Rights and Fundamental Freedoms, E.T.S. 5 (1950), art. 15 (also known as the European Convention on Human Rights; hereinafter ECHR); American Convention on Human Rights, 1144 U.N.T.S. 123 (1969), art. 27 (hereinafter ACHR).

upon that state's agents regardless of the purpose of the activity in question (e.g., "intelligence" or "law enforcement").[5]

In the interest of brevity, this analysis does not address the question of whether a state's obligations under any of the human rights treaties apply extraterritorially.[6] It also does not address the human-rights-related responsibilities of the private-sector entities that transmit or store communications, although this is an important area of inquiry.[7]

Section III below examines the right to privacy as it applies to government efforts to acquire or monitor indiscriminately, or order the systematic retention of, Internet or telephone communications (and/or related data) that individuals have generated or transmitted using the services of corporate entities. Section IV examines the right to freedom of expression and opinion in this context, and also touches briefly upon the rights to freedom of thought, conscience, and religion; freedom of association; and freedom of assembly. Section V discusses the right to a remedy for violations of the foregoing rights as well as the right to freedom from discrimination in the enjoyment of these rights.

At the time of writing, several major cases concerning the application of human rights laws to mass surveillance remained pending before the European regional courts. The European Court of Human Rights (ECtHR), which is a Council of Europe[8] institution and adjudicates claims that a state has violated

5. See, for example, Office of the United Nations High Commissioner for Human Rights, *The Right to Privacy in the Digital Age,* U.N. Doc. A/HRC/27/37 (June 30, 2014) (hereinafter OHCHR report), and G. Alex Sinha, "NSA Surveillance since 9/11 and the Human Right to Privacy," 59 *Loy. L. Rev.* 861 (2013), both of which assume that the ICCPR applies to state intelligence activities. For a presentation of other views, see Ashley S. Deeks, "Confronting and Adapting: Intelligence Agencies and International Law," 102 *Va. L. Rev.* 599 (2016).

6. For a treatment of this issue, see, among many others, Harold Hongju Koh, *Memorandum Opinion on the Geographic Scope of the International Covenant on Civil and Political Rights*, (October 19, 2010), https://www.documentcloud.org/documents/1053853-state-department-iccpr-memo.html; Sinha, above note 5, pp. 900–03; Ashley Deeks, "An International Legal Framework for Surveillance," 55 *Va. J. Int'l L.* 291, 307–12 (2015).

7. See, for example, Human Rights Council, *Report of the Special Rapporteur on the Right to Privacy, Joseph A. Cannataci,* U.N. Doc. A/HRC/31/64 (March 8, 2016), ¶ 9; Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, U.N. Doc. A/HRC/32/38 (May 11, 2016), ¶¶ 56–62. See also Office of the United Nations High Commissioner for Human Rights, *Guiding Principles on Business and Human Rights* (2011), http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf.

8. The Council of Europe is a regional body with 47 Member States; its purpose is to "promote democracy and protect human rights and the rule of law in Europe." Council of Europe, *Do Not Get Confused*, http://www.coe.int/en/web/about-us/do-not-get-confused (last visited April 29, 2017). The European Union is a separate economic and political entity to which 28 Member States belonged at the time of writing; its goals include promoting peace, establishing an internal market, and ensuring the free movement of persons among the Member States. European Union, *The EU in Brief*, https://europa.eu/european-union/about-eu/eu-in-brief_en

its obligations under the European Convention on Human Rights (ECHR), was considering three challenges to the United Kingdom's surveillance practices.[9] Readers are advised to consult the judgments in these cases when they become available, as they are likely to include landmark findings. Additionally, just as this chapter was being finalized, the Court of Justice of the European Union (CJEU)—which, inter alia, answers questions that the domestic courts of the EU Member States refer to it regarding how they should interpret and apply EU law—handed down its judgment in the joined cases of *Tele2 Sverige AB* and *Watson and others*, which concern the legality of state data-retention mandates.[10]

III. THE RIGHT TO PRIVATE LIFE AND CORRESPONDENCE

As the discussion below demonstrates, privacy rights are a common thread that runs through the human rights instruments addressed in this chapter—a fact that serves as a powerful reminder that these rights are indeed rights and not mere considerations to be bartered away easily in the name of state security. Where government monitoring of communications is concerned, the gravity with which the international human rights bodies view any prospective intrusions on these rights is perhaps best captured by the early statement of the UN Human Rights Committee (HRC)—the body charged with monitoring states' implementation of the ICCPR—in its General Comment on the right to privacy that communications surveillance in any form "should be prohibited."[11] Although the regional human rights courts have adopted a more qualified position (and even the HRC itself no longer appears to take such an absolutist stance),[12] it is clear that the

(last visited April 29, 2017); Consolidated version of the Treaty on European Union, 2010 O.J. C 83/01, art. 2.

9. *Big Brother Watch and others v. the United Kingdom*, Application no. 58170/13 (communicated January 7, 2014); *Bureau of Investigative Journalism and Ross v. the United Kingdom*, Application no. 62322/14 (communicated January 5, 2015); and *10 Human Rights Organisations v. the United Kingdom*, Application no. 24960/15 (communicated November 24, 2015).

10. *Tele2 Sverige AB v. Post- och telestyrelsen* (Case C-203/15) and *Secretary of State for the Home Department v. Watson and others* (Case C-698/15), Judgment of the Court (Grand Chamber) of 21 December 2016, http://curia.europa.eu/juris/liste.jsf?num=C-203/15.

11. United Nations Human Rights Committee, *General Comment No. 16: Article 17 (Right to privacy)* (April 8, 1988), ¶ 8. Regrettably, this currently remains the HRC's only General Comment on the right to privacy, despite the enormous changes that have occurred in communications technology since the time of its publication.

12. See, for example, Human Rights Committee, *Concluding Observations on the Sixth Periodic Report of New Zealand*, U.N. Doc. CCPR/C/NZL/CO/6 (April 28, 2016), ¶ 16 (referring to the need for adequate judicial safeguards where the "interception of communications and metadata collection, processing and sharing" are concerned, without suggesting that those practices *per se* constitute violations of the Covenant); Human Rights Committee, *Concluding Observations on the Initial Report of South Africa*, U.N. Doc. CCPR/C/ZAF/CO/1

right to privacy reflects a core set of concerns about human dignity and the position of the individual vis-à-vis the state. Thus, as the Inter-American Court of Human Rights (IACtHR) has stated, the evolution of technology in recent years does not mean that individuals should now necessarily find themselves in "a situation of vulnerability" where the possibility of government monitoring of communications is concerned: instead, "the State must increase its commitment to adapt the traditional forms of protecting the right to privacy to current times."[13]

Although the exact parameters of the right remain the subject of ongoing debate before the human rights courts and treaty bodies, a number of aspects of state privacy obligations as they apply in the digital age appear to be crystallizing (although further confirmation remains necessary). One is that virtually any type of data the user of modern communications technology may generate will fall within the scope of the privacy rights found in the treaties; another is that state interferences with this data will generally be subject to a standard of strict necessity applied on an individualized basis. For these and other reasons, there is presently a trend toward finding that mass surveillance—including systematic state access to data held or transmitted by the private sector—violates the treaties.

The focus of the discussion below is on large-scale monitoring; however, the same treaty laws and norms will apply to any state interference with privacy rights.

A. The Nature of the Privacy Right(s) Articulated in the Human Rights Instruments

Although analyses of human rights law often begin with the Universal Declaration of Human Rights (UDHR), that document was in fact preceded by the American Declaration of the Rights and Duties of Man (American Declaration), a text the Inter-American Commission on Human Rights (IACHR) views as binding upon the members of the Organisation of American States even though it is not a treaty as such.[14] (Thus, as far as the IACHR is concerned, the American

(April 27, 2016), ¶ 43 (similarly, referring to a need to "ensure that interception of communications by law enforcement and security services is carried out only according to the law and under judicial supervision" without suggesting that the Covenant prohibits all surveillance).

13. *Escher et al. v. Brazil*, Judgment, July 6, 2009, ¶ 115.

14. Universal Declaration of Human Rights, U.N. Doc A/810 (1948) (hereinafter UDHR); American Declaration of the Rights and Duties of Man (1948) (hereinafter American Declaration). As per articles 34 *et seq.* of the ACHR, above note 4, the IACHR is a body charged with promoting and defending human rights, including by receiving and examining complaints that a state party to the Convention has violated its obligations under that instrument. In conformity with a process set out in the Convention, the Commission may then submit a case to the IACtHR; see ACHR, art. 61. The IACHR has found that the American Declaration is binding upon the members of the Organization of American States in Res. no. 3/87, Case 9647, Roach and Pinkerton (United States), September 22, 1987, ¶ 48.

Declaration places binding obligations upon the United States of America—a state whose surveillance practices have been the subject of particular scrutiny since former National Security Agency contractor Edward Snowden disclosed a cache of classified documents in 2013.)[15] Meanwhile, scholarly opinions regarding the precise legal status of the UDHR vary, although at least some of the document's provisions are or may be expressive of customary international law (i.e., norms that states so commonly follow in practice, and that are supported by such a significant body of legal opinion, that they have become binding even upon those states that have not formally committed to them).[16] In any event, both declarations show that privacy rights are a foundational concern at the international level: the American Declaration announces that "[e]very person has the right to the protection of the law against abusive attacks upon . . . his private and family life" as well as to "the inviolability and transmission of his correspondence," whereas the UDHR states that no one may be "subjected to arbitrary interference with his privacy, family, home or correspondence" and that "[e]veryone has the right to the protection of the law against such interference."[17]

In the years following their finalization, these two declarations gave rise to several human rights treaties that also contain rights to privacy. The ICCPR, an instrument open to signature by virtually any state, establishes such a right at Article 17 in terms nearly identical to those of the UDHR, save for the addition of "or unlawful" following "arbitrary."[18] The American Convention on Human Rights (ACHR), which members of the Organisation of American States may join, broadly echoes these provisions in mandating that "[n]o one may be the object of arbitrary or abusive interference with his private life, his family, his home, or his correspondence" and that individuals must enjoy the protection of the law in this regard; it also includes a right to the recognition of one's "dignity" as part of the same article.[19]

15. See ibid., at ¶¶ 47–48; for a brief summary of some of the Snowden revelations, see Sinha, above note 5, pp. 892–99. The United States disagrees with the IACHR's conclusion that the American Declaration is binding upon it; see Christina M. Cerna, "Reflections on the Normative Status of the American Declaration of the Rights and Duties of Man Anniversary Contributions—International Human Rights," 30 *J. Int'l L.* 1211, 1220 (2009).

16. See, for example, Hurst Hannum, "The Status of the Universal Declaration of Human Rights in International Law," 25 *Ga. J. Int'l & Comp. L.* 287, 289 (1995); Jochen von Bernstorff, "The Changing Fortunes of the Universal Declaration of Human Rights: Genesis and Symbolic Dimensions of the Turn to Rights in International Law," 19 *Eur. J. Int'l L.* 903, 913 (2008). On the nature of customary international law, see *North Sea Continental Shelf Cases (Federal Republic of Germany v. Denmark; Federal Republic of Germany v. Netherlands)*, Judgment, 1969 I.C.J. 72, ¶ 38.

17. American Declaration, above note 14, arts. 5 and 10; UDHR, above note 14, art. 12.

18. ICCPR, above note 5, arts. 17 and 48(1).

19. ACHR, above note 4, arts. 11 and 74(1); references to "dignity" also appear in articles 5 and 6 of the instrument.

Meanwhile, in Europe, the ECHR and the Charter of Fundamental Rights of the European Union (EU Charter) both include privacy rights.[20] The ECHR contains the most detailed provision on the right to privacy among all the instruments mentioned herein, establishing first that "[e]veryone has the right to respect for his private and family life, his home and his correspondence," and subsequently that a public authority cannot engage in any

> interference . . . with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.[21]

Among the 28 EU Member States, the EU Charter also requires that an individual must enjoy a "right to respect for his or her private and family life, home and communications" and adds an explicit "right to the protection of personal data."[22] The Charter demands that any limitation the state wishes to place upon these rights be "provided for by law," "respect the essence" of the rights, be "necessary," and "genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others."[23]

As a general matter, the treaty texts quoted above all require the same basic inquiry to determine whether a state has committed a violation of the right to privacy:

(1) Does the right apply to the information or behavior in question?
(2) Did the state's action interfere with the right?
(3) Was this interference done in accordance with the law?
(4) Was the interference necessary (or, to the extent that there may be a genuine difference in meaning between the terms, "non-arbitrary" or "non-abusive")?[24]

20. ECHR, above note 4, art. 8; Charter of Fundamental Rights of the European Union, 2000/C 364/01, arts. 7–8 (hereinafter EU Charter).

21. ECHR, above note 4, art. 8.

22. EU Charter, above note 20, arts. 7–8. As this chapter is only intended to provide a brief introduction to some of the major human rights instruments that apply to communications surveillance, it does not address "data protection" laws aside from Article 8 of the Charter. However, readers may wish to be aware of the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, E.T.S. No. 108 (1981); for an introduction to that instrument, see Electronic Privacy Information Center, *Council of Europe Privacy Convention,* https://epic.org/privacy/intl/coeconvention/ (last visited April 29, 2017).

23. EU Charter, above note 20, art. 52(1).

24. Cf. Jordan J. Paust, "Can You Hear Me Now?: Private Communication, National Security, and the Human Rights Disconnect," 15 *Chi. J. Int'l L.* 612, 627 (2015).

B. The Scope of the Right to Privacy and the Occurrence of an Interference

In the relevant case law and commentary, the questions of whether a particular type of data falls within the scope of the right to privacy and whether the state has interfered with that right are sometimes conflated.[25] However, in light of current debates about the sensitivity of various categories of data and whether it may be more acceptable for the state to have systematic access to some types rather than others, it is useful to begin by identifying those that international courts and Special Rapporteurs have specifically described as protected by the right, as well as state behaviors these entities have found to constitute an interference.

1. The Scope of the Right

As then-UN Special Rapporteur on the right of freedom of opinion and expression Frank La Rue has pointed out, the texts of the human rights treaties are largely silent about which types of data may fall within the ambit of the right to privacy, aside from "correspondence" (which is mentioned in the ICCPR, ACHR, and ECHR; the EU Charter refers to "communications").[26] The UN HRC's lone General Comment on the right to privacy, adopted in 1988, fails to clarify matters, mentioning only communications and "personal information" of the kind that may be susceptible to storage in electronic form.[27] Moreover, as La Rue also highlights, the evolution of information technology in recent decades has "irreversibly affected our understandings of the boundaries between private and public spheres," meaning that the question of whether a certain type of information—such as a statement on a social media website—falls within the scope of the right will often be a contested one.[28]

La Rue's commentary can be read to suggest that the ICCPR right to privacy applies very broadly where data is concerned, attaching to any form of communication between individuals that is intended to take place without intervention or observation by others, as well as to information that other parties hold concerning an individual.[29] The jurisprudence of the regional courts, as well as recent recommendations of the UN HRC and the IACHR, indicate that the privacy rights found in the treaties attach to telephone and electronic communications, with the jurisprudence suggesting that location data and biometric data such as fingerprints and

25. See, for example, *Uzun v. Germany*, Application no. 35623/05, Judgment, September 2, 2010, ¶¶ 43 *et seq*.

26. Human Rights Council, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue*, U.N. Doc. A/HRC/23/40 (April 17, 2013), ¶ 21 (hereinafter La Rue report).

27. *General Comment No. 16*, above note 11, ¶¶ 8 and 10.

28. La Rue report, above note 26.

29. Ibid., at ¶¶ 22–23.

DNA are covered as well.[30] According to the ECtHR, the right may also attach to at least some extent where an individual interacts with others "in a public context," especially where a "systematic or permanent record" of this interaction is created.[31] This latter finding suggests that the right may apply, for example, to an individual's posts on social media websites even where a casual observer might characterize those posts as "public."

Although policymakers and scholars continue to debate the sensitivity of metadata (that is, data that describes a communication, such as the date, time, sender, and recipient of an email message),[32] by now there is little question at the international level that the treaty rights to privacy attach to such data. The ECtHR and IACtHR have both explicitly concluded that telephone metadata, such as the number a caller has dialed, is subject to the protection of the right; the ECtHR has also extended this reasoning to "e-mail and Internet usage," and although the IACtHR has not yet addressed the matter of Internet-based communications, there is no reason to believe it would decline to follow the ECtHR's lead.[33] The CJEU has also concluded that the imposition of a blanket requirement that communications service providers retain certain types of metadata and subscriber data, as well as the authorities' ability to gain access to such data, implicate the EU Charter rights to private life and the protection of personal data; according to the Court, this is true regardless of whether the metadata in question is "sensitive."[34] Similarly, the Office of the UN High Commissioner for

30. See, for example, *Copland v. the United Kingdom*, Application no. 62617/00, Judgment, April 3, 2007; Uzun, above note 25; *S. and Marper v. the United Kingdom*, Application no. 30562/04, Judgment (Grand Chamber), December 4, 2008*; Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources et al*., Case C-293/12, Judgment, April 8, 2014; *Escher*, above note 13, ¶ 114; Human Rights Committee, *Concluding Observations on the Fourth Periodic Report of the United States of America,* U.N. Doc. CCPR/C/USA/CO/4 (April 23, 2014), ¶ 22; Inter-American Commission on Human Rights, *Report on the Situation of Human Rights Defenders in the Americas* (2006), p. 84 (recommendation 13). Although this chapter focuses on communications surveillance, biometric data is often of interest to activists in this area and is therefore mentioned briefly here. The list of types of data found in this sentence should not by any means be understood as exhaustive where the forms of "personal data" to which treaty privacy rights can attach are concerned.

31. *P.G. and J.H. v. the United Kingdom*, Application no. 44787/98, Judgment, September 25, 2001, ¶¶ 56–60; *Shimovolos v. Russia*, Application no. 30194/09, Judgment, June 21, 2011, ¶ 65.

32. See Electronic Frontier Foundation and Article 19, *Background and Supporting International Legal Analysis for the International Principles on the Application of Human Rights to Communications Surveillance* (May 2014), pp. 10–14, https://necessaryandproportionate.org/files/2016/03/29/background_and_supporting_legal_analysis_en.pdf.

33. *Escher*, above note 13, ¶ 114*; Malone v. the United Kingdom*, Application no. 8691/79, Judgment (Plenary), August 2, 1984, ¶¶ 83–84; *Copland*, above note 30, ¶¶ 43–44.

34. *Digital Rights Ireland*, above note 30, ¶¶ 29–34; see also *Schrems v. Data Protection Commissioner*, Case C-362/14, Judgment(October 6, 2015), ¶ 87.

Human Rights (OHCHR), the body within the UN Secretariat that takes the lead on promoting and protecting human rights, has affirmed that the ICCPR right to privacy attaches to metadata, and the HRC has implied its agreement in recommendations to several states.[35]

Thus, it does not appear that the international courts or bodies are in any way inclined to adopt what in the United States is known as the "third-party doctrine": that is, the presumption that individuals do not have an expectation of privacy in their metadata, as they have voluntarily conveyed this information to the provider of the communications service.[36] Indeed, the OHCHR has pointedly questioned the notion that consumers make such a "conscious compromise" when using modern communications technologies.[37] Particularly in the era of "big data," the High Commissioner's assertion that consumers may not in fact be "truly aware of what data they are sharing, how and with whom, and to what use [the data] will be put" is a compelling one.[38]

2. Establishing an Interference

After determining that a particular type of data is protected by the right to privacy, the next step is to inquire whether the government action at issue interferes with that right. Since its seminal 1978 judgment in *Klass and others v. Germany*, the ECtHR has maintained that even the "mere existence" of legislation permitting secret surveillance measures constitutes an interference.[39] (Although the Court's Grand Chamber finessed this finding to some extent in 2015 in its combined analyses of victim status and the existence of an interference in *Zakharov v. Russia*, its overall approach appears to remain effectively intact at least insofar as legislation may allow mass surveillance, although further discussion by the Court will be necessary to clarify this point.)[40] Additionally, the Court has previously found that the acquisition, retention, use, and dissemination of communications or other personal information all

35. OHCHR report, above note 5, ¶¶ 19–20; Human Rights Committee, above note 12 (New Zealand); Human Rights Committee, above note 32 (United States); Human Rights Committee, *Concluding Observations on the Seventh Periodic Report of the United Kingdom of Great Britain and Northern Ireland*, U.N. Doc. CCPR/C/GBR/CO/7 (August 17, 2015), ¶ 24.

36. See *Smith v. Maryland*, 442 U.S. 735 (1979); see also Electronic Frontier Foundation and Article 19, above note 32, pp. 11–13.

