Routledge Studies in Surveillance

STATES OF SURVEILLANCE

ETHNOGRAPHIES OF NEW TECHNOLOGIES IN POLICING AND JUSTICE

Edited by
Maya Avis, Daniel Marciniak and Maria Sapignoli

ROUTLEDGE

States of Surveillance

Recent discussions on big data surveillance and artificial intelligence in governance have opened up an opportunity to think about the role of technology in the production of the knowledge states use to govern. The contributions in this volume examine the socio-technical assemblages that underpin the surveillance carried out by criminal justice institutions – particularly the digital tools that form the engine room of modern state bureaucracies.

Drawing on ethnographic research in contexts from across the globe, the contributions to this volume engage with technology's promises of transformation, scrutinise established ways of thinking that become embedded through technologies, critically consider the dynamics that shape the political economy driving the expansion of security technologies, and examine how those at the margins navigate experiences of surveillance.

The book is intended for an interdisciplinary academic audience interested in ethnographic approaches to the study of surveillance technologies in policing and justice. Concrete case studies provide students, practitioners, and activists from a broad range of backgrounds with nuanced entry points to the debate.

Maya Avis is a research fellow at the Max Planck Institute for Social Anthropology.

Daniel Marciniak is Lecturer in Criminology at the University of Hull.

Maria Sapignoli is Associate Professor in Social Anthropology at the University of Milan.

Routledge Studies in Surveillance

Kirstie Ball, William Webster, Charles Raab, Pete Fussey, Sally Dibb, Lachlan Urquhart

Kirstie Ball is Professor in Management at University of St Andrews, UK

William Webster is Professor of Public Policy and Management at the University of Stirling, UK

Charles Raab is Professorial Fellow in Politics and International Relations at the University of Edinburgh, UK

Pete Fussey is a Professor in the Department of Sociology at University of Essex, UK

Sally Dibb is Professor of Marketing and Society at Coventry University, UK

Lachlan Urquhart Senior Lecturer in Technology Law and Human-Computer Interaction at Edinburgh Law School, UK

Surveillance is one of the fundamental sociotechnical processes underpinning the administration, governance and management of the modern world. It shapes how the world is experienced and enacted. The much-hyped growth in computing power and data analytics in public and private life, successive scandals concerning privacy breaches, national security and human rights have vastly increased its popularity as a research topic. The centrality of personal data collection to notions of equality, political participation and the emergence of surveillant authoritarian and post-authoritarian capitalisms, among other things, ensure that its popularity will endure within the scholarly community.

A collection of books focusing on surveillance studies, this series aims to help to overcome some of the disciplinary boundaries that surveillance scholars face by providing an informative and diverse range of books, with a variety of outputs that represent the breadth of discussions currently taking place. The series editors are directors of the Centre for Research into Information, Surveillance and Privacy (CRISP). CRISP is an interdisciplinary research centre whose work focuses on the political, legal, economic and social dimensions of the surveillance society.

CRISP

CENTRE FOR RESEARCH INTO INFORMATION,
SURVEILLANCE & PRIVACY

Resisting State Surveillance in the Digital Age
Precarious Coalitions, Contested Knowledge, and Diverse Opposition to Mass-Surveillance in the UK
Amy Stevens

States of Surveillance
Ethnographies of New Technologies in Policing and Justice
Edited By Maya Avis, Daniel Marciniak and Maria Sapignoli

For more information about this series, please visit: https://www.routledge.com/Routledge-Studies-in-Surveillance/book-series/RSSURV

States of Surveillance

Ethnographies of New Technologies in Policing and Justice

Edited by
Maya Avis, Daniel Marciniak
and Maria Sapignoli

Routledge
Taylor & Francis Group
LONDON AND NEW YORK

First published 2025
by Routledge
4 Park Square, Milton Park, Abingdon, Oxon OX14 4RN

and by Routledge
605 Third Avenue, New York, NY 10158

Routledge is an imprint of the Taylor & Francis Group, an informa business

This title is available under the Creative Commons license CC-BY, with funding from the Max Planck Institute for Social Anthropology, Department of Law and Anthropology.