37. OHCHR report, above note 5, ¶ 18.

38. Ibid.

39. *Klass and others*, above note 2, ¶ 41; *Weber and Saravia v. Germany*, Application no. 54934/00, Decision, June 29, 2006, ¶ 78; *Liberty and others v. the United Kingdom*, Application no. 58243/00, Judgment, July 1, 2008, ¶ 56.

40. *Zakharov v. Russia*, Application no. 47143/06, Judgment (Grand Chamber), December 4, 2015, ¶¶ 171–179.

constitute interferences (with acquisition or retention amounting to interferences even without subsequent use), and the IACtHR has reached similar results.[41] The CJEU, for its part, has indicated that an interference with the relevant EU Charter rights may occur even where the individual concerned does not suffer any adverse consequences, and it has further established that data-retention mandates interfere with these rights.[42]

Where the UN bodies are concerned, the HRC's 1988 General Comment on the right to privacy states flatly that "[c]orrespondence should be delivered to the addressee without interception and without being opened or otherwise read."[43] Drawing upon this conclusion (although evidently taking a more qualified position), the OHCHR, like the ECtHR, maintains that "even the mere possibility of communications information being captured creates an interference with privacy."[44] La Rue's 2013 report on state surveillance implies that interception, data-retention mandates, access to stored content or metadata, location tracking, social media monitoring, the invasion of private devices through hacking, and the individualized or mass monitoring of Internet browsing should all be considered interferences with the ICCPR right, although La Rue likely did not intend for this list to be exclusive.[45] Regarding mass surveillance specifically, the current UN Special Rapporteur on human rights and counterterrorism, Ben Emmerson, has provided a detailed list of some of the means by which states today may gain "bulk access" to metadata and/or content that the private sector holds, concluding that such activities "amount[] to a systematic interference" with the right to privacy as found in the Covenant.[46]

Thus, as far as the international and regional human rights institutions are concerned, there appears to be little doubt that when a state's acquisition of or access to private-sector data—including metadata—is systematic, this practice constitutes an interference with the privacy rights established in the treaties.

41. *Amann v. Switzerland*, Application no. 27798/95, Judgment (Grand Chamber), February 16, 2000, ¶ 45; *Weber and Saravia*, above note 39, ¶ 79; *Rotaru*, above note 2, ¶ 46; *Leander v. Sweden*, Application no. 9248/81, Judgment, March 26, 1987, ¶ 48; *S. and Marper*, above note 30, ¶ 67 (confirming that the storage of data concerning private life constitutes an interference even in the absence of use); *Escher*, above note 13, ¶ 118.

42. *Digital Rights Ireland*, above note 30, ¶¶ 33–36; *Schrems*, above note 34.

43. *General Comment No. 16*, above note 11, ¶ 8.

44. OHCHR report, above note 5, ¶ 20.

45. La Rue report, above note 26, ¶¶ 34 *et seq.*

46. United Nations General Assembly, *Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism*, U.N. Doc. A/69/397 (September 23, 2014), ¶¶ 8–9 (hereinafter Emmerson report).

C. The Lawfulness of the Interference

1. Elements of the Requirement

Once a complainant at the international level has established that a state activity has interfered with his or her right to privacy, he or she will need to demonstrate that the interference was unlawful.

The HRC's General Comment on the right to privacy interprets the legality requirement found in the relevant article of the ICCPR as meaning that "no interference [with the right] can take place except in cases envisaged by the law"—specifically, the state's own legislation, "which itself must comply with the provisions, aims and objectives of the Covenant."[47] In other words, the state entity concerned must stay within the bounds of domestic law, and that law must in turn be consistent with the treaty. The OHCHR has elaborated on this interpretation by stating (in language echoing that of the ECtHR jurisprudence described below) that "the law must be sufficiently accessible, clear and precise" that an individual may, by reading it, "ascertain who is authorised to conduct data surveillance and under what circumstances."[48] Regarding the ICCPR's textually separate requirement that individuals must enjoy "the protection of the law" where this right is concerned, the OHCHR has further stated (again drawing upon ECtHR case law) that

> [t]he State must ensure that any interference with the right to privacy, family, home or correspondence is authorised by laws that (a) are publicly accessible; (b) contain provisions that ensure that collection of, access to and use of communications data are tailored to specific legitimate aims; (c) are sufficiently precise, specifying in detail the precise circumstances in which any such interference may be permitted, the procedures for authorising, the categories of persons who may be placed under surveillance, the limits on the duration of surveillance, and procedures for the use and storage of the data collected; and (d) provide for effective safeguards against abuse.[49]

Additionally, citing HRC observations concerning the United States, the OHCHR emphasizes that "secret" rules and legal interpretations—that is, those that are not made available to the public—lack "the necessary qualities of 'law' " for the purposes of the legality requirement.[50]

The ECtHR's jurisprudence is even more specific on this point insofar as the legal basis for state surveillance activities is concerned. According to the Court,

47. *General Comment No. 16*, above note 11, ¶¶ 2–3.

48. OHCHR report, above note 5, ¶ 23.

49. Ibid. at ¶ 28; see also Human Rights Committee, above note 30 (United States) and note 35 (United Kingdom).

50. OHCHR report, above note 5, ¶ 29, citing Human Rights Committee, above note 30 (United States).

surveillance measures must have a "basis in domestic law" and must further adhere to public international law as well as "the rule of law" more generally.[51] The domestic law in question must be binding (that is, not simply a statement of policy) as well as "sufficiently clear in its terms to give citizens an adequate indication as to the circumstances" in which the surveillance might take place—meaning, inter alia, that at least the following elements must be set out by statute:

(1) the type and scope of the measures;
(2) limits on how long the measures may last;
(3) the grounds on which the authorities may order the measures;
(4) which authorities are entitled to authorize, oversee, or carry out the measures;
(5) the requisite procedures for "examining, using and storing" the data, as well as the scheme for ultimately destroying it;
(6) the safeguards that apply to the sharing of the data with other entities; and
(7) the remedies available for violations of these strictures.[52]

The IACtHR agrees that "the general conditions and circumstances" under which a state may conduct surveillance must be set out in "a law in the formal and substantial sense," and that this law must provide "clear and detailed rules, such as the circumstances in which this measure can be adopted, the persons authorised to request it, to order it and to carry it out, and the procedure to be followed."[53]

Additionally, the ECtHR and OHCHR concur that, in the High Commissioner's words, "laws or rules that give the executive authorities, such as security and intelligence services, excessive discretion" to conduct surveillance will not be sufficient to meet the legality requirement.[54]

When determining whether state surveillance measures are "done in accordance with the law," the ECtHR has also grappled with the difficult question of whether individuals whose communications have been monitored are entitled to be notified of that fact. In its analysis of the matter in the early case of *Klass and others*, the Court adopted a position that was deferential to the state, accepting that "[s]ubsequent notification to each individual affected by a suspended measure might well jeopardise the long-term purpose that originally prompted the surveillance," and concluding that a state's decision not to provide notification,

51. See St.Vincent, above at *, p. 10, and sources cited therein; *Kennedy v. the United Kingdom*, Application no. 26839/05, Judgment, May 18, 2010, ¶ 151; *Zakharov*, above note 40, ¶ 228.

52. St.Vincent, above at *, p. 10, and sources cited therein; *Malone*, above note 33, ¶ 67; *Zakharov*, above note 40, ¶ 231.

53. *Escher*, above note 13, ¶ 131 (internal citation omitted); cf. *Donoso v. Panamá*, Judgment, January 27, 2009, ¶ 77.

54. OHCHR report, above note 5, ¶ 29; *Zakharov*, above note 40, ¶ 230; *Amann*, above note 41, ¶ 56 (quoting *Malone*, above note 33, ¶¶ 67–68).

even after the fact, "cannot itself be incompatible" with the ECHR.[55] However, one reason the Court was willing to take this view was that the applicable German law in fact required the government to provide notification to monitored persons "as soon as notification [could] be made without jeopardising the purpose" of the surveillance.[56] In more recent judgments, the Court has shifted toward stating that domestic law "should" contain this type of post hoc notification requirement and finding violations of the Convention where states have failed to provide for notification under any circumstances.[57] The Court's choice of the term "should" instead of "must" is likely due to its conclusion in *Kennedy v. the United Kingdom* that the respondent state complied with the Convention by providing a tribunal that could examine allegations of unlawful government surveillance even where the complainant had not received notification of any monitoring—that is, where an individual's standing was not dependent upon his or her possession of evidence that surveillance had in fact taken place.[58] It is to be hoped that other human rights courts and bodies will address these key issues of notice and standing in the near future.[59]

In any event, several aspects of the jurisprudence and commentary described above weigh against the notion that systematic government interferences with private-sector data may be "lawful" for the purposes of the human rights treaties. First, a number of the elements that the ECtHR and IACtHR have identified as necessary for any surveillance statute—namely, the enumeration of grounds upon which the authorities may order the surveillance and the potential scope and duration of the measures—along with the notification requirement (to the extent that it applies under the relevant treaty) would essentially be moot if state authorities were entitled to interfere with data concerning anyone at any time.[60]

2. Authorization and Oversight

In addition to complying with domestic law (which must itself meet the criteria described above), state surveillance measures must be subject to adequate

55. *Klass and others*, above note 2, ¶ 58.

56. Ibid.; see also *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, Application no. 62540/00, Judgment, June 28, 2007, ¶ 90 (depicting this fact as a key element of the Court's willingness to reach its holding in *Klass and others*) (hereinafter "Association for European Integration").

57. *Szabó and Vissy*, above note 2, ¶¶ 86–87; *Association for European Integration*, above note 56.

58. *Kennedy*, above note 51, ¶ 167.

59. See OHCHR report, above note 5, ¶ 40 (stating that notice and standing are "critical issues in determining access to effective [*sic*] remedy").

60. See *FDN et al. c/ Gouvernement, Conseil d'État*, Contentious Section, Third-Party Intervention: Center for Democracy & Technology and Privacy International, undated, ¶¶ 32–34, https://cdt.org/files/2016/02/LQN-case_FINAL-2_CLEAN.pdf.

authorization and oversight regimes. As indicated above, it is arguable that systematic government access to private-sector data necessarily violates other elements of the legality requirement—a defect that even an exceptionally strong oversight system would not cure. Speaking generally, however, the UN General Assembly has called upon states to "establish or maintain existing independent, effective, adequately resourced and impartial judicial, administrative and/or parliamentary domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception and the collection of personal data."[61]

Regarding the initial authorization of communications surveillance measures, the ECtHR has indicated that although authorization does not necessarily need to be judicial in order for the process to conform to the Convention, the entity responsible for granting the authorization must be independent of the entities carrying out the monitoring.[62] Any nonjudicial authorizing body should, in turn, ultimately be subject to some form of judicial control, as supervision by a judge provides "the best guarantees of independence, impartiality and a proper procedure."[63] Perhaps due to a reluctance to overturn its holding on this point in *Klass and others*, in which it approved of the nonjudicial German oversight scheme, the Court has stopped short of insisting upon judicial review as such (if only post hoc) in all circumstances.[64] However, it has warned that oversight of surveillance measures by "a judge with special expertise[] should be the rule and substitutions the exception, warranting close scrutiny"—thus arguably limiting *Klass and others* to its facts and rendering judicial supervision at some stage *de rigeur* for all or nearly all other systems.[65] Future judgments will show whether the Court indeed intends to take such an approach. Meanwhile, although the IACtHR has ruled on the compliance of a particular judicial authorization system with the ACHR, it has not yet addressed the requisite nature of surveillance authorization or oversight systems in general.[66]

While the regional human rights courts continue to wrestle with the form that surveillance decision-making bodies must take, the HRC has indicated that regardless of who precisely is responsible for authorizing these types of measures, the authorization must be done on a case-by-case basis.[67] The Committee has yet to

61. United Nations General Assembly, *The right to privacy in the digital age*, U.N. Doc. A/RES/69/166 (December 18, 2014), ¶ 4(d).

62. *Klass and others*, above note 2, ¶ 56; cf. *Kennedy*, above note 51, ¶¶ 166–167. The Court's Grand Chamber recently reiterated this point in *Zakharov*, above note 40, ¶¶ 275 *et seq.*

63. *Szabó and Vissy*, above note 2, ¶ 77.

64. Ibid.; *Klass and others*, above note 2.

65. *Szabó and Vissy*, above note 2, ¶ 77.

66. *Escher*, above note 13, ¶¶ 132 *et seq.*

67. *General Comment No. 16*, above note 11, ¶ 8.

clarify precisely what it means by "case-by-case"; however, there appears to be little reason to question Emmerson's interpretation, which is that the scrutiny must be individualized.[68] As Emmerson points out, this requirement—insofar as it is indeed a requirement under the applicable treaties—effectively forecloses the possibility that a mass surveillance program could comply with the right to privacy.[69]

D. The Necessity or Non-arbitrariness of the Interference

The texts of the human rights instruments vary in their descriptions of the qualities a lawful interference with privacy rights must possess in order to avoid the state's excessive use of what are, after all, capabilities that create an immense differential between the government and the governed. At present, none of the human rights courts or bodies appear to question the notion that states are entitled to monitor communications and related data in at least some circumstances; however, they have demonstrated a deep concern with determining, and thus limiting, exactly what those circumstances are.

Both the ICCPR and ACHR require that interferences with privacy must not be "arbitrary," whereas the ECHR opts for "necessary in a democratic society in the interest of" certain specified aims, and the EU Charter (as noted above) states that limitations on the right must be proportionate as well as "necessary" and "genuinely meet[ing] objectives of general interest recognised by the Union."[70] Meanwhile, the HRC's General Comment 31, which concerns the overall nature of the legal obligations the ICCPR imposes, maintains that any restriction a state places on a Covenant right must be necessary as well as "proportionate to the pursuance of legitimate aims."[71] Likewise, the IACtHR has construed the ACHR as mandating that any state interference with the right to privacy must "serve a legitimate purpose[] and meet the requirements of suitability, necessity, and proportionality which render it necessary in a democratic society."[72] Thus, although the language of the treaty provisions concerning restrictions on the right to privacy are not identical, and although some scholars view them as differing in substance,[73] there is every indication that the texts, jurisprudence, and analyses by UN experts are gradually converging around a standard that could be described as "necessary and proportionate to the pursuit of a legitimate aim."[74] As the

68. Emmerson report, above note 46, ¶ 51.

69. Ibid., at ¶¶ 18, 51–52.

70. Above notes 18–23.

71. Human Rights Committee, *General Comment No. 31: The Nature of the General Legal Obligation Imposed on States Parties to the Covenant*, U.N. Doc. CCPR/C/21/Rev.1/Add.13 (May 26, 2004), ¶ 6.

72. Donoso, above note 53, ¶ 56.

73. For example, Sinha, above note 5, pp. 905–08.

74. Cf. *International Principles on the Application of Human Rights to Communications Surveillance* (2014), https://necessaryandproportionate.org/principles; OHCHR report, above

human rights courts and bodies rarely have difficulty in determining that a state surveillance measure pursues a legitimate aim such as preventing serious crime, this discussion will focus on the concepts of necessity and proportionality.[75]

Although these two concepts are unquestionably related, the proper distinction between the two (and, for that matter, whether they are distinguishable at all) has not yet been clearly or consistently articulated by the relevant international bodies. Helpfully, the opinion of the Advocate General in *Tele2 Sverige AB* and *Watson and others* has set forth the concept of "proportionality *stricto sensu*," suggesting that even surveillance that is "necessary" to achieve a legitimate aim can still be disproportionate in the sense of being beyond the bounds of what is tolerable in a democratic society.[76] Such a theory might indicate, for example, that even if the constant video surveillance of a classroom is regarded as "necessary" to ensure students' safety at every moment, such a measure may nevertheless be disproportionate in the sense that the harms to fundamental rights outweigh the advantages to society.[77]

In any case, regarding the necessity requirement, ECtHR jurisprudence appears to be evolving toward a conclusion that mass surveillance cannot be compliant with this criterion. The Court has long maintained that the term "necessary," as employed in the relevant ECHR provision, means "strictly necessary for safeguarding the democratic institutions."[78] Prior to 2015, its findings concerning potentially large-scale surveillance programs were admittedly unclear at best. In *Klass and others*, for example, the Court found that a state surveillance regime did not violate the Convention right to privacy even though the authorities had broad powers to monitor postal and telephone communications; however, the text of the judgment suggests that legal restrictions on these powers made interferences targeted rather than systematic.[79] In its later admissibility decision in *Weber and Saravia*, the Court accepted the necessity of a program in which the use of "catchwords" during satellite telephone conversations triggered surveillance of those conversations; yet, the use of satellite telephones was relatively unusual at the time, and the Court's treatment of the precise nature

note 5, ¶¶ 23–27; Human Rights Committee, *Concluding Observations on the Fifth Periodic Report of France*, U.N. Doc. CCPR/C/FRA/CO/5, August 17, 2015, ¶ 12.

75. See, for example, *Digital Rights Ireland*, above note 30, ¶¶ 41–44; *Zakharov*, above note 40, ¶ 237; *Kennedy*, above note 51, ¶ 155.

76. *Tele2 Sverige AB v. Post- och telestyrelsen (Case C-203/15) and Secretary of State for the Home Department v. Watson and others (Case C-698/15),* Opinion of Advocate General Øe, July 19, 2016, ¶¶ 247–248.

77. See ibid. for this balancing test. At the time of writing, the compliance of constant video surveillance of a classroom with Article 8 of the ECHR was at issue in the communicated ECtHR case of *Antović and Mirković v. Montenegro*, Application no. 70838/13 (communicated December 3, 2014).

78. Above note 2.

79. *Klass and others*, above note 2, ¶ 17.

and scope of the interference is brief and opaque.[80] Muddying the waters even further, the Court's Grand Chamber found just two years later in *S. and Marper v. the United Kingdom* that the "blanket and indiscriminate" retention of DNA samples and fingerprints by English and Welsh authorities—a practice arguably analogous to mass surveillance—was an unnecessary and disproportionate interference with privacy rights.[81]

With the Grand Chamber's judgment in *Zakharov*, however, the Court seems to have sent a clear signal that mass communication surveillance programs do not comply with the Convention.[82] The Fourth Section's subsequent judgment in *Szabó and Vissy v. Hungary* further found that the requirement of strict necessity has two mandatory elements: a state surveillance measure must not only be strictly necessary for safeguarding the democratic institutions (as indicated above) but must also be "strictly necessary, as a particular consideration, for the obtaining of vital intelligence in an individual operation."[83] The latter criterion, with its references to "vital intelligence" and "individual operation," suggests—as the author has argued elsewhere[84]—that the Court means to indicate that surveillance regimes entailing systematic state access to private data necessarily violate the Convention. In this respect, it seems highly significant that the Court indicated in *Szabó and Vissy* that it would not have ruled in favor of the respondent government in *Kennedy v. the United Kingdom* if the monitoring in that case had involved "indiscriminate capturing of vast amounts of communications."[85]

The CJEU appeared to reach a similar conclusion in *Digital Rights Ireland*, invalidating EU Directive 2006/24 (popularly known as the Data Retention Directive) in part because that legislation required, within the scope of its application, the retention of data concerning all persons in all locations at all times for at least six months and up to two years.[86] Additionally, in its judgment in

80. See Center for Democracy & Technology and Privacy International, above note 62, ¶ 36.

81. *S. and Marper*, above note 32, ¶¶ 125–126; see also Center for Democracy & Technology and Privacy International, above note 62, ¶ 38.

82. *Zakharov*, above note 40.

83. Szabó and Vissy, above note 2, ¶ 73.

84. Sarah St.Vincent, *Did the European Court of Human Rights Just Outlaw 'Massive Monitoring of Communications' in Europe?* (January 13, 2016), https://cdt.org/blog/did-the-european-court-of-human-rights-just-outlaw-massive-monitoring-of-communications-in-europe/.

85. *Szabó and Vissy*, above note 2, ¶ 69 (quoting *Kennedy*, above note 51, ¶ 160)

86. *Digital Rights Ireland*, above note 30, ¶¶ 58–59; Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks, art. 6. But see *Tele2 Sverige AB and Watson and others*, Opinion of the Advocate General, above note 76, ¶¶ 116 and 126 *et seq.*, which interprets the *Digital Rights Ireland* judgment as permitting EU Member States to impose data-retention mandates if other requirements of EU law (including the Charter) are met.

Schrems, the Court found that legislation allowing government authorities to enjoy "access on a generalised basis" to electronic communications must, at least insofar as this generalized access applies to content, "be regarded as compromising the essence of the fundamental right to private life."[87]

Where the ICCPR is concerned, the relevant UN experts continue to grapple with the question of whether mass surveillance can ever comply with the requirement of non-arbitrariness. As noted above, General Comment 16 rejects altogether the idea that secret communications surveillance of any kind may comply with Article 17, although the HRC and the OHCHR appear to have shifted to a less absolutist position over the years.[88] In its 2014 report, the OHCHR drew upon the HRC's 1999 General Comment on the right to freedom of movement in maintaining that in order to be necessary and proportionate, state surveillance must adopt the "least intrusive" approach possible. Applying this logic, the High Commissioner concluded that "[m]ass or 'bulk' surveillance programmes may thus be deemed to be arbitrary, even if they serve a legitimate aim and have been adopted on the basis of an accessible legal regime."[89]

Meanwhile, after suggesting that some states are employing data-mining techniques to search through vast quantities of electronic communications, thus surveilling very large numbers of individuals who are not suspected of having engaged in any wrongdoing, Emmerson notes that "[t]he hard truth is that the use of mass surveillance technology effectively does away with the right to privacy of communications on the Internet altogether." Without directly stating that mass surveillance can never be compliant with human rights, Emmerson goes on to indicate that "[t]he sheer scale of the interference with privacy rights calls for a competing public policy justification of analogical magnitude"—a statement that is perhaps best read as raising serious doubts as to whether such a justification could ever in fact exist.[90]

IV. THE FREEDOMS OF EXPRESSION, RELIGION, ASSEMBLY, AND ASSOCIATION

Although assessments of mass surveillance under the international human rights framework have tended to focus on the implications for the right to privacy, the impact of these practices on the freedom of expression (which includes the right to receive and impart information); the non-derogable freedoms of opinion, thought, conscience, and religion; and the freedoms of association and

87. *Schrems*, above note 34, ¶ 94.

88. Above notes 11–12 and accompanying text.

89. OHCHR report, above note 5, ¶ 25.

90. Emmerson report, above note 46, ¶¶ 12–13.

peaceful assembly may be equally serious.[91] Each of these rights is found in the UDHR, ICCPR, ACHR, ECHR, and EU Charter; the American Declaration does not contain an explicit freedom of thought but otherwise generally tracks the other human rights instruments in these respects.[92] While the UN General Assembly and at least two UN Special Rapporteurs have depicted the right to privacy as a type of gateway for the enjoyment of free-expression (and presumably other) rights, these latter entitlements stand on an equal footing with the right to privacy and merit far more scrutiny in the surveillance context than they have received to date.[93]

The ECtHR has seldom addressed cases involving both communications surveillance—particularly on a large scale—and free-expression rights, although two communicated cases against the United Kingdom that remain pending at the time of writing raise these issues.[94] At present, the Court's main observations on this point remain those found in its admissibility decision in *Weber and Saravia*, in which the Third Section (based on the text of the ECHR, in which the provision concerning the right to free expression broadly mirrors that concerning the right to respect for private life) effectively proceeded through a compressed version of the four-step analysis outlined above in examining the impact of an arguably mass surveillance program on a journalist.[95] The Court began by referring to "the vital public-watchdog role of the press" and finding that the existence of legislation allowing secret surveillance constituted an interference with the journalist's right to free expression, as the threat of surveillance might reveal her sources or deter them from speaking with her.[96] After finding that the interference was lawful and had a legitimate aim, the Court turned to the question of whether the surveillance was necessary in a democratic society, noting its

91. Cf. generally OHCHR report, above note 5, ¶ 14. On the non-derogability of the freedom of opinion, see Human Rights Committee, *General Comment No. 34: Article 19: Freedoms of Opinion and Expression,* U.N. Doc. CCPR/C/GC/34, September 12, 2011, ¶ 5.

92. UDHR, above note 14, arts. 18–20; ICCPR, above note 4, arts. 18–19, 21–22; ACHR, above note 4, arts. 12–13, 15–16; ECHR, above note 4, arts. 9–11; EU Charter, above note 20, arts. 10–12; American Declaration, above note 14, arts. 3–4, 21–22.

93. General Assembly, above note 61, preamble ("recognizing that the exercise of the right to privacy is important for the realization of the right to freedom of expression and to hold opinions without interference and the right to freedom of peaceful assembly and association"); United Nations General Assembly, *The Right to Privacy in the Digital Age*, U.N. Doc. A/RES/68/167 (December 18, 2013), preamble (containing similar language concerning the right to freedom of opinion and expression); Human Rights Council, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye*, U.N. Doc. A/HRC/29/32 (May 22, 2015), ¶ 16 (deploying the "gateway" concept; hereinafter Kaye report); La Rue report, above note 26, ¶ 24.

94. *10 Human Rights Organisations v. the United Kingdom and Bureau of Investigative Journalism and Ross v. the United Kingdom*, above note 9.

95. *Weber and Saravia*, above note 39, ¶¶ 143 *et seq.*

96. Ibid., at ¶¶ 143–146.

own long-established rule that a state's interference with a journalist's exercise of free-expression rights will violate the Convention unless the action is "justified by an overriding requirement in the public interest."[97] In the Court's view, the German regime at issue was subject to strict safeguards; the fact that the surveillance was not "aimed at monitoring journalists" was also a deciding factor for the judges, as they believed this meant that the interference could not be characterized as a "particularly serious" one.[98] Ultimately, the Court concluded that Germany's surveillance activities had not violated the right.[99]

Aside from *Weber* (whose persuasiveness, as a single admissibility decision, is debatable), international jurisprudence concerning these issues is scant. The ECtHR found in a succinct 2013 judgment against Serbia that the state had failed to comply with domestic law in refusing to disclose, upon request by a nongovernmental organization, the number of individuals it had subjected to secret surveillance; thus, the state violated the right to receive information, which is part of the Convention right to free expression (and has been further explicated in non-binding form in the Global Principles on National Security and the Right to Information, known as the Tshwane Principles).[100] Regrettably, the CJEU did not reach the issue of free-expression rights in *Digital Rights Ireland* despite the fact that the referring court had presented it with an opportunity to do so.[101]

Notwithstanding this lag on the part of the international courts, the Special Rapporteurs of the UN and IACHR who focus on the freedom of expression have been addressing electronic surveillance issues proactively since at least 2011.[102] The most recent UN Special Rapporteurs in this area have focused on the importance of online anonymity for facilitating the exercise of the right, especially

97. Ibid., at para. 149 (citing *Goodwin v. the United Kingdom*, Application no. 17488/90, Judgment (Grand Chamber), March 27, 1996, ¶¶ 39–40).

98. Ibid., at ¶¶ 147–152.

99. Ibid., at ¶ 153.

100. *Youth Initiative for Human Rights v. Serbia*, Application No. 48135/06, Judgment, June 25, 2013, ¶¶ 24–26; *Global Principles on National Security and the Right to Information (Tshwane Principles)* (2013), https://www.opensocietyfoundations.org/sites/default/files/global-principles-national-security-10232013.pdf. The Tshwane Principles posit, inter alia, that "[n]o restriction on the right to information on national security grounds may be imposed unless the government can demonstrate that: (1) the restriction (a) is prescribed by law and (b) is necessary in a democratic society (c) to protect a legitimate national security interest; and (2) the law provides for adequate safeguards against abuse, including prompt, full, accessible, and effective scrutiny of the validity of the restriction by an independent oversight authority and full review by the courts" (Principle 3).

101. *Digital Rights Ireland*, above note 30, ¶¶ 18, 70.

102. See Human Rights Council, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue*, U.N. Doc. A/HRC/17/27 (May 16, 2011), ¶¶ 53 *et seq.*

where controversial topics are concerned;[103] they have also encouraged state respect for individuals' use of strong encryption technologies, as encryption, like anonymity, "create[s] a zone of privacy to protect opinion and belief."[104] As current UN Special Rapporteur on free expression David Kaye has written: "The ability to search the web, develop ideas and communicate securely may be the only way in which many can explore basic aspects of identity, such as one's gender, religion, ethnicity, national origin or sexuality."[105] It is easy to imagine that systematic government access to private-sector data, whether through real-time interception, data-retention laws, or some other means, may burden the freedoms of thought, opinion, religion, and/or expression in a manner that does not comply with the treaties. Indeed, shortly after the Snowden disclosures, La Rue and his IACHR counterpart Catalina Botero released a joint declaration stating that "indiscriminate access to information on communication between persons can have a chilling effect on the free expression of thought and the search for and distribution of information," and emphasizing that "the law must authorise access to communications and personal information only under the most exceptional circumstances defined by legislation."[106]

Meanwhile, the effect of mass surveillance on the freedoms of opinion; thought, conscience, and religion; assembly; and association appear to remain unaddressed in international case law. However, Kaye has pointed out that both mass and targeted surveillance "may undermine the right to form an opinion, as the fear of unwilling disclosure of online activity, such as search and browsing, likely deters individuals from accessing information, particularly where such surveillance leads to repressive outcomes."[107] The same observation likely applies to the chilling effect on individuals' ability to explore and form religious views; indeed, in Europe, systematic government access to private data may necessarily entail violations of what the ECtHR has described as an individual's right "not to be obliged to disclose his or her religion or beliefs,"[108] as these will often be obvious from communications, browsing histories, and so on. Moreover, it is easy to imagine that a government's systematic surveillance of communications and/or related data (such as location information) could have an impermissible

103. Ibid., at ¶¶ 53 and 55; Kaye report, above note 93, ¶ 12.

104. Kaye report, above note 93; cf. Human Rights Council, above note 102, ¶ 55 (implying that states should allow individuals to use encryption).

105. Kaye report, above note 93, ¶ 12.

106. United Nations Special Rapporteur on the protection and promotion of the right to freedom of opinion and expression and the Special Rapporteur for freedom of expression of the Inter-American Commission on Human Rights, *Joint Declaration on Surveillance Programmes and Their Impact on Freedom of Expression* (June 21, 2013), http://www.oas.org/en/iachr/expression/showarticle.asp?artID=926&lID=1.

107. Kaye report, above note 93, ¶ 21.

108. *Işik v. Turkey*, Application no. 21924/05, Judgment, February 2, 2010, ¶ 41.

deterrent effect upon individuals' right to assemble and associate with others—for example, at political protests, union meetings, or religious study groups.

V. REMEDIES AND FREEDOM FROM DISCRIMINATION IN THE ENJOYMENT OF RIGHTS

A. The Right to a Remedy for Violations of the Foregoing Rights

Each of the human rights instruments described herein manifests a concern with ensuring that states cannot violate their legal obligations with impunity. In the earlier instruments, this concern takes the form of requiring states to provide individuals with a remedy for acts violating constitutional or other legal rights.[109] The later-developed ICCPR, ACHR, and ECHR make it clear that the obligation to provide a remedy extends to violations of the rights found in these treaties as such.[110] This requirement is formally distinct from, although closely related to, the oversight- and notification-related obligations identified in the case law and commentary described above.

The salient provision of the American Declaration refers explicitly and exclusively to accountability through the courts, whereas the ACHR refers to the need for a "court or tribunal," the EU Charter uses the term "tribunal," and the ECHR refers to a "national authority."[111] Meanwhile, the ICCPR suggests that redress for rights violations may be provided by "judicial, administrative or legislative authorities, or by any other competent authority provided for by the legal system of the State," but specifically requires states parties to undertake to "develop the possibilities of judicial remedy."[112] Thus, whether the redress in question must necessarily be judicial will likely depend upon the instrument(s) by which a state is bound as well as the case law of the international human rights bodies.

The ECtHR, for its part, has developed a substantial body of findings on this subject, thus far declining to find that a remedy must be judicial but emphasizing the need for the pertinent body—whatever form it takes—to be independent and effective.[113] Although the Court once adopted the stance that the availability of a remedy in the surveillance context is only required after the interference has been disclosed, it now appears to demand at least a limited remedy while the surveillance (whether confirmed or alleged) remains underway. Such a limited remedy might include, for example, "one where the proceedings are secret and

109. UDHR, above note 14, art. 8; American Declaration, above note 14, art. 18.

110. ICCPR, above note 4, art. 2(3); ACHR, above note 4, art. 25; ECHR, above note 4, art. 13.

111. American Declaration, above note 14, art. 18; ACHR, above note 4, art. 25; ECHR, above note 4, art. 13; EU Charter, above note 20, art. 47.

112. ICCPR, above note 4, art. 2(3)(b).

113. See, for example, *Leander*, above note 41, ¶¶ 81, 83–84; *P.G. and J.H.*, above note 31, ¶ 88.

where no reasons are given, and the persons concerned are not apprised whether they have in fact been monitored—even at this stage."[114] The remedial body must nevertheless be able to "grant appropriate relief."[115]

B. Discrimination in Respect of Treaty Rights

As a final point where state obligations are concerned, the human rights instruments are uniform in demanding that government authorities uphold the rights contained in those instruments in a manner that does not discriminate on the basis of, for example, race, color, religion, sex, language, or political or other opinion.[116] Thus, if a state were to seek access to private-sector data (thus interfering with privacy rights) on a discriminatory basis, or use data-mining techniques to identify individuals who may belong to a certain religion or hold a certain opinion (again interfering with privacy and potentially other rights), these practices would presumably run afoul of the state's non-discrimination obligations. Where a state is a party to the International Convention on the Elimination of All Forms of Racial Discrimination, its commitments under that instrument will also be salient.[117]

Although this chapter does not address the question of whether ICCPR or other human rights treaty obligations apply extraterritorially, the OHCHR has recently taken the novel approach of applying the anti-discrimination principles to suggest that a state must respect privacy and other human rights "regardless of the nationality or location" of the individual who is being monitored.[118] It remains to be seen whether the regional human rights courts will follow the UN entities' lead in this respect.

VI. CONCLUSION

As state demands for systematic access to communications held or transmitted by the private sector increase, it is crucial to recall the danger against which the ECtHR and other commentators have so bluntly warned: the creation of legal regimes in which fundamental rights are traded away in the name of crime prevention and national security—in other words, police states. The consistency with which the international human rights treaties, courts, and experts have

114. *Association for European Integration and Human Rights and Ekimdzhiev*, above note 56, ¶ 100.

115. *P.G. and J.H.*, above note 31, ¶ 85.

116. UDHR, above note 14, art. 2; American Declaration, above note 14, art. 2; ICCPR, above note 4, art. 2(1); ACHR, above note 4, art. 1; ECHR, above note 4, art. 14; EU Charter, above note 20, art. 21

117. International Convention on the Elimination of All Forms of Racial Discrimination, 660 U.N.T.S. 195 (1965).

118. OHCHR report, above note 4, ¶¶ 35–36.

identified and interpreted the relevant rights, as well as their increasing criticisms of mass surveillance, should serve as a reminder that state interferences with private data are not necessarily legal simply because they may currently be ubiquitous. Both states and individuals should take the long view by following the apparent trend among the international bodies and concluding that mass surveillance violates human rights—and that, for all of us, those rights are too valuable to relinquish.

20

Standards for Independent Oversight

The European Perspective

NICO VAN EIJK

I. ABSTRACT

The point of departure for this chapter is the decision of the European Court of Justice in the *Digital Rights Ireland* case, which annulled the European Data Retention Directive, in part because the use of retained data was not made subject to independent oversight. Next, it examines judgments from the national courts of the Netherlands and the UK, also focusing on the independent oversight issue, declaring invalid the data retention laws of those two countries. From the *Digital Rights Ireland* case and others, seven standards for oversight of intelligence services can be drawn: the oversight should be complete; it should encompass all stages of the intelligence cycle; it should be independent; it should take place prior to the imposition of a measure; it should be able to declare a measure unlawful and to provide redress; it should incorporate the adversary principle; and it should have sufficient resources.

II. INTRODUCTION

There are many ways to approach the question of government access to private-sector data. Much of the recent public debate has focused on access in the context of national security and traditional law enforcement, with respect to both targeted and untargeted access ("bulk collection" or "mass surveillance") to data collected and processed by third parties. As more and more data is collected and stored by the private sector ("big data"), the amount of data that can be retrieved by governments is steadily increasing. Traditional impediments, such as storage and processing costs, no longer apply. Moreover, data collected

Bulk Collection. Fred H. Cate and James X. Dempsey.

privately is increasingly used not just for national security and traditional law enforcement purposes. A new "third domain" has emerged, where data is used for social security and tax surveillance and other types of nontraditional law enforcement. For lack of a better term, we call this third category "public task surveillance."[1]

Government access to private data implies the deployment of government power. In a classic rule of law tradition this requires an explicit basis in law and a carefully crafted system of checks and balances: special powers require special guarantees. Independent oversight is an undeniably crucial element of such a system of checks and balances.

The major preconditions for independent oversight can be found in the judgment of the European Court of Justice (ECJ) in the *Digital Rights Ireland* case,[2] which annulled the European Data Retention Directive.[3] Particularly, the Court took the view that the Directive did not comply with Article 7 (Privacy) and Article 8 (Data protection)[4] of the Charter of Fundamental Rights of the European Union (the Charter).

The *Digital Rights Ireland* case is the point of departure of this chapter.[5] Next, two recent judgments by national courts are described, in which national data

1. Readers of this chapter are encouraged to come up with a better name. Access for other types of use, such as statistical analysis, fall outside the scope of this essay. However, we note that several similar questions are at stake. For example, the collection of statistical data can be based on a legal obligation. In such a case, questions arise on the existence of free consent, proportionality, function creep, etc.

2. Judgment of the Court (Grand Chamber) of 8 April 2014 (requests for a preliminary ruling from the High Court of Ireland (Ireland) and the Verfassungsgerichtshof (Austria))—*Digital Rights Ireland Ltd (C-293/12) v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, The Commissioner of the Garda Síochána, Ireland and the Attorney General, and Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and Others (C-594/12)*, (Joined Cases C-293/12 and C-594/12.

3. Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, Pb. L 105/54, 13 April 2006.

4. Article 7 (Respect for private and family life): "Everyone has the right to respect for his or her private and family life, home and communications." Article 8 (Protection of personal data): "1. Everyone has the right to the protection of personal data concerning him or her; 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified; 3. Compliance with these rules shall be subject to control by an independent authority."

5. The Data Retention decision of the ECJ was an important element in the Safe Harbor decision, which annulled the agreement between Europe and the United States on the transfer of

retention rules were tested against the ruling in the *Digital Rights Ireland* case, and the necessity of independent oversight was discussed in further detail.

We draw from a recent study by the IViR to formulate standards for independent oversight.[6] These standards are based on a broader analysis of the relevant jurisprudence of the European Court of Justice—including the *Digital Rights Ireland* case—and of the European Court of Human Rights (ECtHR).[7] The analysis is also based on selected studies, reports, resolutions, and recommendations.

In the IViR study and in this chapter, we use a broad definition of the term "oversight" to include the various ways of holding government agencies accountable before the public and the government: internal oversight by the responsible minister, parliamentary oversight, judicial oversight, and external independent oversight. In the surveillance context, oversight can focus on specific instances in which surveillance measures are implemented against a particular target, on bulk interception of electronic communications, or on the overall functioning of a system of secret surveillance and data collection.

III. THE EUROPEAN DATA RETENTION DIRECTIVE

As a result of the 2004/2005 bombings in Madrid and London, the so-called Data Retention Directive came into effect in 2006. This Directive was based on general powers under the EU-treaties to harmonize rules in the European Union. It did not concern national security as such, as the European Union does not have any powers in this domain. National security is the sole responsibility of the Member States. The European Union does have some authority with respect to traditional law enforcement, but in this domain, too, the role of the Member States is decisive to a large extent.

data (European Court of Justice (*Schrems v. Data Protection Commissioner*), Case C-362/14, 6 October 2015).

6. Sarah Eskens, Ot van Daalen & Nico van Eijk, "10 Standards for Oversight and Transparency of National Intelligence Services," 8 *J. Nat'l Security L. & Pol'y*, no. 3, (2016) pp. 553–594, http://jnslp.com/wp-content/uploads/2016/07/10_Standards_for_Oversight__Transparency.pdf.

This chapter focuses on the oversight elements of the study.

7. The European Court of Human Rights in Strasbourg—applying the European Convention on Human Rights—has a rich tradition of jurisprudence on surveillance. This jurisprudence is also applicable to the European Union. The Charter makes this explicit in article 52, par. 3: "In so far as this Charter contains rights which correspond to rights guaranteed by the European Convention on Human Rights, the meaning and scope of those rights shall be the same as those laid down by said Convention. This provision shall not prevent Union law providing more extensive protection." Recently, the European Court of Human Rights issued two important decisions confirming and deepening its earlier jurisprudence on surveillance (Case of *Roman Zakharov v. Russia* (Application no. 47143/06, Strasbourg, 4 December 2015) and Case of *Szabó and Vissy v. Hungary* (Application no. 37138/14, Strasbourg, 12 January 2016).