British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library

Library of Congress Cataloging-in-Publication Data
Names: Avis, Maya, editor. | Marciniak, Daniel, editor. | Sapignoli, Maria, editor.
Title: States of surveillance: ethnographies of new technologies in policing and justice/edited by Maya Avis, Daniel Marciniak and Maria Sapignoli.
Description: Abingdon, Oxon; New York, NY: Routledge, 2025. |
Series: Routledge studies in surveillance | Includes bibliographical references and index.
Identifiers: LCCN 2024025432 (print) | LCCN 2024025433 (ebook) |
ISBN 9781032536118 (hardback) | ISBN 9781032536439 (paperback) |
ISBN 9781003412908 (ebook)
Subjects: LCSH: Electronic surveillence. | Police. | Crime prevention–Technological innovations. | Law enforcement–Technological innovations.
Classification: LCC HV7936.T4 S73 2025 (print) | LCC HV7936.T4 (ebook) |
DDC 363.2/32–dc23/eng/20240624
LC record available at https://lccn.loc.gov/2024025432
LC ebook record available at https://lccn.loc.gov/2024025433

ISBN: 978-1-032-53611-8 (hbk)
ISBN: 978-1-032-53643-9 (pbk)
ISBN: 978-1-003-41290-8 (ebk)

DOI: 10.4324/9781003412908

Typeset in Sabon
by Deanta Global Publishing Services, Chennai, India

Contents

PART 1

PART 2
Shaping epistemology: Problematising knowledge production in law enforcement 109

Figures

Acknowledgements

This book is the result of a workshop “Situated AI – Global Ethnographies of New Technologies in Policing and Justice” held online in December 2021 by the research group “*AI*ming Toward the Future: Policing, Governance, and Artificial Intelligence” (later renamed “The Anthropology of AI in Policing and Justice”) at the Max Planck Institute for Social Anthropology in Halle (Saale), Germany. We had originally planned to meet in person, but COVID-19 had other ideas. However, despite only ever meeting remotely, the workshop took on a life of its own, and this volume is just the next step in the ongoing conversation. We would like to thank the authors for their contributions, the productive discussions we were able to have, and their patience throughout the process. We also express our gratitude to the Max Plack Society and the Max Planck Institute for Social Anthropology, especially to Prof Marie-Claire Foblets, Director of the Law and Anthropology Department, for their unwavering support and the funding that made this project possible.

Contributors

Maya Avis is a research fellow in the research group "Anthropology of AI in Policing and Justice" at the Max Planck Institute for Social Anthropology in Halle (Saale), Germany. She earned her PhD at the Department of Anthropology and Sociology at the Graduate Institute, Geneva. Her dissertation considered the organisation of the legal environment in Palestine/ Israel, with a particular focus on Palestinian Bedouin land claims. The research was based on extensive ethnographic research. In 2018, she was a visiting fellow at the Centre for Human Rights and Global Justice at New York University.

Tessa Diphoorn is an associate professor in the Department of Cultural Anthropology at Utrecht University. Her research and teaching focus on security, violence, and sovereignty in Kenya and South Africa. She is the author of *Twilight Policing: Private Security and Violence in Urban South Africa* (2016), co-author of *Nairobi Becoming: Security, Uncertainty, Contingency* (2024), and co-editor of *Security Blurs: The Politics of Plural Security Provision* (2019). In addition to her writing, she is also the co-founder of the podcast series *Travelling Concepts on Air*, where she explores the notion of travelling concepts with her colleague Brianne McGonigle Leyh.

Simon Egbert is a sociologist, currently working on the socio-technical relations of predictive analytics at the University of Bielefeld. He received his PhD at Universität Hamburg in 2018 with a dissertation on drug testing. He was a postdoctoral fellow at Technische Universität Berlin as well as a research fellow at Universität Hamburg and Universität Bremen.

Maximilian Heimstädt is a senior researcher at Bielefeld University and head of the research group "Reorganising Knowledge Practices" at Weizenbaum Institute for the Networked Society in Berlin. To better understand the interplay of emerging technologies and organisations, he draws on analytic sensibilities from management studies, sociology, and science and technology studies (STS).