Therefore, the Directive was intended to harmonize the laws of Member States concerning the obligations of the providers of publicly available electronic communications services or of public communications networks with respect to the retention of certain data that is generated or processed by them, in order to ensure that the data would be available for the purpose of the investigation, detection, and prosecution of serious crime, as defined by each Member State in its national law. The scope of the Directive included both location and traffic data, but content fell outside the Directive. It should be noted that if topics fall outside the scope of a directive, they can still be subject to regulation. Member States are entirely free to step in (or have regulation in place already).

The Directive provided only a framework for national laws, as shown not only by its short length but also by the general nature of its provisions on access, retention duration (between six months and two years), data storage and security, and oversight. Detailing these aspects was left to the Member States.

A. European Court of Justice Declares Directive Invalid

As soon as the Directive entered into effect, it was challenged on fundamental grounds. Consequently, its implementation was blocked completely or partly by national courts in several countries, for instance in Bulgaria (2008), Romania (2009), Germany (2010), and Cyprus (2011).

In the *Digital Rights Ireland* case, the Directive was eventually submitted to the European Court of Justice (ECJ).[8] In his preceding opinion, the Advocate-General concluded that the Directive was not in compliance with the Charter, but that some room should be allowed for repair.[9]

The Court found no such room and declared the entire Directive invalid. Such a step is very unusual. Declaring a directive invalid is an extreme measure.

As to oversight, the Court based its judgment on Article 8 of the Charter, in which data protection is guaranteed as a fundamental right. Paragraph 3 of Article 8 provides that "compliance with these rules shall be subject to control by an independent authority." The paragraph doesn't allow exceptions. The Court stated "In particular, Directive 2006/24 does not lay down any objective criterion by which the number of persons authorised to access and subsequently use the data retained is limited to what is strictly necessary in the light of the objective pursued. Above all, the access by the competent national authorities to the data retained is not made dependent on a prior review carried out by a court or by an

8. In an earlier case, the ECJ had decided that the EU treaty as such provided sufficient ground for the Directive (Case C-301/06, *Ireland v European Parliament and Council of the European Union*). However, the ECJ made explicit that it was not looking into the substance: "It must also be stated that the action brought by Ireland relates solely to the choice of legal basis and not to any possible infringement of fundamental rights arising from interference with the exercise of the right to privacy contained in Directive 2006/24."

9. Opinion 12 December 2013 (ECLI:EU:C:2013:845).

independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued and which intervenes following a reasoned request of those authorities submitted within the framework of procedures of prevention, detection or criminal prosecutions. Nor does it lay down a specific obligation on Member States designed to establish such limits."[10]

Noting another consideration, the Court completed its reasoning with respect to independent oversight by stating: "the directive does not require the data in question to be retained within the European Union, with the result that it cannot be held that the control, explicitly required by Article 8(3) of the Charter, by an independent authority of compliance with the requirements of protection and security, as referred to in the two previous paragraphs, is fully ensured. Such a control, carried out on the basis of EU law, is an essential component of the protection of individuals with regard to the processing of personal data."[11]

Additionally, the Court made one other comment that is relevant to the question of oversight when it noted that the Directive did not make any distinction concerning the collection of data concerning individuals (such as lawyers) who are bound by a duty of professional secrecy: "Directive 2006/24 affects, in a comprehensive manner, all persons using electronic communications services (. . .). Furthermore, it does not provide for any exception, with the result that it applies even to persons whose communications are subject, according to rules of national law, to the obligation of professional secrecy."[12] With this, the Court seemed to indicate that independent oversight in the case of 'professional secrecy'—and perhaps with regards to other uniquely sensitive matters as well—requires special attention and safeguards.

B. National Courts Follow ECJ Decision

After the judgment of the European Court of Justice, various national courts have had to rule on the consequences of the judgment for national legislation. After all, the cancellation of a directive does not automatically mean that the national implementation is invalid. A directive allows Member States some leeway for further specification by which the national regulations might be in compliance with the preconditions. The countries where the implementation of the judgment of the Court has been tested include the Netherlands, Belgium, Slovenia, and the United Kingdom. In each of these countries, the national implementations of the Data Retention Directive were annulled after judicial review. In the Netherlands and the United Kingdom, the Court explicitly focused on the independent oversight issue.

10. ¶ 62.

11. ¶ 68.

12. ¶ 58.

1. The Netherlands

On March 11, 2015, a district court in the Netherlands annulled the Dutch implementation of the Directive.[13] The Netherlands had implemented the Directive via a special law, the Wbt (Act Data Retention Telecommunication Services). With respect to oversight, the court concluded that independent oversight was not provided for in the Dutch implementation: "The foregoing is all the more important considering that the Wbt and related regulations do not require a prior authorisation by a judicial authority or independent administrative body in order to access the retained data. Different from that which is argued by the State, the office of public prosecution cannot be considered an independent administrative body. That the Court[14] has considered this as a compelling objection can be derived from the words 'above all' in consideration 62 of the judgment."[15] The decision of the district court was not challenged pending an upcoming review of the Dutch Intelligence and Security Services Act.

In an October 2015 decision, the same court dealt with the lack of restrictions on the surveillance of lawyers.[16] Because no special EU legislation or regulation is applicable to lawyers, the court did not use the EU Charter as a reference but relied instead on Article 8 of the European Convention on Human Rights (the Convention), which provides for protecting privacy and has been used in several cases dealing with surveillance. The court was of the opinion "that the breaching of journalists' and lawyers' privilege has serious consequences for the principles of a democratic state governed by the rule of law."[17] The court continued: "The mere possibility of breaches of lawyers' privilege affects the confidentiality of communications between lawyers and their clients and thus the right to an effective defence and the availability of lawyers. So in a sense this breach is also irreversible. Having regard to the serious consequences of (possible) breaches of lawyers' privilege and given that in individual cases abuse is potentially easy, the judge considers that, in accordance with the reasoning of the ECtHR in para. 98 of the *Telegraaf* case,[18] it is highly desirable that there should be independent oversight of the exercise of special powers, such that the oversight body must possess inter alia the power to prevent or to terminate the exercise of special powers."[19] The decision forced the Dutch government to implement an

13. ECLI:NL:RBDHA:2015:2498. Unofficial translation: http://theiii.org/documents/DutchDataRetentionRulinginEnglish.pdf

14. The ECJ in the *Digital Rights Ireland* case.

15. ¶ 3.11.

16. ECLI:NL:RBDHA:2015:7436, no translation available; the Hague court of appeal upheld the verdict ECLI:NL:GHDHA:2015:2881. Unofficial translation of the decision by the Hague court of appeal: http://www.advocates.org.uk/media/1912/dutchspyingruling.pdf.

17. ¶ 4.10.

18. Case of *Telegraaf Media Nederland, Landelijke Media bv and others v. The Netherlands* (Application no. 39315/06), 22 November 2012.

19. ¶ 4.10.

exective order introducing a first form of ex ante independent oversight. A special independent committee assesses the proposed orders and can block them.[20] The order only deals with lawyers and the protection of journalists' sources.

2. United Kingdom

In response to the Data Retention Directive being declared invalid in the *Digital Rights Ireland* case, the United Kingdom immediately adopted a new act, the Data Retention and Investigatory Powers Act 2015 (DRIPA), in an effort to address the gaps in the Directive identified by the ECJ and thus provide an adequate basis for data retention. The act was fast-tracked through Parliament and adopted within three days. In a High Court ruling of July 17, 2015, however, the act was declared invalid.[21] The complainants argued that the act violated Articles 7 and 8 of the Charter, and the Court agreed. With respect to prior independent oversight the Court referred to the considerations noted by the ECJ in the *Digital Rights Ireland* case and tested the UK legislation against them. The High Court pointed out that "the provisions of RIPA, as applied by DRIPA, require (as we have noted above) that an application for access to communication data must be considered by a senior person who is independent of the investigation. There is already a need for there to be a written request for approval. The need for that approval to be by a judge or official wholly independent of the force or body making the application should not, provided the person responsible is properly trained or experienced, be particularly cumbersome [. . .]; but if EU law requires independent approval, as we are satisfied it does, that must be put in place. It is not for us to devise the appropriate system."[22]

It is interesting that the British Court paid close attention to the same subject that had been dealt with earlier in the second Dutch case, that is, the special position of lawyers—but others are added as well—and stated: "However, communications with practising lawyers do need special consideration. The same in our view can properly be said to apply to communications with MPs." As far as oversight is concerned, it concludes: "As to the question of what level of consideration should be given to applications involving access to data involving communications with lawyers, Members of Parliament, or journalists, that too is not for us to determine. We only observe that such cases do require special consideration."[23]

20. The order by the ministers of the Interior and of Defence, responsible for national security, is named "Tijdelijke regeling onafhankelijke toetsing bijzondere bevoegdheden Wiv 2002 jegens advocaten en journalisten" (no translation available) and was published in the Official Journal of 23 December 2015 (No. 46477).

21. [2015]EWHC 2092 (Admin), Case No: CO/3665/2014, CO/3667/2014, CO/3794/2014, dd. 17/7/2015.

22. ¶ 98.

23. Ibid.

Finally, the High Court emphasized that it was distingusihing in its analysis between access and retention: "We add the important proviso that the requirement of prior approval relates to access, not to retention. We see no reason why the exercise of the power to retain should need prior independent approval, and we do not understand the CJEU to have held that it does."[24]

IV. STANDARDS FOR INDEPENDENT OVERSIGHT

The *Digital Rights Ireland* decision of the European Court of Justice forms a core element in our IViR study *Ten Standards for Oversight and Transparency of National Intelligence Services*. In this study, we formulate generally applicable standards for independent oversight. These standards are based on the jurisprudence of the European Court of Justice and the European Court of Human Rights, including what can be deduced from that jurisprudence as best practices, and our assessment of the direction future case law is likely to take. In order to further substantiate the standards, the study draws from a selection of reports and soft law measures that have been issued in Europe and the United States.

The following list from the study relates to oversight of intelligence services, especially in the context of communication interception using the sophisticated technologies now associated with untargeted ("mass") surveillance. The standards should be read in combination—one would not work without the others. For example, independence in oversight will only be effective if oversight is supported by adequate resources. No references are included but can be found in the report.

A. Intelligence Services Need to Be Subject to Oversight That Is Complete

Under this standard, oversight should be complete in three respects: (1) The oversight *bodies themselves*: the government, parliament, the judiciary, and a specialized (non-parliamentary, independent) commission should all play a role in oversight. (2) The *moment* of oversight: oversight should include prior oversight, ongoing oversight, and oversight after the fact. (3) *Mandate*: the oversight bodies' mandate should encompass review of both lawfulness and effectiveness.

Disclosures in the media have demonstrated that there is a need for enhanced oversight, even in countries where oversight appears to be quite comprehensive. The overall blend of oversight mechanisms for national intelligence services is important. In the end, oversight encompassing all of the above elements is essential to ensure that adequate and effective guarantees against abuse and arbitrary use of secret surveillance and data collection powers are in place. Because the effectiveness or ineffectiveness of intrusive measures is relevant to the

24. ¶ 99.

proportionality test, we deduce from the jurisprudence that courts can address both lawfulness and effectiveness.

B. Oversight Should Encompass All Stages of the Intelligence Cycle

Surveillance occurs in stages, including the collection, storage, querying, and analysis of data. As each of these stages amounts to an interference with the right to privacy, each should be subject to oversight to a certain degree. In practice, this means that not only collection and selection stages should be subject to prior independent oversight, but also the analysis itself.

C. Oversight of the Intelligence Services Should Be Independent

Some of the oversight bodies must be independent of the intelligence services and the government. For example, public prosecutors in most political systems cannot be regarded as independent of the government. Similarly, government ministers cannot provide for independent oversight, as they are part of the government that is both the tasking body and the customer of the intelligence services. Judicial oversight offers the best guarantees of independence. Therefore, it is preferable to entrust oversight of secret surveillance and data collection to a judge, as is already the case in certain jurisdictions. However, the independence of judicial-like bodies is not a given. However, the fact that some courts in the past "rubber-stamped" government requests or took quite long in making their decisions is not an argument against judicial oversight as such. Rather, such concerns merely underline that adequate resources are essential to guarantee the independence and effectiveness of oversight bodies.

The independence of a specialized commission can be guaranteed by having its members appointed by parliament using an open and transparent selection and nomination procedure, where the voting power should not depend on parliamentary size, but where, for example, each political party including the opposition gets a vote. Furthermore, a standing parliamentary committee specializing in oversight of the intelligence services can be regarded as independent only if its members represent the opposition as well as the ruling parties, and the member's voting power does not depend on its parliamentary size. The procedure for dismissing members of an oversight body should also guarantee independence. Preferably, national law or the national constitution should provide that specialized commissions and parliamentary committees cannot be subject to instructions from the government.

There is some overlap between oversight by parliamentary committees and specialized (parliamentary-appointed) commissions, in the sense that both are independent and democratically legitimized. Nevertheless, there are advantages in having both of them. A parliamentary committee is in a better position to defend itself vis-à-vis parliament as a whole and the public, whereas a specialized commission allows for greater expertise in oversight.

To summarize: independence is reflected in several elements, including: (1) transparent and objective procedures for the nomination of the members of oversight bodies, (2) no governmental interference with the activities and decisions of the institution performing the oversight, (3) effective powers, and (4) adequate resources and budgetary independence.

D. Oversight Should Take Place prior to the Imposition of a Measure

In the field of secret surveillance of communications, especially using the sophisticated technologies now associated with untargeted surveillance, the risk of abuse is high, and abuse can have harmful consequences not only for individual rights but also for democratic society as a whole. Therefore, prior judicial oversight of the application of surveillance and collection powers is strongly preferred. Furthermore, the transfer of personal data to third countries requires prior approval by the competent supervisory authority. As an alternative to prior judicial oversight, a system of ministerial orders combined with prior oversight by an independent, specialized commission, after-the-fact oversight on the overall functioning of the system of surveillance by a parliamentary committee, and the possibility for individuals to complain before an independent body could also be compliant with human rights standards. Regardless of the structure, effective oversight will only exist if the body performing prior oversight has adequate powers (see the next Standard).

It should be noted that prior oversight is not at odds with ministerial responsibility: in a system of prior oversight, the minister gives an order for surveillance, and the oversight body merely has the power to block this order. Where—due to exceptional circumstances—it is not possible to wait for a decision by the oversight body because of the urgent nature of the order, the order should be subject to oversight as soon as possible. In addition, the oversight body should have sufficient resources to handle orders quickly. Political responsibility and optimizing the protection of fundamental rights are different topics.

E. Oversight Bodies Should Be Able to Declare a Measure Unlawful and to Provide for Redress

Bodies providing prior and ongoing oversight for intelligence services should have the power to prevent or end a measure imposed by intelligence services, and oversight bodies should have the power to declare a measure unlawful after the fact. In all cases, the oversight body should have the power to order the purging of personal data. Obviously, oversight powers will be effective only if combined with the power to make legally binding decisions and to provide for redress of the unlawfulness of a measure. Given the gravity of the decision to block or end use of a particular surveillance measure, the minister should simultaneously have the power to appeal such descisions to a court. Initial orders to conduct

surveillance should contain sufficient reasoning to allow oversight bodies and appellate courts to evaluate the lawfulness of the measure.

F. Oversight Should Incorporate the Adversary Principle

Where there is no prior judicial oversight, oversight mechanisms have survived the ECtHR's scrutiny under Article 8 of the European Convention on Human Rights only if they included an adequate complaint procedure. In such a procedure, the individual concerned can challenge the lawfulness of measures of secret surveillance and data collection directed against him after the fact. In recent case law, the Court also implied that it should be possible to provide some form of adversarial proceeding prior to approval of a surveillance measure, albeit one where the proceedings are secret. There is some overlap between the Court's interpretation of Article 8 in cases about secret surveillance and data collection for the purpose of national security and cases about deportation for the purpose of national security. In the context of the latter, the Court expressly requires "some form of adversarial proceedings."

This could mean involving a special advocate who defends the public interest (or the interest of affected individuals). This would introduce some form of adversarial proceedings without jeopardizing the secrecy of measures to be imposed. Where the surveillance is more general in nature, the special advocate would rather take on the role of an expert for the court, in order to allow the court to be in a better position to weigh the interests of the intelligence services against the interests of the public in not being subject to surveillance. Where the surveillance is more targeted, the special advocate would defend the rights of the individuals affected. In its 2007 report, the Venice Commission was critical of special advocates, but in its 2015 update of the report it argues for the involvement of privacy advocates as regards searching data obtained by strategic surveillance.[25] One of the most important recommendations of the United States Privacy and Civil Liberties Oversight Board called for the establishment of special advocates before the FISA Court.[26]

25. Report on the democratic oversight of the security services, adopted by the European Commission for Democracy through Law (Venice Commission), Venice, 1–2 June 2007 (CDL AD(2007)016); Update of the 2007 report on the democratic oversight of the security services and report on the democratic oversight of signals intelligence agencies, adopted by the European Commission for Democracy through Law (Venice Commission), Venice, 20–21 March 2015 (CDL-AD(2015)006).

26. Privacy and Civil Liberties Oversight Board, *Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court*, PCLOB 215 Report (January 23, 2014), p. 185. In 2015, in the USA FREEDOM Act, Congress in fact authorized the appointment of special advocates in cases before the FISA Court, and the Court has since appointed advocates in several cases and designated a small pool of advocates who could be drawn upon in future cases.

G. Oversight Bodies Should Have Sufficient Resources to Perform Effective Oversight

For oversight bodies to function effectively in practice, it is critical that they have the resources to obtain the necessary equipment and staff as well as resources in terms of information[27] and technical expertise. Having adequate resurces will ensure that oversight bodies are independent of the intelligence services and the government. Without access to sufficient resources, oversight bodies cannot fulfil their mandate in a meaningful way. As the technological sophistication of intelligence services will only increase, oversight will become more complicated, and it is to be expected that a commensurate increase in resources for oversight bodies will be necessary.

V. ANALYSIS AND CONCLUSION

European courts consider independent oversight a "condition sine qua non" of government surveillance. Governments cannot access private data without sufficient guarantees, including independent oversight. Recent jurisprudence by the European Court of Justice in the *Digital Rights Ireland* case—annulling the Data Retention Directive—confirms this. It should also be noted that the Charter of Fundamental Rights of the European Union explicitly mentions independent oversight in Article 8 (on data protection), paragraph 3: "Compliance with these rules shall be subject to control by an independent authority." In most European countries, Data Protection Authorities (DPAs) are the independent authority. However, DPAs often have no or only limited authority in the domain of national security or law enforcement.

Access to data to prevent serious crime or terrorism requires an assessment by a judge or an independent body of similar qualifications. This assessment needs to be made before access takes place, but it also needs to be really independent and effective. To achieve this, several standards have been formulated. Not all of these standards are based directly on explicit requirements articulated in the jurisprudence: this is not possible because courts have not yet been in the position to deal with every situation and element. However, for a country that takes the rule of law seriously the implementation of these standards is unavoidable.

The constitutional framework as defined in Articles 7 and 8 of the Charter makes no distinction between the three domains (national security, law enforcement, public tasks). As a consequence, oversight needs to comply with the same standards whenever personal data is accessed for (mass) surveillance. The *Digital Rights Ireland* case makes clear that mass surveillance is worse than targeted

27. Transparency contributes to access to information. In the report, we have three standards on transparency: (1) intelligence services and their oversight bodies should provide layered transparency; (2) oversight bodies, civil society, and individuals should be able to receive and access information about surveillance; and (3) companies and other private legal entities involved in national surveillance should be able to impart information about their involvement.

surveillance but sets oversight standards that are at least similar to those applicable to targeted surveillance. This is why these oversight standards also apply to the third domain (public tasks). Having the same level of qualified independent oversight does not exclude that—by applying subsidiarity and proportionality tests—the allowed use of particular methods and practices can differ among the three domains.

Because the constitutional framework makes no distinction, independent oversight needs to cover not only collection (the acquistion and storage of data into government databases) but also querying the data stored in private systems. Particularly in Europe, it is very likely that governments will collect data autonomously by accessing data stored by private entities. Furthermore, once accessed, data will often move into government-controlled databases. Finally, EU Member States used the Data Retention Directive to oblige operators to collect and store data that they would normally not collect or store. There is only a thin line between collection and access as well as between "metadata" and content. In my view, these lines have no real value anymore from a European fundamental rights perspective.

The ECJ's Data Retention decision gave renewed attention to the special position of "persons whose communications are subject, according to rules of national law, to the obligation of professional secrecy,"[28] requiring special attention in the context of oversight. The Court did not specify who falls within the category of persons subject to the obligations of professional secrecy, leaving it to the national legislator, nor did the Court say anything about what the repercussions should be in the oversight system. This issue is part of the first standard ("Intelligence services need to be subject to oversight that is complete"), and it will be interesting to see how the debate on the position of lawyers, judges, politicians, doctors, and journalists for instance will develop. The question might arise whether thin lines will make clear distinctions still possible.

28. ¶ 58.

21

Stakeholders in Reform of the Global System for Mutual Legal Assistance

PETER SWIRE AND JUSTIN HEMMINGS*

I. ABSTRACT

This chapter briefly explains the reasons that Mutual Legal Assistance Treaties (MLATs) and other forms of trans-border access to electronic data are vital and becoming increasingly more so for law enforcement in this age of globalized evidence. It then adds to the previous literature by presenting the goals of key stakeholders in MLAT reform: national governments other than the United States; the US government, both for law enforcement and other goals; technology companies, such as email and social network providers; and civil society, seeking goals including privacy, free speech, and democracy. This chapter is part of our broader research and law reform project on law enforcement access to electronic evidence held in other nations.[1] Other parts of our ongoing research will delve into the complex procedures and obstacles that characterize international mutual legal assistance today. Our ultimate goal is to propose reforms (or meaningful alternatives) to the Mutual Legal Assistance

* For support of our ongoing MLAT research, the authors wish to thank: the Future of Privacy Forum, the Georgia Tech Institute for Information Security and Privacy, the Georgia Tech Scheller College of Business, and the Hewlett Foundation. In addition, we thank Apple, Facebook, Google, and Microsoft for their research support. The views expressed here are solely those of the authors.

1. The other initial article in this research project is Peter Swire and Justin D. Hemmings, "Mutual Legal Assistance in an Era of Globalized Communications: The Analogy to the Visa Waiver Programme," 71 *NYU Annual Survey of American Law* 687 (2017), http://ssrn.com/abstract=2728478. One theme of that article is the possibility of enacting a Mutual Legal Assistance statute, rather than treaty, modeled on the statutory basis for the Visa Waiver Programme. Our discussion thus generally applies to Mutual Legal Assistance (MLA) issues, and uses the term "MLAT" where the treaties are directly implicated.

(MLA) system.[2] Any such reforms, however, will have to be built on an accurate understanding of the incentives and perspectives of the major stakeholders. This chapter focuses on that task.

II. BRIEF INTRODUCTION TO CURRENT MLAT ISSUES

An example illustrates the rising importance of the MLA process. Suppose there is a burglary in Germany, and the two suspected burglars are both German nationals, living in Germany. The German police learn that the suspects subscribe to an email service and a social networking service, and the police seek the content of those communications. Those records, however, are stored in the United States, where government access to the content is governed by the Fourth Amendment to the US Constitution, generally requiring a search warrant signed by a neutral judge based on probable cause of a crime.[3] The content is also governed by the Electronic Communications Privacy Act (ECPA), which makes it illegal for the technology company to turn over the content of communications unless the statutory provisions are met.[4]

Under ECPA and other current law, the German police would have an office in the German government contact the US Department of Justice, whose Office of International Affairs (OIA) processes requests under a Mutual Legal Assistance Treaty. OIA, working with others in the Department of Justice, would determine whether a legal basis exists for gaining a court order, and then have a prosecutor seek the order. Once granted, the court order would go to the technology company, which would produce the records. Those records would then be reviewed by OIA for compliance with US law, such as no violation of First Amendment

2. For discussion of current MLAT issues, see Andrew K. Woods, "Data beyond Borders: Mutual Legal Assistance in the Internet Age," *Global Network Initiative* (January 2015) 6–7; Richard A. Clark and others, *Liberty and Security in a Changing World: Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies* (December 12, 2013), https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf. One part of our research project is to analyze how MLAT issues interact with the issues about how cross-border personal data will flow between the European Union and the United States in the aftermath of the *Schrems* decision that found the EU/US Safe Harbor unlawful. An interesting aspect of that discussion will be that *Schrems* focused on instances where the European concern has been that data protection rules in the United States are too lax, whereas MLATs involve instances where the concern is that the rules in the United States are too strict. This article, originally written before the *Schrems* decision, will note the interactions but not focus on that complex topic.

3. See *United States v Warshak*, 631 F 3d 266 (6th Cir, 2010). The holding in *Warshak* has not been adopted by appellate courts outside the Sixth Circuit, nor has it been addressed by the Supreme Court, leaving the issue unresolved in the rest of the United States. In practice, however, all major companies based in the United States insist that government agencies obtain a warrant to compel disclosure of content, and it now appears to be the practice of all US law enforcement agencies to do so.

4. 18 U.S.C. SS 2702(a), 2703(c) (2012).

free speech protections. Eventually, after a delay averaging roughly 10 months,[5] the records would be provided to German law enforcement.

One can appreciate the frustration the German police might feel in encountering this cumbersome process. At least two major technology trends contribute to the increased prevalence of such MLAT requests, even for routine local criminal investigations. First, in contrast to traditional paper records, a globalized Internet and pervasive use of cloud technologies mean that records far more often are stored outside the country conducting an investigation. Second, real-time wiretaps on email and other Internet communications are increasingly frustrated because the data flowing between the user and the cloud is often encrypted by default, so a wiretap on the communications link in Germany gathers only encrypted zeros and ones.[6] In short, the once-unusual MLAT request becomes the only means of obtaining records that are encrypted in transit and stored on a cloud server in another country. The once-obscure MLAT process becomes a far more prominent part of global law enforcement investigations. Even more broadly, the impediments that the current MLA system poses to evidence sharing across borders become an argument in favor of localizing evidence, potentially with a large impact on the practice of globalized communications, and implicating governance of the Internet itself.

For all these reasons, there is widespread interest in reforming the MLAT system or developing viable alternatives to it. The following interest analysis should inform that process.

III. THE PERSPECTIVE OF NON-US GOVERNMENTS

We begin by examining the concerns of countries outside of the United States. Non-US governments, which for ease of exposition we call "foreign" governments, face particular frustrations with the current MLAT process, because a great deal of electronic evidence is housed in the United States, which has relatively strict legal requirements for turning over the evidence.

Some steps to address transborder sharing of electronic evidence were taken in the Council of Europe Cybercrime Convention, often called the "Budapest Convention," issued in 2001. The Budapest Convention sought to facilitate international criminal investigations of cybercrimes such as hacking and more broadly to facilitate international cooperation in cases involving electronic evidence.[7] To achieve this, the Convention sought to assure that a lawful basis would exist to transfer evidence between nations, notably by requiring

5. Clark et al., "Report and Recommendations," above note 2.

6. Peter Swire, "From Real-Time Intercepts to Stored Records: Why Encryption Drives the Government to Seek Access to the Cloud," 2 *Intl Data Privacy Law* 200 (November 2012), http://idpl.oxfordjournals.org/content/2/4/200, http://ssrn.com/abstract=2038871.

7. Convention on Cybercrime (entered into force January 7, 2004) CETS No 185, http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.

signatories to cooperate with each other in criminal investigations when seeking to search and seize computers, compel disclosure of data stored in computers, and carry out real-time interceptions in other countries. However, the treaty did not address in any detail the more granular question of ensuring that such cross-border cooperation occurs in a timely fashion.

The example of the German burglary shows that MLAT requests now apply far beyond cybercrimes and can include any traditional local crime with digitized evidence, often stored on a server in another country. To the extent that foreign law enforcement agencies seek to use MLATs, they must learn the unfamiliar and relatively strict substantive US legal standards, such as what a US magistrate will agree is "probable cause" of a crime under the US Fourth Amendment. They must also learn how to overcome procedural obstacles, including how to send a proper request from the correct officials in their own country to the correct officials in the United States.

Compared with gaining evidence from local providers under well-understood local rules, seeking evidence through the MLAT process can thus seem slow, confusing, and burdensome to foreign law enforcement. In response, foreign governments understandably have reason to seek faster access to evidence held in the United States, under procedures that are more streamlined and more transparent to the requesting government. Foreign governments thus would support reforms such as greater funding for OIA to respond to requests and a reduction in bureaucratic obstacles to obtaining the evidence.

These governments also face incentives to take measures to address the technological changes mentioned above—the storage of evidence in other countries and the increased prevalence of encryption. One way to respond to these trends is to enact data localization requirements, such as Russia has done and other countries have considered.[8] In the wake of the Snowden revelations, there are a number of possible motives for such localization requirements, including: (1) concern about how records of their citizens will be treated in the United States; (2) protectionist support for local cloud providers and other technology companies, which would reduce the market share of US providers; and (3) use of localization proposals as a way to highlight concerns about US intelligence activities and to create leverage for possible changes in US policy.[9] In this setting, foreign

8. Natalia Gulyaeva and Maria Sedykh, "Russia Enacts Data Localization Requirement; New Rules Restricting Online Content Come into Effect," *Hogan Lovells Chronicle of Data Protection* (July 18, 2014), http://www.hldataprotection.com/2014/07/articles/international-eu-privacy/russia-enacts-new-online-data-laws/; Federal Law of 27 Jul. 2006 No 152-FZ "On Personal Data" (Russia); Allison Grande, "Brazil Nixes Data Localization Mandate from Internet Bill," *Law360* (March 2014), http://www.law360.com/articles/520198/brazil-nixes-data-localization-mandate-from-internet-bill.

9. All three of these possible motives are implicated in the aftermath of the European Court of Justice decision in *Schrems*, striking down the Safe Harbor. The Court concluded that personal data about Europeans would not be protected adequately in the United States. At the time of writing, there is uncertainty about whether data protection authorities will make similar inadequacy findings about other lawful bases for transferring data, such as model

frustrations with the MLAT process provide an additional rationale for localization initiatives: making the data more readily available to local authorities. We believe there are compelling arguments against data localization of this sort, as explained for instance by President Obama's Review Group on Intelligence and Communications Technologies.[10] Nonetheless, any failure to address MLAT issues can contribute to the incentives that countries have to consider measures to localize evidence for law enforcement purposes.

Non-US governments also could take measures to reduce the effectiveness of encryption used in sending information from their country to servers in the United States or elsewhere. UK prime minister Cameron, for instance, has proposed requiring technology companies to design their products and services to ensure government access to encrypted communications, which might enable wiretaps within the UK rather than requiring access to servers located in other countries.[11] As with localization proposals, there are numerous and compelling reasons to object to such proposals.[12] In addition, as discussed below, effective MLAT reform could provide a useful alternative to mandates against effective encryption.

Even more broadly, problems with MLAT requests could be used as a reason to support changes in Internet governance itself. In general, the United States has promoted an open, interoperable, secure, and reliable information and communication structure. In the debates over Internet governance, to achieve these goals, the United States along with allies such as the European Union has strongly supported an inclusive multi-stakeholder model of Internet governance. As the Review Group wrote:

> A competing model, favored by Russia and a number of other countries, would place Internet governance under the auspices of the United Nations

contracts or Binding Corporate Rules. To the extent lawful bases do not exist or become more difficult to implement, then data localization in the European Union becomes a more important option for businesses. In addition, some writing after the *Schrems* decision, such as by Europe-based cloud providers, has emphasized the business incentives for companies to hire EU-based cloud providers rather than other global providers, which potentially raises issues of protectionist effects after the *Schrems* decision.

10. Clark et al., "Report and Recommendations" (above note 2) 214–16.

11. Rob Price, "David Cameron Is Going to Try and Ban Encryption in Britain," *Business Insider* (July 1, 2015), http://www.businessinsider.com/david-cameron-encryption-backdoors-iphone-whatsapp-2015-7?r=UK&IR=T; James Temperton, "No U-Turn: David Cameron Still Wants to Break Encryption," *Wired* (July 15, 2015), http://www.wired.co.uk/news/archive/2015-07/15/cameron-ban-encryption-u-turn.

12. Going Dark: Encryption, Technology, and the Balance between Public Safety and Privacy: Hearing Before the S Comm on the Judiciary, 114th Cong (2015) (statement of Peter Swire, Huang Professor of Law and Ethics, Scheller College of Business, Georgia Institute of Technology), http://www.judiciary.senate.gov/meetings/going-dark-encryption-technology-and-the-balance-between-public-safety-and-privacy.

> and the International Telecommunications Union (ITU). This model would enhance the influence of governments at the expense of other stakeholders in Internet governance decisions, and it could legitimize greater state control over Internet content and communications.[13]

To the extent non-US governments experience frustrations in obtaining electronic evidence from the United States through MLATs, there is a risk they may shift support to approaches that offer "greater state control over Internet content and communications."

IV. US GOVERNMENT GOALS

As a general matter, with respect to MLA, agencies across the US government share the goal of promoting good relations with other countries by responding quickly and positively where possible to their requests for information. Beyond that, our discussion of US government goals distinguishes between the law enforcement perspective and other governmental goals. Roughly speaking, law enforcement agencies such as the DOJ and FBI have a stake in making law enforcement information sharing more efficient and cost-effective. Other parts of the US government are more concerned with broader economic and diplomatic implications, including reducing other countries' incentives to mandate localization of data. Both sets of goals are shaped by the fact that US-based companies currently provide a large share of online services globally, and consequently hold an important fraction of the world's electronic data within the United States and therefore governed by US law. At least for the near future, the United States is a primary exporter of electronic evidence—many more requests for mutual legal assistance for electronic evidence are made *of* the US government than *by* the US government.[14]

A. Law Enforcement Goals

US law enforcement goals concern: (1) export of electronic evidence, (2) import of electronic evidence, and (3) the role of MLA in addressing encryption. For export of evidence, the US government has treaty obligations to respond to legitimate MLAT requests. In 2013, President Obama's Review Group on Intelligence and Communications Technologies recommended substantial funding increases for OIA to respond to the rising number of MLAT requests. The administration has included such funding in its proposed budgets,[15] but Congress has not yet

13. Clark et al., "Report and Recommendations" (above note 2) 214–15.

14. Factual statements here, such as the position of the United States as a net evidence exporter, are based on the extensive interviews we have conducted to date.

15. Clark et al., "Report and Recommendations" (above note 2) 227.

agreed to the increases.[16] Funding increases, reforming the MLAT process, or both would be a sign that the United States is addressing the MLA problems, and could ease relations with foreign law enforcement partners increasingly frustrated by the inefficiencies of the current process. Ensuring good relations with foreign partners is critical not just for maintaining beneficial relationships in the present, but also for cooperation when US law enforcement seeks to import evidence, as is likely to happen more often as US-based investigations encounter evidence held in other nations.

In ways that have not been widely appreciated to date, MLA reform can also provide a response to the concerns expressed by FBI Director James Comey and others about increasingly prevalent encryption by technology companies.[17] Director Comey has expressed particular concern about encrypted devices such as smartphones. MLA reform would not affect use of that encryption. However, prompt and effective use of MLA would in many cases provide detailed information useful to law enforcement, even if a device is encrypted and communications are encrypted in transit between the user and the cloud. For instance, many smartphone users retain photos, emails, and a vast array of other content to the cloud, where, as of now, service providers can often access the plain text of records when served with a court order. In addition, transborder requests can obtain access to the abundant metadata typically associated with a smartphone, such as the time and duration of calls and location of the phone, which is also available to service providers when served with a court order.[18]

B. Other US Government Goals

Addressing foreign concerns about today's MLA process implicates other important goals of US policy, such as economic growth, the competitiveness of US industry, the protection of free speech and other human rights, and governance of the Internet itself. Localization laws, such as the recent Russian law, affect all

16. HR Rep No 113-448 (2015) 43–44, https://www.congress.gov/congressional-report/113/house-report/448.

17. Going Dark: Encryption, Technology, and the Balance between Public Safety and Privacy: Hearing Before the S Comm on the Judiciary, 114th Cong (2015) (statement of James Comey, Director, Fed Bureau of Investigation), http://www.judiciary.senate.gov/meetings/going-dark-encryption-technology-and-the-balance-between-public-safety-and-privacy. For one response to Comey's concerns, see Going Dark: Encryption, Technology, and the Balance between Public Safety and Privacy: Hearing Before the S Comm on the Judiciary, 114th Cong (2015) (statement of Peter Swire, Huang Professor of Law and Ethics, Scheller College of Business, Georgia Institute of Technology), http://www.judiciary.senate.gov/meetings/going-dark-encryption-technology-and-the-balance-between-public-safety-and-privacy.

18. Nicholas Weaver, "iPhones, the FBI, and Going Dark," *Lawfare* (August 4, 2015), https://www.lawfareblog.com/iphones-fbi-and-going-dark.

of these goals.[19] These laws can serve as a protectionist barrier to trade, creating an economic burden on technology companies, such as requiring them to spend resources to create expensive new server facilities or making it too expensive to enter a foreign market. Localization rules create security risks, as company-managed flows of data come under the supervision of national authorities who may themselves conduct surveillance on those records, or may access records and not retain them in a secure fashion. They also can reduce human rights protections, when the country with the localization laws can access all data, in contrast to the screening done by the US Department of Justice to ensure protection of free speech and other human rights when responding to MLA requests.

For countries that object to strict rules concerning access to data in the United States, frustration with the MLA process can also be used as a rationale for shifting power to the International Telecommunications Union or some other mechanism for legally requiring greater access. The US government has opposed such proposals, believing instead that top-down Internet governance by nation-states would threaten the "open, interoperable, secure, and reliable information and communications infrastructure that supports international trade and commerce, strengthens international security, and fosters free expression and innovation."[20]

V. GOALS OF TECHNOLOGY COMPANIES

The companies most involved in current MLA debates are US-based email, social network, and other companies that provide online consumer services in numerous countries.[21] These companies have been driving the two trends affecting the current MLAT process: the offering of services in one country with the data being stored on cloud servers in another country (often the United States) and expanding the use of encryption for communications that previously were subject to local wiretaps.

The views of these companies with relation to MLA are complex, because multiple goals of these companies and their employees are affected. For instance, the companies wish to provide high-quality services to customers. While doing so, leaders of these companies have a sincere belief in fostering human rights and protecting free speech on the Internet; they also have a sincere desire to cooperate with lawful requests for prosecution of dangerous criminals. Based on extensive interviews, we have identified six goals, which we present here in order of

19. Gulyaeva and Sedykh, "Russia" (above note 8); Federal Law of 27 July 2006 No 152-FZ "On Personal Data" (Russia); Grande, "Brazil" (above note 8).

20. White House, International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World (May 2011).

21. As noted in the initial footnote, funding for our ongoing research comes in part from technology companies as well as foundation funding, all of whom have provided such funding in order to advance research and reform on these issues but without overseeing the content of our writing. The views expressed here are solely those of the authors.

expositional clarity, and not from most to least important: (1) avoiding conflicting legal rules, (2) opposing data localization requirements, (3) cooperating with appropriate requests from law enforcement, (4) acting consistently with human rights goals, (5) retaining access to as many markets as feasible, and (6) developing practices that enhance the company's reputation, especially for trustworthy stewardship of emails, social networking, and other records.

A first concern is to avoid conflicting legal rules, notably where the United States prohibits release of records under the Electronic Communications Privacy Act but another country requires release of those same records. Companies have faced credible threats from foreign countries that local employees would be jailed or otherwise punished if the company did not comply with local demands for evidence. Companies, facing these threats, understandably would like to support an MLA system that provides clear rules for when records should be produced, in ways that comply with the laws of all relevant countries.

A second understandable concern of global technology companies is to minimize the burdens they face from data localization laws. The United Nations has nearly two hundred Member States.[22] By contrast, Google lists 14 data centers as of September 2015,[23] and a single Microsoft data center in Virginia cost $1 billion.[24] The mismatch between number of countries and number of data centers led the Review Group to write: "Global inter-operability has been a fundamental technical feature of the Internet; bits flow from one user to the next based on technical considerations rather than national boundaries. National efforts to tamper with this architecture would require pervasive technical changes and be costly in economic terms."[25]

Third, companies would like to comply with legitimate law enforcement records requests, for reasons including the business benefits of cooperating with governments as well as a sincere desire to assist in deterring and punishing criminal conduct. Major technology companies today employ former prosecutors and law enforcement agents, who often have special sympathy for and insight about the law enforcement mission.