Mark Maguire is Dean of Maynooth University Faculty of Social Sciences. His research explores public behaviour during terror attacks, behavioural detection, and counterterrorism policing. He is the author, with David A. Westbrook of *Getting Through Security: Counterterrorism, Bureaucracy, and a Sense of the Modern* (2020). He co-edited several recent volumes on security, including, with Setha M. Low, *Spaces of Security: Ethnographies of Securityscapes, Surveillance, and Control* (2019). His latest work, with Setha Low, *Trapped: Life under Security Capitalism and how to Escape it* (2024) is on the middle-class love of security and safety .

Daniel Marciniak is a lecturer in criminology at the University of Hull. Drawing on concepts from science and technology studies and surveillance studies, his research focuses on the development and use of new technologies in policing. Previously, Daniel was a research fellow in the research group "Anthropology of AI in Policing and Justice" at the Max Planck Institute for Social Anthropology in Halle (Saale), Germany. Daniel earned his doctorate within the Human Rights, Big Data and Technology project at the University of Essex, UK, with a thesis titled "Data-driven policing: how digital technologies transform the practice and governance of policing".

Andrea Miller is an assistant professor of telecommunications and women's, gender, and sexuality studies at The Pennsylvania State University. In their work, they draw from transnational and postcolonial feminist studies, science and technology studies, and cultural studies to consider how technology, security, and empire shape sensibilities of race and gender. Their work has examined the racialised logics of drone warfare and preemption, the criminalisation of online speech acts, predictive policing and biometric surveillance technologies, and US counterterrorism policy. They are currently completing a book project that examines the cyber ecosystem as a sense-making concept for the US security state.

Shivangi Narayan is a research fellow at the "Algorithmic Governance and Cultures of Policing" Project funded by Oslo Metropolitan University and the Norwegian Research Council. She recently completed her PhD titled "Predictive Policing and the Construction of the Criminal: Study of Delhi Police" at the Centre for the Study of Social Systems, Jawaharlal Nehru University, New Delhi, India. She is a former engineer and journalist making sense of socio-technical interactions in India. In 2021, she published her book, *Surveillance as Governance*, on UID/Aadhar, India's system for biometric identification.

Maria Sapignoli is an associate professor in social anthropology and member of the PhilTech Research Center for the Philosophy of Technology at the University of Milan, Department of Philosophy. She is on the scientific advisory board of the research cluster "Anthropology of AI in Policing and Justice" at the Max Planck Institute for Social Anthropology. Sapignoli has conducted ethnographic fieldwork in southern Africa, New Zealand, as well as in several international organisations, on topics of institutional reform, indigenous rights, social movements and advocacy, and, ultimately, justice. Most recently, she has been working on the legal and social challenges and opportunities presented by the use of new technologies in society and in environmental governance. She is the author of *Hunting Justice: Displacement, Law, and Activism in the Kalahari* (2018) and co-editor of the Oxford Handbook of Law and Anthropology (2022).

Martín Javier Urtasun has a PhD in sociology from La Plata's National University and continues his research supported by a postdoctoral grant from the National Council for Scientific and Technological Research. He is an associate professor of criminology at Juan Vucetich University Institute and is currently working as an advisor for the Security Ministry of Buenos Aires Province. He focuses his academic interests on preemptive security policies and surveillance devices, particularly urban video surveillance systems. He has conducted an in-depth ethnography of the daily functioning of the video surveillance system of Ensenada City, Argentina. His research is theoretically informed by Foucauldian approaches to surveillance and governance, pragmatic sociologies, and Actor-Network Theory. He is part of Buenos Aires' Security Study Group (NESBA) and the Latin American Network on Surveillance, Technology and Society Studies (LAVITS).

David A. Westbrook is the Louis A. Del Cotto professor at the University of Buffalo Law School and co-directs the NYC Program in Finance and Law. His work influences numerous disciplines, and he has spoken on six continents to academics, business and financial leaders, members of the security community, civil institutions, and governments, often with the sponsorship of the US State Department. His books include *Navigators of the Contemporary: Why Ethnography Matters* (2008), *Deploying Ourselves: Islamist Violence and the Responsible Projection of U.S. Force* (2010), and *Getting Through Security (2020) with Mark Maguire*.