Fourth, the reasons to assist each nation's law enforcement, by providing ready access to records, can be in tension with the companies' desire to act consistently with human rights goals such as promotion of privacy, democracy, and free speech. Google, Microsoft, and Yahoo! were the founding corporate members of the Global Network Initiative, dedicated to "protecting and advancing freedom

22. United Nations Members States, United Nations http://www.un.org/en/members/.

23. Data Center Locations, Google http://www.google.com/about/datacenters/inside/locations/index.html.

24. Rich Miller, "Microsoft's $1 Billion Data Center," *Data Center Knowledge* (January 31, 2013), http://www.datacenterknowledge.com/archives/2013/01/31/microsofts-1-billion-roofless-data-center/.

25. Clark et al., "Report and Recommendations" (above note 2) 223.

of expression and privacy in information and communication technologies."[26] Such companies, and many people employed by them, have strong ties to civil society organizations in the Digital Due Process Coalition, which supports stricter rules for US government access to records under ECPA.[27]

Fifth, the companies for business reasons would like to retain access to as many national markets as feasible. The business benefits of expanding to all countries are balanced by the risks of doing business in certain markets, such as potential punishments of employees if records are not produced from the United States, employees' opposition to support for dictators or violations of human rights, and reputational harm resulting from any such support. An improved MLA system would clarify which nations are following procedures consistent with a company's policies about which national markets to participate in.

Sixth, in the post-Snowden era, major companies wish to assure customers that the companies will provide trustworthy stewardship of communications. Both within and outside of the United States, the companies have an incentive to demonstrate that use of their services is not tantamount to providing access to the NSA. Clarity in the MLA process helps the companies show that they comply with appropriate requests for government access, but that consumers can fundamentally expect careful handling of communication records.

Smaller companies also face negative consequences from localization requirements. Such firms lack the economies of scale to construct multiple data centers and face obstacles to competing with local companies while paying the costs of relying on local data centers. Although smaller companies could choose not to comply with data localization laws, doing so would require them to hold no assets in a territory with a data localization law, and employees traveling to those territories could face the risk of arrest.[28]

In sum, these six goals show the complex considerations that major technology companies face with respect to MLAT reform. Reconciling these considerations will by no means be a simple task, but clarifying the multiple goals will assist in crafting a thoughtful and sustainable overall strategy.

VI. GOALS OF CIVIL SOCIETY

Civil society groups support international institutions, including MLATs, that protect privacy and free speech, and promote democracy and democratic dissent.

26. *Core Commitments*, Global Network Initiative http://www.globalnetworkinitiative.org/corecommitments/index.php.

27. *About the Issue*, Digital Due Process https://digitalddueprocess.org/about-the-issue/.

28. Notably, previous Russian data protection legislation has specifically applied only to businesses with a legal presence in Russia and that process personal data on Russian soil. It has not yet been determined whether the same limits will apply to the data localization law, but if they do then smaller companies would only need to comply with the law if they sought to open operations within Russia. Gulyaeva and Sedykh, "Russia" (above note 8).

The current system already has many positive features from the civil society perspective, and reforms might result in an even more positive system. On the other hand, civil society groups may differ in the priorities they set on protections that apply in the United States, in Europe and other democratic countries, and in repressive regimes. Failure to update the MLAT process also risks data localization and other measures that could strengthen the position of non-democratic governments in Internet governance.

The positive features of the current MLA system derive from the strong US protections for both privacy and free speech. Under current law, foreign governments seeking communications stored in the United States generally must show probable cause of a crime, as found by a neutral US magistrate, before the contents of those communications can be shared to the requesting country. In contrast to other areas of privacy law, the United States is often stricter than European and other countries when it comes to the standard for law enforcement access to communications data.[29] In addition, before sending evidence to the requesting country, OIA reviews communications to ensure compliance with the First Amendment, which is an important protection for free speech and democratic dissent. A broad array of civil society groups in general favor these sorts of privacy and free speech protections.

Civil society groups may have somewhat different priorities in the MLA reform process, depending on the extent to which they focus on the rules that apply in the United States, in making disclosures to Europe and other democratic countries, and when information is shared with repressive regimes. US-based groups have supported stricter standards for US government access to communications information, some of which were enacted in 2015 in the USA Freedom Act, which among other provisions created new privacy protections limiting bulk collection for foreign intelligence purposes.[30] US-based civil society groups hope to achieve comparable reform for law enforcement purposes under ECPA, most prominently through the campaign of the Digital Due Process Coalition. In summary, the Coalition seeks: (1) communication contents and location information only with a probable cause warrant, (2) to/from and other metadata under stricter standards than today, and (3) no bulk collection by subpoena.[31] These reforms would heighten the standards within the United States for law enforcement access.

29. One part of our research project on MLATs is to explore how the relatively strict US approach to transborder flows for law enforcement intersects with the relatively strict EU approach to other transborder data flows, as shown in the 2015 decision striking down the EU/US Safe Harbor. We are researching a forthcoming article for the *Emory Law Journal* that addresses that subject.

30. Peter Swire, "The USA FREEDOM Act, the President's Review Group and the Biggest Intelligence Reform in 40 Years," *IAPP Privacy Perspectives* (June 8, 2015), https://iapp.org/news/a/the-usa-freedom-act-the-presidents-review-group-and-the-biggest-intelligence-reform-in-40-years.

31. *Our Principles*, Digital Due Process https://digitaldueprocess.org/our-principles/.

EU civil society groups have reason to place a priority on the protections that apply to communications made in or from the EU. For these groups, the MLA process presents an opportunity to advocate for stricter rules for access in EU countries. For instance, EU groups could favor having the United States stand firm on the requirement for a neutral magistrate, as a way to push for a judicial role for access requests in the EU.

In considering MLAT reform, civil society groups focused on protecting human rights in repressive regimes have a similar incentive to favor maintaining the current US rules. Notably, the free speech protections in current US law generally bar release of evidence from the United States for "political" crimes that constitute protected speech under the US First Amendment. These groups would be wary of any proposal that reduced the US Department of Justice scrutiny of evidence under the First Amendment.

Possible tensions could exist among these priorities of different civil society groups. For instance, consider the example of the German burglary, with German suspects, but with evidence in the United States. Some reform proposals would apply German law to such requests, so that US companies could provide the evidence under German procedural rules, even where ECPA would otherwise require a probable cause warrant. That approach could be disappointing for EU-based civil society groups, because of the lost opportunity for strengthening EU law. The approach, however, might be more tempting for US-based civil society groups if it were part of a package that created other reforms supported by the Digital Due Process Coalition. This example is not given to take a position on such a reform proposal; instead, the point is that different civil society groups may understandably have different priorities, while generally wishing to strengthen civil liberties protections.

As with other reform efforts, civil society groups can face trade-offs among multiple goals. One goal is to strengthen the standards for law enforcement, such as the Digital Due Process Coalition proposals would do. Another goal is to maintain an open Internet, including skepticism about data localization and a large role for the International Telecommunications Union. ECPA reform would enhance privacy by raising the standards for US government access to records, as well as the standards that non-US requests would have to meet. ECPA reform would also be a model for other nations to follow, and the desire to use MLA to gain evidence could create leverage to encourage other nations to level up to the US procedural standards. On the other hand, stricter US standards for MLA could backfire. If MLA becomes even more unworkable, then non-US countries have stronger reasons to consider localization proposals or other measures to gain records without recourse to the rule-of-law MLA process. More nations could similarly be tempted to look to the ITU or other Internet governance arrangements that grant greater sovereignty to each nation, if such reforms helped nations gain access to the evidence they seek. In short, civil society organizations thus face strategic choices about how to pursue both the US law reform agenda as well as measures that will protect privacy, free speech, and democratic dissent outside of the United States.

VII. CONCLUSION

This chapter, based on extensive interviews to date with relevant stakeholders, has sought to articulate the goals of major stakeholders in the MLAT process. This sort of realistic assessment of the major actors is an essential step, we believe, toward designing and achieving significant reform of the MLAT process.

22

From Real-Time Intercepts to Stored Records

Why Encryption Drives the Government to Seek Access to the Cloud

PETER SWIRE

I. ABSTRACT

This chapter complements the country-by-country chapters for The Privacy Project's initiative on Systematic Government Access to Private-Sector Data. This chapter describes technological changes that shift law enforcement and national security attention from traditional wiretap techniques to greater emphasis on access to stored records, particularly records stored in the cloud.

The major and growing reliance on surveillance access to stored records results from the following changes:

(1) Encryption. Adoption of strong encryption is becoming much more common for data and voice communications, via virtual private networks, encrypted webmail, SSL web sessions, and encrypted Voice over IP voice communications.
(2) Declining effectiveness of traditional wiretaps. Traditional wiretap techniques at the ISP or local telephone network increasingly encounter these encrypted communications, blocking the effectiveness of the traditional techniques.
(3) New importance of the cloud. Government access to communications thus increasingly relies on a new and limited set of methods, notably featuring access to stored records in the cloud.
(4) The "haves" and "have-nots." The first three changes create a new division between the "haves" and "have-nots" when it comes to government access to communications. The "have-nots" become

Bulk Collection. Fred H. Cate and James X. Dempsey.

increasingly dependent, for access to communications, on cooperation from the "have" jurisdictions.

This chapter explains how changing technology, especially the rising adoption of encryption, is shifting law enforcement and national security lawful access to far greater emphasis on stored records, notably records stored in the cloud. Section II describes the changing technology of wiretaps and government access. Section III documents the growing adoption of strong encryption in a wide and growing range of settings of interest to government agencies. Section IV explains how these technological trends create a major shift from real-time intercepts to stored records, especially in the cloud.

II. THE CHANGING TECHNOLOGY OF WIRETAPS AND GOVERNMENT ACCESS

This section of the chapter provides a brief history of wiretap technology. The history reveals two themes: (1) a shift in the place of interception from the local to the remote, and (2) a shift from "voice" wiretaps in real time to "data" access to stored Internet records. Taken together, this history shows a shift in how government accesses records, with a far greater emphasis today on access to records stored remotely.

Figure 22.1 shows the traditional wiretap of a copper phone line. In the Figure, Alice is calling Bob. For a copper wire, the technology of a wiretap is quite simple—touch another copper wire to the phone line, and induction makes it possible to listen to the call. This wiretap might take place near Alice's (or Bob's) house, such as if a police officer tapped the phone line near the house. It could also take place at the telephone company's central office, where the officer could similarly implement a wiretap.

By the early 1990s, however, many phone lines were shifting from copper to fiber optics. Copper touching a copper wire is satisfying for the wiretapper—the police officer can listen to the call. Glass touching glass is distinctly unsatisfying—no current passes from glass to glass, and no sound emerges. Along with changes in telephone switches, this shift from copper wire to digital telephony was an important justification for passage in the United States in 1994 of the Communications Assistance for Law Enforcement Act (CALEA).[1] A core requirement of CALEA was that telecommunications carriers and manufacturers of telecommunications equipment design their products and services to ensure that they could carry out a lawful order to provide government access to communications. The Department of Justice and Federal Communications Commissioner were given important powers to assess whether products and services complied with the CALEA requirements.

1. Communications Assistance for Law Enforcement Act, 47 U.S.C. §§ 1001–1010 (2012) (CALEA).

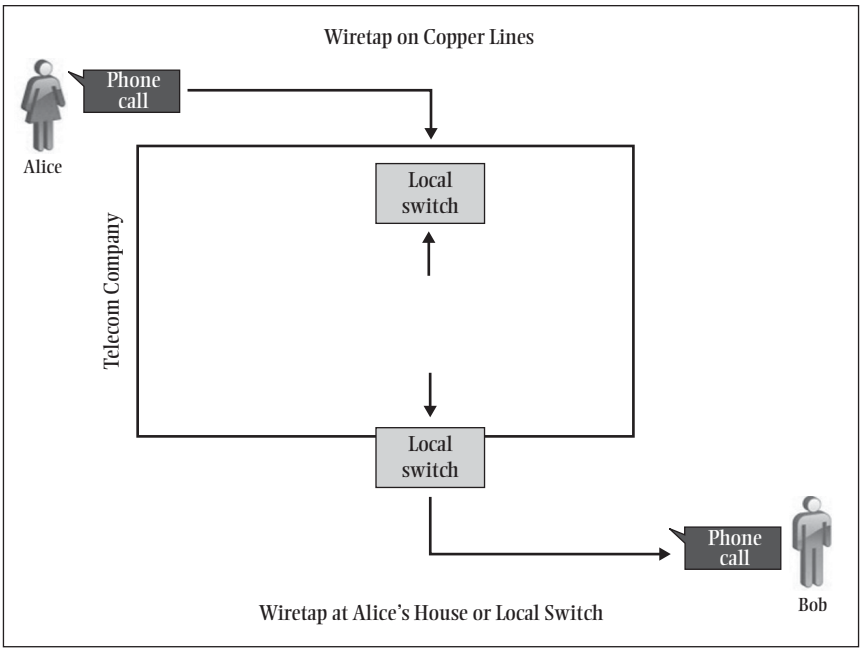

Figure 22.1 Wiretap of a copper phone line.

In Figure 22.2, Alice once again calls Bob. Even if Alice has fiber optic to the home, the telephone company is required to design its system so that lawful access is available at the switch. For mobile telephone calls, there may be encryption between Alice and the cell tower, but the telephone company has to be able to carry out a lawful access order at the cell tower or elsewhere in its network. The emphasis on access at the switch or cell tower is a step from the local to the remote. The wiretap no longer occurs next to Alice's house; instead, the wiretap typically occurs at a switch in a digital network. This change puts the fruits of the wiretap closer to the center of the network—an interception at the central switch likely can be sent easily to a centralized location for the law enforcement or national intelligence agency.

CALEA as enacted in 1994 made an important distinction between "telecommunication services," which are covered by the law, and other "information services," which are not.[2] CALEA clearly applied to the traditional voice calls made over a public switched telephone network. By contrast, CALEA did not apply to the nascent use of data sent over the Internet. The first commercial activity over the Internet was permitted only in late 1992.[3] Thus, the meteoric rise of the Internet occurred after CALEA was drafted, and the

2. CALEA, 47 U.S.C. § 1001 (2012).

3. Peter P. Swire, "Trustwrap: The Importance of Legal Rules to Electronic Commerce and Internet Privacy," (2003) 54 *Hastings LJ* 848, 860 n.33.

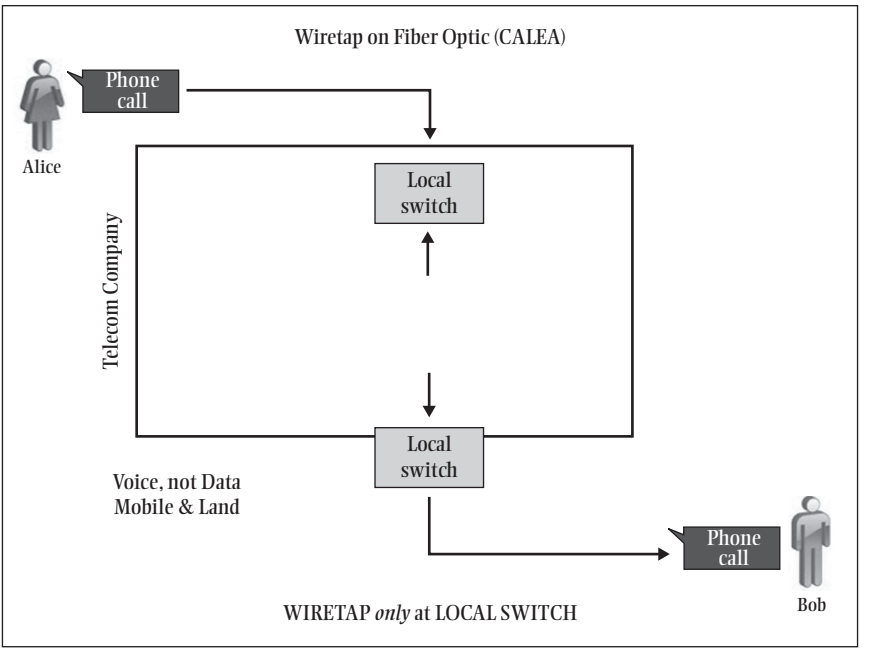

Figure 22.2 Wiretap on a fiber optic network after CALEA.

Internet was left unregulated by the CALEA requirements to design products and services as wiretap ready. In a 2005 order by the Federal Communications Commission, CALEA was interpreted to apply to Voice over Internet Protocol (VoIP) providers who connect calls to the public switched telephone network.[4]

As shown in Figure 22.2, CALEA applied to the traditional phone network, which had one or a few dominant telephone companies in most countries. The rise of the Internet, however, placed an enormous number of different entities in the communication path from Alice to Bob. Figure 22.3 shows that, as Alice's packets go from Alice to Bob, a large and unknown set of actors are potentially in the position to store those packets and read them. Some of these actors are actually or potentially malicious, from amateur hackers through organized crime groups to hostile nation-states. The operators of numerous other nodes have weak cybersecurity, so that malicious parties can create "bots" under their remote control, or can gain root access to servers and thus send data back to the intruding party.

The fundamental insecurity of the intervening nodes was well known in the 1990s, and was a key technical reason in favor of strong encryption for Internet communications. The "crypto wars" of the 1990s resulted from the tension between (1) this technical need for strong communications security, and (2) the opposing concern of law enforcement and national security agencies that strong

4. The official press release for the Order is http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-260434A1.pdf.

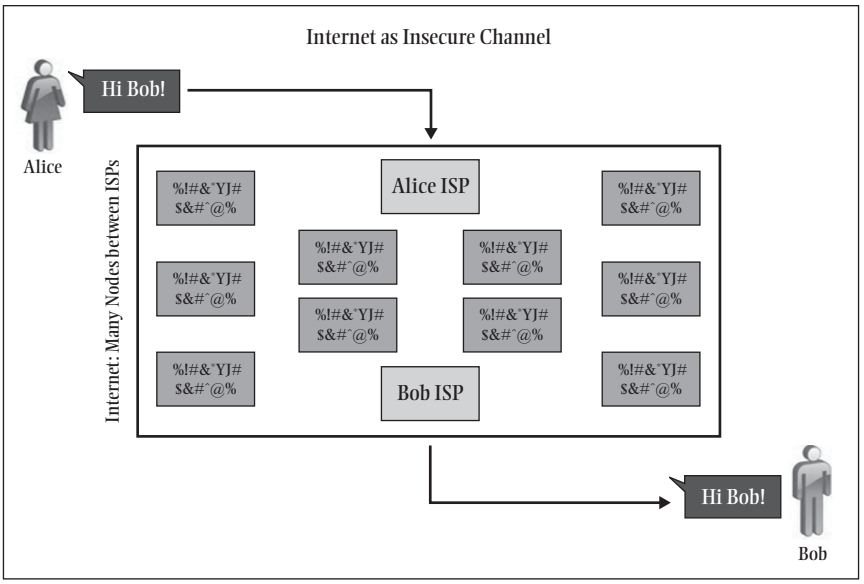

Figure 22.3 Many intervening nodes in Internet communications.

encryption would block access to data, a problem that has since become known as "going dark."[5] In 1999, the US government shifted its position, and permitted the export of strong encryption to most countries and for most purposes.[6]

III. THE GROWING ADOPTION OF STRONG ENCRYPTION

Although export of strong encryption from the United States became generally legal in 1999, actual adoption was lower than expected for email and other Internet actions. After all, few of us make a conscious decision to use an encryption program as part of sending and receiving email. Despite this previously low adoption, a major point of this chapter is that effective encryption is in the midst of becoming the default way that many communications occur on the Internet.

Figure 22.4 illustrates the effect of strong encryption on lawful access at an Internet Service Provider or in the other nodes of the Internet between Alice and Bob. In the diagram, Alice wraps her message in Bob's "public key." This public key is a long set of numbers that Bob posts publicly, to enable anyone to send a message to him. The message is thus encrypted all the way between Alice and Bob. At Bob's end, he deploys his "private key," known only to him, to return the encrypted communication to plain text.

5. Peter Swire and Kenesa Ahmad, "'Going Dark' versus a 'Golden Age of Surveillance,'" *CDT Blog* (November 28, 2011), https://cdt.org/blog/%E2%80%98going-dark%E2%80%99-versus-a-%E2%80%98golden-age-for-surveillance%E2%80%99/.

6. The White House announcement of this policy is http://intellit.muskingum.edu/cryptography_folder/encryption2.htm.

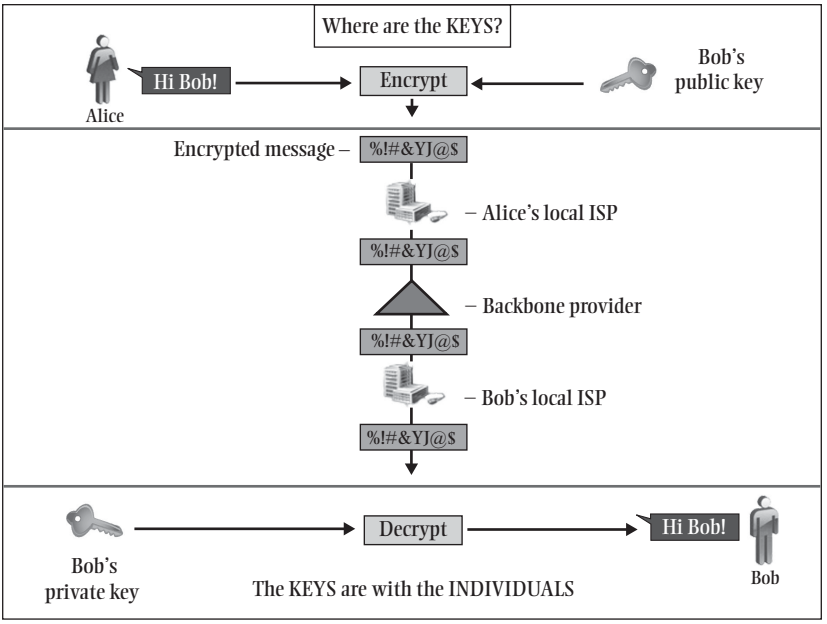

Figure 22.4 Encryption and Internet communications.

This encryption by Alice and Bob limits the usefulness of a lawful access order implemented at Alice or Bob's Internet Service Provider (ISP), or at any node in the Internet between Alice and Bob. The reason is simple—the order may capture the bits of Alice's message, but those bits are strongly encrypted. The lawful order does not give the government agency access to the content of the communication, unless special circumstances exist (e.g., use of weak encryption or government knowledge of Bob's private key).

For today's Internet, one variation is worth noting. Major webmail providers, including Gmail and Hotmail, now automatically encrypt emails from Alice to Bob. A lawful order at the ISP level thus sees only encrypted, unreadable ones and zeros. However, and central to the emerging strategies for lawful access, emails saved by Alice or Bob on the webmail's servers are not strongly encrypted. Instead, by default the server owner retains the technical ability to read the plain text of the emails. A lawful access order to the server owner (often referred to as a "cloud provider") can successfully compel disclosure of the email content.

The shift to encryption for major webmail providers, all by itself, substantially reduces the effectiveness of a lawful access order to an ISP. This shift occurs in the context of other widespread adoption of effective encryption:

- Corporate and government users have widely adopted Virtual Private Networks (VPNs) for remote users. VPNs are strongly encrypted, thus protecting the organization's emails and other communications.

- Electronic commerce, including credit card numbers, is overwhelmingly conducted today using SSL (Secure Sockets Layer).
- Facebook now supports SSL. If it enables SSL by default, then its social networking communications would not be readable at the ISP level.
- Research in Motion's Blackberry products use strong encryption, and RIM itself does not have the keys for corporations who manage keys themselves.
- Major web locker services, such as Dropbox, use SSL by default.
- Skype, the leading VoIP provider, encrypts end-to-end. Many international calls are made using Skype. VoIP enables voice communications to be encrypted at scale.
- Many Internet games and other services use encryption, often with accompanying voice and chat channels.

Taken together, these changes indicate that widespread encryption adoption is well underway for email and voice communications. This shift brings greater cybersecurity, greatly reducing the risk that the millions of nodes of the Internet can be used to read the content of communications. The shift also means that government agencies will be far less likely in the future to be able to intercept the content of communications at the local ISP or telephone company.

IV. WHY THESE TECHNOLOGY TRENDS RESULT IN GREATER FOCUS ON CLOUD PROVIDERS

The widespread adoption of encryption for communications affects the choices for government agencies seeking lawful access. Logically, there are four ways for agencies to access communications:

1. Break encryption in transit.
2. Intercept before or after encryption.
3. Assure access in unencrypted form.
4. Access after the fact, in stored form, often in the cloud.

A major descriptive conclusion of this chapter is that a wide range of law enforcement and national security agencies will face large or insuperable obstacles to the first three methods. These agencies will thus increasingly depend on access to stored records, notably those stored in the cloud.

A. Break Encryption in Transit

By definition, "strong" encryption means that it is extremely difficult for government agencies or others to get the plain text of encrypted communications.[7]

7. For discussion of current technical, legal, and policy issues on encryption, see Peter Swire and Kenesa Ahmad, "Encryption and Globalization," 13 *Colum Sci & Tech L Rev* 416 (2012), http://ssrn.com/abstract=1960602.

For an unbroken encryption algorithm, attackers must use a brute force attack, trying each possible key until the plain text is revealed. A higher key length exponentially increases the average number of calculations needed on average to decrypt a communication. Today, users of encryption can simply increase the key length to make brute force attacks ever more difficult.

After the United States permitted export of strong encryption in 1999, routine commercial deployment of encryption became unbreakable, as a practical matter, for most law enforcement and national security agencies. Academic cryptographers constantly test for flaws in widely-used cryptosystems, and publish known attacks. This constant and public testing of cryptosystems means that flaws become widely known.

As with other methods of access, it is possible that there are "haves" when it comes to breaking encrypted messages.[8] One recent publication claimed that the US National Security Agency has made a significant breakthrough against the globally used Advanced Encryption Standard.[9] Without access to classified information, it is not possible to assess this claim, or the extent of any such breakthrough. This sort of breakthrough, however, is at most available to a tiny subset of all law enforcement and national security agencies that may wish to gain lawful access to communications. For the rest, breaking modern encryption is not feasible.

B. Intercept before or after Encryption

If it is too difficult to break an encrypted message, then government agencies may try to get access to real-time communications before or after they are encrypted. One way to do this is by physically entering a person's home or business, and installing a bug or other surveillance device. Such a physical entry may be used in high-priority cases, but it is risky and costly for government agencies to insert such devices often.

An approach with less risk of an agent being caught would be for the government agency to hack into the target's computer remotely. The large size and number of "bot farms" and other compromised computers suggests that an appreciable fraction of computers may be open to such attacks. According to one estimate, at least 6 percent of the world's 4 billion IP addresses are part of a zombie network,[10] and another expert estimates that the top four botnets alone control over 20 million computers.[11]

8. My thanks to Chris Soghoian for his insights on the effects on the "haves" and "have nots."

9. James Bamford, "Inside the Matrix," *Wired* (March 15, 2012), http://www.wired.com/threatlevel/2012/03/ff_nsadatacenter/.

10. Mark Clayton, "Biggest-Ever Criminal Botnet Links Computers in More than 172 Countries," *Christian Science Monitor* (June 29, 2011), http://www.csmonitor.com/USA/2011/0629/Biggest-ever-criminal-botnet-links-computers-in-more-than-172-countries.

11. "Major Botnets Have Infected over 20 Million Computers, Says Kaspersky," *Infosecurity Magazine* (September 27, 2011), http://www.infosecurity-magazine.com/view/20986/major-botnets-have-infected-over-20-million-computers-says-kaspersky/.

The adoption of strong encryption creates a motive for government agencies to break into a target's computer before or after encryption. The large number of vulnerable computers creates an opportunity for such entry. Press reports of an FBI "computer and internet protocol address verifier," placed remotely on a user's computer, provide evidence that these sorts of software break-ins have occurred in at least some instances.[12] Sophisticated government agencies may thus employ this strategy in high-priority cases.

There are nonetheless important reasons to believe that hacking into targets' computers is not and will not be a major strategy for lawful access. First, this sort of secret and routine access, into users' actual computers, is unlikely to remain secret over time. Second, the legal infrastructure for this sort of government hacking is uncertain or nonexistent in many jurisdictions. Third, the growing recognition of the importance of cybersecurity creates strong policy reasons to improve computer security, rather than rely on weak security for lawful access.[13]

C. Assure Access in Unencrypted Form

Another route for lawful access is for the law to mandate a communications infrastructure that assists lawful interception. As discussed above, CALEA is a prominent example, requiring that telecommunications products and services in the United States be wiretap-ready. Similar rules exist under the Regulation of Investigatory Powers Act of 2000 in the United Kingdom, and Canada is now considering similar legislation. The analysis here suggests that such laws may remain an important source of lawful access in some settings, but are unlikely to succeed for many types of communications of interest to government agencies.

For landline telephone calls, CALEA means that telephone calls can be accessed "in the clear" (unencrypted) at the switch. For wireless calls, there typically is encryption from the handset to the tower, and the telephone company decrypts the call at the tower or elsewhere so that the wiretap can operate. The handsets themselves must comply with CALEA as well. CALEA is thus an example of an architectural rule—the telecommunications architecture is created in a manner that enables lawful access to the telephone call.

Going forward, a key question is the scope of this architectural rule as communications shift from the traditional telephone network to the Internet. Telephony has historically covered a small number of large, regulated companies, and a tiny fraction of telephone equipment has used strong encryption that would frustrate a wiretap. Implementation of CALEA even in this environment took a number of years and included contentious court suits. Yet it is relatively

12. Kevin Poulsen, "FBI's Secret Spyware Tracks Down Teen Who Made Bomb Threats," *Wired* (July 18, 2007), http://www.wired.com/politics/law/news/2007/07/fbi_spyware?currentPage=all.

13. Swire and Ahmad, "Encryption and Globalization," (above note 7) (discussing relation between cybersecurity and encryption).

easy to enforce CALEA in this setting of a few companies, experienced with regulators, and with little encryption.

The Internet, by contrast, features a large and shifting array of (often unregulated) information services providers, not just for VoIP but for a burgeoning array of text, audio, and video services. And the computers, game console, and other products that use these services are also incredibly diverse. Requiring "wiretap readiness" for all of these products and services would be considerably more difficult than for traditional telephony, given the diversity of products and services, the lack of regulatory experience among many of the actors, and the widespread use of encryption in many Internet activities.

A popular online video game such as World of Warcraft (WoW) illustrates the different perspectives of government agencies and Internet users. To players of WoW (such as my sons), WOW is a fun game. They often wear headsets to talk with teammates while playing, and keep a chat window scrolling as well. To law enforcement, WoW (or any other similar game) can seem instead to be a global terrorist communications network. Players can talk and send chat messages, internationally, outside of the traditional telephone network and outside of the scope of CALEA. The architecture is based on what works for the game, and not what facilitates lawful access.

To summarize on this architectural approach, government agencies will face a number of practical obstacles in attempts to require "in the clear" communications over the Internet. The fundamentally insecure nature of the Internet (as shown in Figure 22.3, above) means that effective encryption is vastly more common and more important for Internet services than for traditional telephone services. Even when government agencies temporarily learn how to gain access to a particular product or service, the rate of innovation on the Internet remains high—when a new game or a new version of a game is issued, the access that worked previously may no longer succeed. At a minimum, the complexity and innovation on the Internet will likely cause further separation between "have" and "have not" agencies, with far greater ability to adapt for leading national agencies than for local police departments or agencies in poorer countries.

D. Access after the Fact, in Stored Form, Often in the Cloud

The discussion thus far has highlighted new obstacles in the path of access to communications at the local ISP or telephone company. Where strong encryption is used, then attempts at such access will produce random ones and zeros rather than the contents of the communication. The widespread use of encryption is spreading from VPNs to standard webmail, social networks, and VoIP such as Skype.

When local attempts to access fail, then government agencies have a strong incentive to turn to the system owners, such as the operators of webmail or VoIP. Most emails using Gmail or Hotmail are unencrypted at the server level, so government agencies around the world have reason to seek access from Google and Microsoft. Similarly, because Skype interconnects with the traditional telephone

network, it is required to be wiretap-ready under the 2005 FCC CALEA order, and agencies have reason to come to that company for access.

Beyond webmail and VoIP, the widespread use of encryption for e-commerce, banking, and other Internet communications means that a vast range of data is generally accessible from a party to the communication (such as a bank or e-commerce company) but not from wiretaps in transit. The bank or e-commerce company generally needs to be able to store and read the information in the clear. Even if the company encrypts its own databases, it will have the keys, so lawful access will not be blocked due to that encryption.

Encryption at the cloud may block lawful access in some other settings. For instance, a locker or cloud provider might enable storage of email and other content in encrypted form, with the keys held only by the client of the locker or cloud service. In such instances, access to the locker or cloud service will not enable the agency to read the content. The prevalence of this sort of encrypted storage is unclear, but at least two reasons suggest it is not now, nor will it soon be, a general barrier to lawful access. First, there are significant technical challenges for efficient search and retrieval of encrypted data.[14] There are thus business and functional reasons not to store all data in encrypted form. Second, it is extremely risky for users to store data in the cloud without having a backup of the keys—loss of the keys will irretrievably lose access to the data. For that reason, cloud providers (who wish to provide assured access to the data) have a strong business reason to provide key backup.

At a practical level, then, cloud providers and commercial parties to a transaction very often have access to the contents of communications and transactions. It will thus very often be technically possible for the companies to respond to lawful access requests.

This technical possibility to respond to process leads an important, specific split between the "haves" and "have nots." Some jurisdictions will have the cloud server in their jurisdiction, with relatively straightforward access to the stored records under local law. Other jurisdictions will not have such access. They will have to use a Mutual Legal Assistance Treaty (MLAT) or other mechanism to gain access to the holder of the records. These "have not" jurisdictions may well face added expense and delay in gaining access to the records. In some (or perhaps many) cases they will not be able to access records that they consider important for law enforcement or national security purposes. Conversely, cloud providers and other holders of records are likely to face an increasing number of lawful access requests, from a potentially bewildering array of jurisdictions.

14. See, for example, Huang Yongfeng, Zhang Jiuling, and Li Xing, "Encrypted Storage and Retrieval in Cloud Storage Applications," [2010] 4 *ZTE Communications*, http://wwwen.zte.com.cn/endata/magazine/ztecommunications/2010Year/no4/articles/201012/t20101220_197082.html.

V. CONCLUSION

The focus of this chapter is to describe the effect of technical changes on likely paths for lawful access to communications information. This chapter does not propose how best to resolve legal issues, including the complex multi-jurisdictional issues that will occur increasingly often. An improved understanding of the technology, however, can help clarify what legal and practical options may exist going forward.

PART THREE

Conclusion

23

Recommendations for Government and Industry

JAMES X. DEMPSEY AND FRED H. CATE

I. ABSTRACT

The chapters in this volume represent a diversity of voices from around the world, but they are uniform in their commitment to the proposition that terrorism can be effectively fought and national security interests can be defended within a system of oversight and control that protects both corporate interests and individual privacy. Moreover, they are remarkable in their consistency in describing the components of an effective system of checks and balances. It turns out, when it comes to government surveillance, the tools of control and accountability are already known. They are just not comprehensively applied. This chapter draws on the work of the contributors to this volume and on the flood of court opinions, legislative enactments, official reports, academic writings, corporate developments, and NGO advocacy over the past five years, to recommend a coherent framework for the collection of private-sector data. For governments, the elements of this framework can be summarized in three key concepts: legality, proportionality, and accountability. For corporations, they are based on adoption of internal policies, internal and external accountability, and transparency, backed up by a willingness to challenge overbroad or unjustified government demands. The elements of this framework are drawn from long-accepted principles of the rule of law, human rights, and democratic governance. Some of them have even been applied for decades, in at least some democratic countries, to intelligence and national security surveillance. The one new recommendation that emerges from our study, however, is a strong rejection of bulk collection.

Bulk Collection. Fred H. Cate and James X. Dempsey.

II. INTRODUCTION

When we began this project in 2011, our initial research identified various examples of "systematic access" in a wide range of countries, but it also found a general lack of transparency about the nature of, and legal basis for, data collection practices carried out in the name of national security or foreign intelligence.

Beginning in June 2013, unauthorized and authorized disclosures of intelligence programs in the United States, the UK, and some other European countries partly lifted the shroud of secrecy, at least with respect to some countries. "Bulk surveillance" came to be featured prominently in national and international debates over governmental power, corporate responsibility and individual privacy. Although much of the commentary was exaggerated or misleading, it is undeniable that the disclosures confirmed our core concerns about expansive and lightly regulated government demands for access to data held (or transmitted) by the private sector.

In the ensuing years, there have been a number of remarkable developments:

- The president of the United States issued a directive expressly stating that the United States would respect the privacy rights of all persons "regardless of their nationality or wherever they might reside" and placed limits on the retention and use of signals intelligence collected in bulk by US agencies.[1]
- The US Congress adopted legislation, signed by the president, that ended a domestic program that had compelled telephone companies to turn over call detail records in bulk. The legislation amended several statutes to make it clear that they could not be used to authorize bulk collection in the future.[2]
- The US legislation also introduced the possibility of appointing independent advocates to participate in the proceedings of the secret Foreign Intelligence Surveillance Court, which had previously examined programmatic surveillance demands based on the filings and arguments of only the government.[3]

1. Presidential Policy Directive/PPD-28, "Signals Intelligence Activities" (January 17, 2014).

2. USA FREEDOM Act, Pub. L. 114-23 (June 2, 2015). In addition to amending Section 215 of the PATRIOT Act to prohibit is use for bulk collection, the Act also amended various provisions authorizing issuance of National Security Letters, making it clear that they could not be used for bulk collection.

3. The FISA Court has since taken advantage of the special advocates role, publicly appointing an independent advocate in one case dealing with the final stages of the bulk telephone records program and designating a pool of five qualified lawyers that can be drawn upon in the future.

- The US Privacy and Civil Liberties Oversight Board developed into a fully functioning independent oversight body, issuing detailed reports and recommendations on US surveillance programs.[4]
- Other countries adopted legislation at least nominally designed to increase oversight of their intelligence services.
- The Court of Justice of the European Union annulled the EU data retention mandate, which had required communications service providers to collect and retain transactional data on all the communications of all their customers.[5]
- Insisting that strong protections were needed lest technological developments erode the constitutional right to privacy, the US Supreme Court held that police needed a judicial warrant, issued under the Constitution's highest standard, to conduct prolonged GPS tracking or to examine the contents of a mobile phone seized in the course of arrest.[6]
- Internet and telecommunications companies published on a regular basis increasingly detailed transparency reports, statistically documenting the number and types of government demands for disclosure of customer data.
- Device makers and providers of online communications services increasingly incorporated encryption into the default settings of their products and services, protecting data both at rest and in transit. Applications providing strong encryption from one user to another (sometimes called "end-to-end," although that term can be ambiguous) proliferated.
- US-based providers of Internet services became advocates for the privacy of their customers worldwide, supporting greater transparency of government demands and stronger legislative standards for government access, and strongly opposing bulk collection of communications data.[7]
- The Privacy Bridges project, launched by then-chair of the Dutch Data Protection Authority Jacob Kohnstamm, identified "Government Access to Private Sector Personal Data" as one of 10 critical areas where transatlantic cooperation is needed, recommending that companies faced with surveillance demands "establish uniform internal practices for handling such [government] requests regardless of jurisdiction,

4. Of the 22 recommendations issued by the Board so far, all have been implemented in whole or in part, including in the legislation ending the bulk telephony metadata program.

5. *Digital Rights Ireland* ECLI:EU:C:2014:238 (2014). See also *S and Marper v. UK*, [2008] ECtHR 1581(UK DNA collection/retention).

6. *Riley v. California*, 573 U.S. 783 (2014) (mobile phone searches); *United States v. Jones*, 565 U.S. 400 (2012) (GPS tracking).

7. See https://www.reformgovernmentsurveillance.com/.

> citizenship, and data location," "report on practices relating to government access requests on a regular basis," and develop "a framework for assessing and responding to requests for data originating outside national territory."[8]

Not all developments, however, have been privacy-friendly. While the United States has curtailed some of its programs, other countries have expanded theirs. In response both to the revelations of intrusive US government programs and to the changing communications environment and the growing importance of digital evidence in both criminal and national security matters, a number of countries have adopted laws expanding government surveillance powers or requiring service providers to make data more readily accessible.

III. THE RECOMMENDATIONS

The chapters in this volume represent a diversity of voices from around the world, but they are uniform in their commitment to the proposition that terrorism can be effectively fought and national security interests can be defended within a system of oversight and control that protects both corporate interests and individual privacy. Moreover, they are remarkable in their consistency in describing the components of an effective system of checks and balances. It turns out, when it comes to government surveillance, the tools of control and accountability are already known. They are just not comprehensively applied.

In this chapter, we draw on the work of the contributors to this volume and on the flood of court opinions, legislative enactments, official reports, academic writings, corporate developments, and NGO advocacy over the past five years, to recommend a coherent framework of oversight and accountability.

The elements of the framework are really nothing new. They are drawn from long-accepted principles of the rule of law, human rights, and democratic governance. Some of them have even been applied for decades, in at least some democratic countries, to intelligence and national security surveillance. The one new recommendation that emerges from our study, however, is a strong rejection of bulk collection.