Abbreviations

ADRIN Advanced Data Processing and Research Institute

AI Artificial intelligence

AIDS Acquired immunodeficiency syndrome

AK Kalashnikov's automatic [rifle]

ARIS Anonymous Reporting Information System

ARW Irish Army Ranger Wing

AWS Amazon Web Services

BMT Group: British Maritime Technology Group

CABA Autonomous City of Buenos Aires

CAJ Commission on Administrative Justice

CAS crime administration system

CCTNS Crime and Criminal Network Tracking System

CCTV Closed Circuit Television

CEO Chief Executive Officer

CISA Cyber and Infrastructure Security Agency

CMAPS Crime Mapping Analytics and Prediction System

COMPSTAT COMPuter STATistics

CONARC Consulta Nacional de Rebeldías y Capturas (national database of individuals with arrest warrants)

COVID-19 Coronavirus disease 2019

CPCR Central Police Control Room

CrPC Criminal Procedure Code

DARPA The Defense Advanced Research Projects Agency

DMD Digital Mapping Division

DV Domestic violence

EACC Ethics and Anti-corruption Commission

ERU Emergency Response Unit

ESE Elbit Systems Emirates

EU European Union

FIR First information report

FOOB Folklore of operational banality

FRS Facial Recognition System

GA Georgia

GIGN Gendarmerie, Groupe d'intervention de la Gendarmerie nationale

GIS Geographic Information System
GIZ German Development Agency
GPS Global Positioning System
HIV Human immunodeficiency virus
HQ Headquarters
IAU Internal Affairs Unit
IBM International Business Machines Corporation
ICT Information Communication Technology
ID Identification
IMF International Monetary Fund
INCLO International Network of Civil Liberties Organizations
INDI Israel National Drone Initiative
IPCRM Integrated Public Complaints and Referral Mechanism
IPOA Independent Policing Oversight Authority
ISDEF Israel Defence Exhibition
ISRO Indian Space Research Organisation
IT Information technology
KNCHR Kenya National Commission on Human Rights
LA Los Angeles
LKA NRW Landeskriminalamt Nordrhein-Westfalen (State Criminal Police Office North Rhine-Westphalia)
London Metropolitan Police's SCO-19 London Metropolitan Police's Specialist Firearms Command-19
MOC Municipal Operating Center
MSJC Mathare Social Justice Centre
NACCSC National Anti-Corruption Campaign Steering Committee
NCF National Critical Functions
NCIC National Cohesion and Integration Commission
NGO Non-governmental organisation
NICE Neptune Intelligence Computer Engineering
NORTHCOM US Northern Command
NPS National Police Service
NRC National Register of Citizens
NSO Niv, Shalev and Omri (the names of the company's founders)
NYPD New York City Police Department
PR Public relations
PRECOBS Pre Crime Observation System
RAID Recherche, Assistance, Intervention, and Dissuasion
RMS Record management system
RYaN Programme: Raketno-Yadernoe Napadenie
SAS Britain's Special Air Service
SAS Statistical Analysis System
SEAL The United States Navy Sea, Air, and Land Teams
SHO Station Head Officer
SIBIOS Federal System of Biometric Identification for Security Purposes

SKALA System zur Kriminalitätsauswertung und Lageantizipation (System for crime evaluation and situation anticipation)
SMS Short Message Service
SPSS Modeller Statistical Package for the Social Sciences Modeller
STS Science and Technology Studies
SWA Special Weapons and Tactics
TI-K Transparency International-Kenya
UAE United Arab Emirates
UAM Unmanned air mobility
UAVs Unmanned aerial vehicles
UK United Kingdom
UNOCT The United Nations Office of Counterterrorism
UNODC United Nations Office on Drugs and Crime
US United Nations
USA United States of America
USD United States Dollar
USSR Union of Soviet Socialist Republics
VR Virtual reality
WC Water closet
WH White House
XR Extended reality

States of surveillance

Ethnographic perspectives on technology in policing

Maya Avis, Daniel Marciniak, and Maria Sapignoli

Introduction

Research on surveillance has been strongly inspired by Foucauldian ideas of discipline and the panopticon (Haggerty, 2006), and later biopower and security (Gandy, 1993; Marx, 2002; Lyon, 2003). Based on Deleuze's (1992) contribution of societies of control, Haggerty and Ericson (2000) have imagined control to work as a surveillant assemblage in which recorded information about individuals, "data doubles", circulates through centres of calculation that, based on statistics of the whole population, gives selective access to resources. In this volume and Deleuze's imagination, power no longer only flows through the classic agents of discipline (the teacher, the prison guard, the drill sergeant) but gradually becomes automated. We can see this sort of automation emerging all around us with scholars like Ruha Benjamin (2019), Virgina Eubanks (2018), Andrew Ferguson (2017), and Oscar Gandy (1993, 2009) pointing at automated decision-making systems that further entrench existing inequalities when they feed on data traces to "improve" social security, inform banks' mortgage decisions, or decide who poses a security threat.

These concerns become particularly pertinent with these systems increasingly shaping the functioning of our criminal justice systems. In the face of the combined impacts of resource cuts and accusations of discriminatory practices, police leaders and institutions have turned to technology to reorient policing. Digitalisation and artificial intelligence (AI) promise a "smart, effective, and accountable" way to adjust to diminished resources and to "police the police". Systems are supposed to improve practitioners' discretion throughout the criminal justice system, including decisions around who and where to police, individual's access to parole and probation, and "internal matters" such as the risk of police misconduct (Ferguson, 2017; Brayne and Christin, 2020; Brayne, 2021). Together with the presumed "rationality" of new technologies and their promise of a "better" society come fears of Orwellian surveillance, increased social injustice, and the indifferent judgement of machines.

Focusing on criminal justice institutions, the contributions to this edited volume show through ethnography that with every attempt at automation,

DOI: 10.4324/9781003412908-1

pre-existing configurations of power, control, values, accountability, and profits are reshaped as new technological assemblages involve a large array of interests and possibilities. This includes the interests of those who govern, but also business interests, bureaucrats, and those who seek to escape the ways these systems are designed to shape their lives. Instead of perceiving surveillance as a panopticon, a set of relations between a centralised observer and the observed, this volume centres on the multiplicity of agents involved and how their respective agendas shape the ways power operates through new surveillance technologies. Each of the chapters focuses on different actors, technologies, or logics that shape and inform what McCahill (2021) has described as a "field of struggle" around recent technological transformations.

What unites the contributions in this volume is that rather than "opening the black box and finding it empty" (Winner, 1993), contributions re-politicise the perceived "mechanical objectivity" (Daston and Galison, 2010) of the stale, bureaucratic processes enacted by digital technologies. The chapters demonstrate that approaching surveillance technology through its social relations opens up novel approaches to established questions in surveillance studies around the role of surveillance in social control, as well as new avenues of research around, for example, the epistemologies built into these technologies and their at times precarious existence within strained socio-technical relations. Informed by a range of different disciplinary approaches to the topic, some contributions take apart the functioning of the assemblage itself while others examine the larger socio-political contexts that shape the adoption and use of new technologies. They provide insight into how technologies (re)shape surveillance relations with intimate, often ambivalent and contradictory, consequences, for those who are supposed to use them and, especially, for those who are their intended and unintended targets.

The volume is divided into two main parts: navigating surveillance and shaping epistemology. This distinction relates to where researchers look. The chapters in the first part tend to cast a wide net in terms of their focus emphasising the context in which technologies are embedded, while contributions in the second part provide more detailed insights about particular technologies and problems. Taken together these give a fuller impression of the promises and challenges related to new surveillance technologies. This introduction will discuss these approaches in more detail, before attending to questions related to what ethnography can tell us about these processes.