Before we present the recommendations, it is first necessary to consider briefly their scope. When we began this research in 2011, we used the term "systematic access" to refer to large-scale government access mainly to data in storage. However, we found that it was often difficult to separate concerns over access to data at rest from concerns about data in transit. Some of the surveillance programs that have attracted the largest attention in recent global policy debates have involved access to data in transit. Also, given the architecture of cloud services, data in storage may move between servers or between the cloud and

8. "Privacy Bridges: EU and US Privacy Experts in Search of Transatlantic Privacy Solutions," (2015) at 6, https://privacybridges.mit.edu/sites/default/files/documents/PrivacyBridges-FINAL.pdf.

end users, meaning that it can be accessed in transit. One clear difference that exacerbates concerns with data in storage is that it allows retrospective surveillance. Ongoing improvements in storage capacity mean that third-party service providers can and do hold data reaching back to the inception of their services. In terms of oversight and control, however, the mechanisms and standards are in many ways the same. Consequently, our recommendations, and many of the chapters in this compilation, address both access to data in transit and access to data in storage.

Also, we have found it difficult to separate concerns with bulk or mass surveillance—surveillance that sweeps up, for example, data about all individuals using a service—from concerns with surveillance that is targeted (that is, focused on specific individuals or accounts) but that nevertheless is massive in that it collects a large amount of data on a large number of individuals. That said, the distinction between mass, bulk, or indiscriminate collection and massive but targeted collection remains valid and is reflected in our recommendation against bulk collection.

A. Recommendations for Governments

1. Three Core Principles: Legality, Proportionately, and Accountability

From the various governmental, intergovernmental, corporate, academic, and civil society statements and rulings and reports both before and especially after the Snowden revelations, three core principles emerge for the conduct of government surveillance programs: legality, proportionately, and accountability. These three principles can be described and expanded with further elements. Together, they form a set of standards that we believe can permit responsible, effective government surveillance, while ensuring that it is conducted in a manner that protects privacy as fully as possible. In many instances, the same tools that help protect privacy also help focus surveillance so that it is more likely to be effective. In others, surveillance and privacy may be in tension. But in either case, a growing consensus has emerged from a rich body of international law and norms on the proper conduct of government surveillance. We believe the following principles reflect that consensus:

Legality. The principle of legality has two components. The first focuses on the adoption of the framework defining governmental powers. The authorities and standards for government surveillance (data acquisition) should be spelled out in a publicly accessible law or regulation in terms precise enough to protect against arbitrary application and to inform the public of which entities can conduct surveillance and under what criteria.[9]

9. Several human rights instruments use the phrases "in accordance with law" and "necessary in a democratic society." The core principle is that the law authorizing government data acquisition "must not only be accessible and foreseeable in its application, it must also ensure that secret surveillance measures are applied only when necessary in a democratic society, in particular by providing for adequate and effective safeguards against abuse." *Szabó and Vissy v. Hungary*, ECtHR, App. no. 37138/14, Judgment, January 12, 2016, ¶ 59.

The second component of legality focuses on the specific application of a particular power, that is, a particular exercise of that power in carrying out a specific instance or program of access. More intrusive measures should require authorization by an independent judicial officer (with possible exception for emergency circumstances). In all situations, surveillance or data acquisition should require approval of a senior official. For national security matters, approval should be required of both a senior intelligence official and from a senior official outside the security service.

Proportionality. The concept of proportionality has several components. One concerns the *purpose* of the surveillance or data acquisition. As Special Rapporteur Frank La Rue stated, "Legal frameworks must ensure that communications surveillance measures . . . [a]re strictly and demonstrably necessary to achieve a legitimate aim." In the criminal justice context, the purpose of surveillance should be limited to the investigation of specified serious crimes. In the national security context, the topics of surveillance should be narrowly defined and/or limited to specified serious threats or subjects.

Proportionality also concerns *scope*. (The concept of "necessity" is also relevant to scope.) Bulk surveillance should be disfavored. Surveillance should be limited to a specifically designated person or account.[10] "Strategic" or generalized monitoring should be disfavored and, if permitted, should be more closely regulated. The government should be required to ensure that irrelevant data is not recorded or, if collected, is destroyed or is not searched or used. This is sometimes referred to as "minimization."

Another element of proportionality is *justification*. Approval of the initiation of surveillance should require a showing of a strong factual basis for believing that the target is engaged in criminal conduct or activities of national security significance. Approval should require a showing that other less intrusive means will not suffice or are unlikely to obtain the needed information. (Again, the concept of "necessity.") The duration of a surveillance, or the time period covered by stored data, should be limited, subject to renewal.

Proportionality also means that the *use and disclosure* of data should be limited to the purposes that justified the initial collection. For example, in the criminal investigative context, data collected should be used only for investigation or prosecution of crimes at least as serious as those that justified the surveillance.

Finally, proportionality means that there should be a *time limit* set on how long the government can retain information it acquires.

Accountability. Accountability has three components: transparency, oversight, and redress. *Transparency* is closely tied to the first element of legality: not only should the government's powers be publicly specified, but basic information about the interpretation and use of those powers should be published. Independent *oversight* bodies (judicial, executive, legislative) should oversee the actual implementation of surveillance procedures to protect against abuse.

10. This is sometimes referred to as "particularity."

Individuals should be able to obtain *redress* for violations of the established standards. In order for individuals to claim redress, they must have notice. The target of government data collection should be provided notice of the government's action. Such notice may be delayed in order not to frustrate the investigation.

We recognize that no country in the world uniformly applies all of these concepts to all forms of surveillance. There are legitimate differences between surveillance for law enforcement purposes as opposed to surveillance for national security purposes, and the administrative purposes of the modern welfare state may justify certain data reporting requirements. Different rules may apply to the content of communications versus metadata. Nevertheless, recognizing all of these caveats, the foregoing factors, discussed in the chapters in this volume by Sarah St.Vincent, by Ashley Deeks, and by Ira Rubinstein, Greg Nojeim, and Ron Lee, provide the source of an effective oversight and accountability system.[11]

The chapters in this compilation, as well as the research of others, have substantially fleshed out several elements of this framework. We highlight three here.

Independent Oversight: As Nico van Eijk effectively argues, oversight, broadly defined, must be comprehensive, independent, and adequately resourced. Effective oversight can be achieved only with a web of checks and balances, implemented by multiple bodies of varying competencies, reinforcing each other. A lesson of the past four years is that no one body or structure can be relied on to provide adequate control of government surveillance. Courts, no matter how independent, can approve programs that seem unreasonable in the light of day. Parliamentary bodies may grant broad powers. An effective system of controls will include the legislature, the judiciary, the executive (through internal compliance, auditing and inspection), and some form of special commission or reviewer. Effective oversight must encompass prior authorization, post hoc review, and a meaningful complaint and redress system. It should encompass all stages of the intelligence cycle: collection, querying and analysis, retention, dissemination, and use. At least somewhere in the process, there should be an adversarial function, representing the interests of affected individuals and challenging the claims of the government.

Transparency: There must be transparency both as to what the authorities of the government are and as to how those authorities are exercised. This can be done without jeopardizing sources and methods. At the most fundamental level, all authorities exercised by the state should be specified in statute. Companies should be able to publish statistical reports on the number and types of government demands received.

Much of the criticism of the bulk surveillance program of telephone metadata, initially disclosed by Edward Snowden, that the United States was conducting under section 215 of the USA PATRIOT Act reflected the importance

11. See also D. Korff, "Note on European and International Law on Transnational Surveillance prepared for the Civil Liberties Committee of the European Parliament" (August 23, 2013), http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/note_korff_/note_korff_en.pdf.

of transparency and the impact on public trust when it is absent. The bulk surveillance was based on a series of secret court orders that offered a sweeping new interpretation of section 215 that was not in any way suggested by the text of the statute. Finally, after unauthorized disclosures, the US government officially acknowledged the interpretation, and Congress moved to amend the statute to prohibit its use for bulk collection.

Accountability: Courts, including regional human rights courts, play a crucial role. This has been demonstrated most clearly by the jurisprudence of the European Court of Human Rights and more recently by the Court of Justice of the European Union. Claims of secrecy should not be used to bar access to the courts.

B. Recommendations for Companies

Although the work TPP has supported on systematic government access to private-sector data initially focused on government activities, in its later stages it included greater attention to the activities of private-sector targets of government surveillance demands. As we explain in our chapter on accountability, the responsibility of companies as data stewards extends both to their own processing of data and to processing by their vendors and partners to whom data is disclosed. However, when a government entity demands that a company disclose data in its possession or control, that introduces a gap in the accountability structure if the governmental entity itself is not acting within a structure of accountability. This gap—the inability of a company to assure its regulators and its customers that information will be disclosed to governments only under a system of legality, proportionality, and accountability—is what led to the *Schrems* decision striking down the system for data flows from Europe to the United States. A company cannot meet its privacy obligations to its customers if it is subject to government demands that are not themselves compliant with core human rights norms. In this regard, there is a direct link between human rights protections and corporate self-interest.

There is of course a further linkage, which is trust. Even if companies were not lawfully obligated to adopt accountable data governance practices, the market creates incentives to establish and maintain the trust of their customers. Especially with the unprecedented growth of cloud services, as individuals, corporations, and other entities turn over vast amounts of highly sensitive data to third parties for storage and processing, it is literally existential that companies holding the data can assure their customers that it is secure.

A core group of Internet companies has made progress in addressing this challenge of accountability and trust, through the Global Network Initiative. Under the GNI implementation guidelines, it is not sufficient for companies merely to say, "We only comply with lawful demands." The GNI guidelines specify that companies should have in place procedures to carefully assess not only whether a government demand is lawful but also whether it is overbroad or inconsistent with international human rights standards. The guidelines state that, when

required to provide personal information to governmental authorities, participating companies will:

- Narrowly interpret and implement government demands that compromise privacy.
- Seek clarification or modification from authorized officials when government demands appear overbroad, unlawful, not required by applicable law or inconsistent with international human rights laws and standards on privacy.
- Request clear communications, preferably in writing, that explain the legal basis for government demands for personal information, including the name of the requesting government entity and the name, title and signature of the authorized official.
- Require that governments follow established domestic legal processes when they are seeking access to personal information.
- Adopt policies and procedures to address how the company will respond when government demands do not include a written directive or fail to adhere to established legal procedure. These policies and procedures shall include a consideration of when to challenge such government demands.
- Narrowly interpret the governmental authority's jurisdiction to access personal information, such as limiting compliance to users within that country.
- Challenge the government in domestic courts or seek the assistance of relevant authorities, international human rights bodies or non-governmental organizations when faced with a government demand that appears inconsistent with domestic law or procedures or international human rights laws and standards on privacy.[12]

In our chapter on accountability, we also discuss how transparency plays as critical a role in private-sector responses to government demands for personal data as it does with respect to government surveillance activities. Transparency in this context concerns both legal authorities and the scope of the government's exercise of those authorities: what types of information are being disclosed to government agencies and under what legal authorities and for what purposes; and how much data, affecting how many customers, is disclosed? Companies are largely at the mercy of national laws and government policy in terms of what they can disclose. Companies in the United States and elsewhere have made huge strides in developing transparency reports in which they publish statistical information about the number of government disclosure demands they receive and/or the number of accounts affected, although they remain constrained by some government-imposed limits.

12. http://globalnetworkinitiative.org/implementationguidelines/index.php.

IV. CONCLUSION

An increasingly broad consensus is emerging around the key requirements that should guide and constrain both government and industry when governments seek broad access to personal data held by the private sector. The work supported by TPP for more than five years has helped to inform and support that consensus. The country reports in this volume amply demonstrate the prevalence of bulk or large-scale surveillance, the importance of the need for ensuring that it is conducted subject to appropriate controls, the inadequacy of many of the controls already in place, and the growing consistency about the necessary components of an effective system of checks and balances. The findings of this project and many others have also highlighted the need for action. The tools for ensuring accountability when governments engage in systematic surveillance of private-sector data, and when industry is confronted with government demands for data, are well known. They just need to be implemented.

PART FOUR

Appendices—Project Workshops: Participants

Systematic Government Access to Private-Sector Data Workshop
Washington, DC, April 3, 2012

Ellen Blackler
Disney

Ian Brown
Oxford Internet Institute

Beth Cate
Indiana University

Fred H. Cate
Indiana University

Peter Cullen
Microsoft

Jim Dempsey
Center for Democracy & Technology

David Frazee
3M

Lynn Goldstein
JP Morgan Chase

William King
IBM

John Kropf
Reed Elsevier

Ron Lee
Arnold & Porter

Toby Levin
US Department of Homeland Security (retired)

Mark MacCarthy
Software and Information Industry Association

Deirdre Mulligan
Univ. of California Berkeley School of Information

Bulk Collection. Fred H. Cate and James X. Dempsey.

Stephanie Pell
SKP Strategies, LLC

Audrey Plonk
Intel

Stuart Pratt
Consumer Data Industry Association

Mark Rasch
Cybersecurity and Privacy Consulting/CSC

Kathryn Ratte
Disney

Ira Rubinstein
New York University School of Law

Bryan Schilling
Microsoft

Anna Slomovic
Equifax

Peter Swire
Ohio State University

Scott Taylor
HP

Jeff Ubois
MacArthur Foundation

Hilary Wandall
Merck & Co., Inc.

Systematic Government Access Workshop
London, June 3, 2013

Eric King
Privacy International

Christopher Kuner
Wilson, Sonsini, Goodrich & Rosati LLP

Cornelia Kutterer
Microsoft

Ronald Lee
Arnold & Porter

Rebecca MacKinnon
New America Foundation

Winston Maxwell
Hogan Lovells

Simon Milner
Facebook

Caroline Wilson Palow
Privacy International

Nicolette Phong
AT&T

Audrey Plonk
Intel/The Privacy Projects

Mary Pothos
Visa

Stuart K. Pratt
Consumer Data Industry Association

Ian Brown
Oxford Internet Institute

Emma Butler
LexisNexis

Fred H. Cate
Indiana University

Stan Crosley
Indiana University

Peter Cullen
Microsoft

Stephen Deadman
Vodafone Group

Jim Dempsey
Center for Democracy & Technology

Emma Jelley
Google

Jens-Henrik Jeppesen
Center for Democracy & Technology

Nate Jones
Microsoft

John Kampfner
Council of King's College, London

Stuart K. Pratt
Consumer Data Industry Association

Giorgio Resta
University of Bari

Patrick Robinson
Yahoo!

Jonathan Sage
IBM

Joris van Hoboken
University of Amsterdam

Cristina Vela
Telefonica

Ian Walden
University of London

Pat Walshe
GSM Association

Systematic Government Access to Private-Sector Data
Brussels, November 12, 2013

Lotte Abildgaard
Telenor

Antoine Aubert
Google

François Bach
Orange

Allon Bar
Ranking Digital Rights

Irena Bednarich
Hewlett-Packard

Thomas Boue
BSA-The Software Alliance

Paul Breitbarth
College Bescherming Persoonsgegevens

Ian Brown
Oxford Internet Institute

Emma Butler
LexisNexis

Carlos Cortés Castillo
Center for Freedom of Expression (CELE)
University of Palermo

Katrina Destrée Cochran
Alcatel-Lucent

Richard Danbury
Ranking Digital Rights

Willem Debeuckelaere
Privacy Commission, Belgium

Hannah Draper
Open Society Foundation

Philip Eder
Apple

Audrey Ferrazzini
RIM

Vera Franz
Open Society Foundation

Leslie Harris
Center for Democracy & Technology

Eric Heath
LinkedIn

Elonnai Hickok
Centre for Internet and Society

Sharon Hom
Human Rights in China

Jens-Henrik Jeppesen
Center for Democracy & Technology

John Jolliffe
Adobe

Jim Killock
Open Rights Group

Jacob Kohnstamm
College Bescherming Persoonsgegevens
Article 29 WG

Ron Lee
Arnold & Porter

Karim Lesina
AT&T

Christoph Luykx
Intel

Cornelia Kutterer
Microsoft

Raegan MacDonald
Access

Rebecca MacKinnon
New America Foundation

Erika Mann
Facebook

Ragnhild Mathiesen
Telenor Group

Joe McNamee
European Digital Rights (EDRi)

Paul Moynan
Allegro

Paul Nemitz
European Commission, DG Justice

Greg Nojeim
Center for Democracy & Technology

Ebele Okobi
Yahoo!

Krys O'Meara
Vodafone Group

Sonja Gittens Ottley
Yahoo!

Tom Riege
Telenor

Corinna Schulze
IBM

Chris Sherwood
Allegro

Matthew Shears
Center for Democracy & Technology

Emery Simon
BSA—The Software Alliance

Fiona Taylor
Verizon

Dalia Topelson
Berkman Center for Internet and Society

Torild Uribarri
Telenor Norway

Cristina Vela
Telefónica

Mathias Vermeulen
European University Institute

James Waterworth
Computer & Communications Industry Association

Cynthia Wong
Human Rights Watch

Enhancing Accountability in Government Access to Private-Sector Data

Montreal, May 9, 2014

Martin Abrams
Information Accountability Foundation

Sigrid Arzt
Former Commissioner to the Federal Institute of Public Information, Mexico

Kevin Bankston
Open Technology Institute

Karim Benyekhlef
Universite de Montreal

Fred H. Cate
Indiana University

Bret Cohen
Hogan Lovells

Jim Dempsey
Center for Democracy & Technology

José Alejandro Bermúdez Durana
Superintendent of Industry and Commerce, Colombia

Jacobo Esquenazi
Hewlett Packard

Adam Kardash
Osler

John Kropf
Information Accountability Foundation

John Lawford
Public Interest Advocacy Centre

Sophie Paluck-Bastien
Office of the Privacy Commissioner of Canada

Chris Prince
Office of the Privacy Commissioner of Canada

Jennifer Stoddart
Former Privacy Commissioner of Canada

David Sullivan
Global Network Initiative

Wesley Wark
University of Toronto

Karen Zacharia
Verizon

Enhancing Accountability in Government Access to Private-Sector Data
London, May 30, 2014

Martin Abrams
Information Accountability Foundation

Joseph H. Alhadeff
Oracle Corporation

Julie Brill
US Federal Trade Commission

Fred H. Cate
Indiana University

Peter Cullen
Microsoft Corp.

Gary Davis
Apple

Stephen Deadman
Vodafone Group

John DeLong
US National Security Agency

Jim Dempsey
Center for Democracy & Technology

Michael Donohue
Organisation for Economic Co-operation and Development

Jacobo Esquenazi
Hewlett-Packard

Yoram Hacohen
Institute for National Security Studies

Natasha Jackson
GSM Association

Jens-Henrik Jeppesen
Center for Democracy & Technology

Simon Milner
Facebook

Meagan Mirza
UK Information Commissioner's Office

Kenneth R. Propp
US Mission to the European Union

Marie Shroff
Former New Zealand Privacy Commissioner

Jennifer Stoddart
Former Privacy Commissioner of Canada

JoAnn C. Stonier
MasterCard Worldwide

Fiona Taylor
Verizon

Nico van Eijk
Institute for Information Law
Faculty of Law, University of Amsterdam

David C. Vladeck
Georgetown Law School

Patrick Walshe
GSM Association

Systematic Government Access to Private-Sector Data Final Workshop

London, March 1–2, 2016

Martin Abrams
Information Accountability Foundation

Eduardo Bertoni
University of Palermo

James Boyd
Indiana University

Julie Brill
US Federal Trade Commission

Giovanni Buttarelli
European Data Protection Supervisor

Fred Cate
Indiana University

Stan Crosley
CLEAR Health Information

Peter Cullen
Information Governance Solutions

Gary Davis
Apple

Elizabeth Denham
Information and Privacy Commissioner for British Columbia

Jim Dempsey
University of California, Berkeley

Michael Donohue
Organisation for Economic Co-operation and Development

Yoram Hacohen
ISOC-IL

Alex Joel
US Office of the Director of National Intelligence

Gail Kent
Facebook

Eric King
Queen Mary University of London

Jacob Kohnstamm
Dutch Data Protection Authority

Cian Murphy
King's College London

Ken Propp
BSA-The Software Alliance

Becky Richards
US National Security Agency

Romain Robert
European Data Protection Supervisor

Elettra Ronchi
Organisation for Economic Co-operation and Development

Natasha Simonsen
King's College London

Nico van Eijk
University of Amsterdam

Ian Walden
Queen Mary University of London

Nimra Zaheer
Consultative Committee of Convention 108
of the Council of Europe

Index

Bulk Collection. Fred H. Cate and James X. Dempsey.