Navigating surveillance: contending with promises of transformation

The contributions in the first part of the volume shed light on the practices, hopes, worries, and daily experiences of those who use, shape, and navigate changing technological landscapes. They highlight the political shifts that come with the introduction of new technologies, from the "small" politics of bureaucratic organisations to the "large" politics of newly opening up fields of governance, such as cybersecurity. We have put this section at the beginning of the volume to highlight the very tangible consequences new surveillance technologies have for people's lives. This makes apparent what the stakes are for the design and function of technology, which is the focus of the second part of the volume. In introducing this section, we reflect on the consequences, frictions, and refusals that emerge in relation to new technologies of policing and surveillance. We address the unforeseen consequences of the introduction of technologies, attend to the broader societal shifts that can emerge with their adoption, and reflect on the various forms of resistance encountered in the literature and in the contributions in this part of the volume. The section ends with a reflection on the dynamic interaction between the multiplicity of relevant agents and the resulting difficulty in pinpointing a single address for resistance.

New technologies bring with them promises of transformation that rest on an assumption that states need information about their subjects to both care for them and control them (Marx, 2015). This information is portrayed as more efficiently collected, sorted, and analysed with the introduction of new digital technologies. Yet, the propensity of new technologies to collect increasingly large quantities of data often leads to a host of unforeseen consequences that can emerge alongside the intended outcome behind their introduction. In **Windows into the Soul*, Gary Marx addresses some of the fallacies associated with approaches to surveillance, one group of which relates to the notion that technologies fix existing problems without creating new ones (Marx, 2016). The problems new technologies are supposed to fix can be diverse and include almost anything from resource allocation within policing to broader societal problems. In some cases, technology fails to deliver on its promises altogether. In the case of Diphoorn in this volume, imaginations of a technological fix to bureaucratic accountability and transparency encounter the realities of bureaucratic politics and people's distrust of government agencies which leads to the technology failing. Other times, the consequences are more serious. Some research has focused on the implications of the over-surveillance of marginalised populations (Browne, 2015), while other work highlights the effects of under-surveillance and the kinds of "inequalities of access and opportunity" (Ball *et al.*, 2006: 281) this may bring about. The effects of surveillance on peoples' life chances can be dramatic when a state's decision-making is automated (Gandy, 2009; O'Neil, 2016; Eubanks, 2018; Benjamin, 2019).

Conversely, rather than looking at the consequences surveillance technologies have, Ball *et al.* (2006) think about what the increasing prevalence of surveillance technology tells us about social relations. In particular they state "surveillance processes and practices bespeak a world where we know we're not really trusted" and "permitting ourselves to undermine [trust] in this way seems like slow social suicide" (Ball *et al.*, 2006: 3). This concern for society has been central to research on the effect of new surveillance technologies on democratic values (Stevens *et al.*, 2023). Miller, in this volume, mirrors this when they interrogate the disregarded expansion of policing powers into new areas of cybersecurity governance. They explain that the policy changes new technologies bring about have huge social significance despite the general atmosphere of indifference which might be related to the technicality of the subject. Where the new systems and technological objects Miller describes are met by boredom and indifference, Avis' contribution traces attempts to circumvent, confuse, and even destroy new technologies. Her contribution reveals how producers of surveillance technologies and representatives of the Israeli state are guided by a logic which imagines that state security can be achieved through technological domination before addressing a gamut of Palestinian responses to these technologies which are directly related to the violence of this logic. She argues that these acts of resistance can build solidarity among people locally and internationally.

This research reflects existing scholarship that investigates reactions to surveillance technology and distinguishes between organised forms of opposition to surveillance and everyday resistance (Gilliom and Monahan, 2012). Drawing on work by Marx (2003) and Gilliom (2001), Gilliom and Monahan (2012: 405) describe everyday resistance as "invisible forms" of objection to surveillance, which can include "lying, evading, masking, and cheating" or generally trying "to circumvent or quietly disrupt the surveillance systems to which [individuals] are exposed". For example, migration scholars have pointed to the ways irregular migrants try to bypass biometric border regimes (Amoore, 2006; Broeders, 2007; Scheel, 2019). On the other end of the spectrum, police officers repurpose the body-worn cameras that have been brought in to hold them accountable to protect themselves by choosing which of their actions become recorded (Sandhu, 2019). Gilliom and Monahan (2012) draw attention to the fact that non-compliance by the poor (such as welfare fraud) is less likely to be socially accepted and more likely to lead to prosecution than similar actions carried out by the rich (such as tax evasion). In terms of organised resistance researchers have focused on counter-veillance or sous-veillance practices in which citizens gather information about powerful actors (Mann, Nolan, and Wellman, 2003; Huey, Walby, and Doyle, 2006), while others have centred on the evasion of surveillance, whether this is through artistic initiatives of facial recognition camouflage (Monahan, 2015) or in preemptive attempts by activists to evade data-veillance practices (Kazansky, 2021). This kind of opposition is often public and demands new kinds of surveillance practices.

This volume makes apparent that the nature of surveillant assemblages means there is a multiplicity of possible addresses for resistance. In Avis' contribution the target of opposition is the Israeli surveillance assemblage as a whole, while Urtasun shows that surveillance practices are the result of a fraught field of struggle between surveillance workers, their superiors, and global surveillance trends. Urtasun's ethnography depicts surveillance workers grappling with possible changes to their profession in anticipation of the arrival of live facial recognition. His close study of the work of recognition that surveillance workers in a small town in Argentina perform, and the concerns of his interlocutors around the fact that this may soon be digitised, reveals the broader frictions (between workers and technologists and between small places and global trends) that come with technological change. His contribution shows that power has to be traced and is not self-evident. Alliances can form in interesting and unpredictable ways given the less centralised forms of power. Various contributions in this volume show that with the introduction of new technologies multiple different agendas and actors can come to shape governance decisions, making a clear source of power difficult to pinpoint.

Deleuze (1992) describes the problem as being one in which control becomes amorphous when the factory owner, as the focus for workers' unions resistance, disperses into a more anonymous stakeholder model and when systems of control undermine solidarity by centring competition between workers. By highlighting the variety of actors involved in shaping the epistemologies of systems of control, all the contributions in this volume can be read as investigations into addresses for grievances about the harms of surveillant assemblages in their various forms. They do this by injecting humans back into anti-terror policing (Maguire and Westbrook), balancing public, state, and private interests (Urtasun, Marciniak), mapping the points at which social inequalities enter the system (Egbert and Heimstädt, Narayan), or showing how significant these changes are regardless of how obvious the violence is (Avis, Miller).

Shaping epistemology: problematising knowledge production in law enforcement

While the first part of the book is concerned with the ways surveillance workers, bureaucrats, and citizens are affected by and relate to new technologies, the chapters in the second part take a closer look at the technologies themselves – the ways they are built, the assumptions they contain, and how they are part of socio-technical assemblages. Contributions sit with a tradition of work trying to take apart the mechanisations of bureaucracies and the ways they produce knowledge, often through quantification of phenomena and the neoliberal impetus of governing through statistical indicators (Porter, 1996; Espeland and Sauder, 2007; Rottenburg *et al.*, 2015; Beer, 2016). They consider the epistemologies embedded in the technologies that produce the state's vision and reflect on the fundamental justice implications this vision has for the subjects of surveillance. Varying in how explicitly this is addressed, the accounts in this volume are driven by common concerns in the literature that we want to briefly outline here: a concern for the authority derived from the "objectivity" of technologically produced knowledge, a concern for technologies locking actors into problematic patterns of action, and a reflection on who gets to shape how technologies operate.

We do not have to look long to find a plentitude of examples in which new technologies are supposed to replace the subjective decision-making of policy-makers and bureaucrats with the objectivity of reproducible numbers. In the 1990s and early 2000s neoliberal governments across the Western world decided to set numerical goals and have bureaucracies figure out how to fulfil them in an effort to instil competition into state actions (Rottenburg *et al.*, 2015). We find this in indicators like the Global COMPACT that have been directing politicians to adjust their policies in search of funding from international organisations and financial markets (Merry, 2011). This is particularly pronounced in the area of policing, where the consequences of officers "cooking the books" to make the statistics fit their performance goals affect how they work in ways that can have detrimental impacts on marginalised communities (Guilfoyle, 2012). While many of these policies have later been rolled back, a new obsession with the objectivity of algorithms, AI, and machine learning seems to be bringing back similar dynamics.

The scholarly response is still often one of deconstruction: informed by the work of science and technology studies researchers, a common impulse in the study of the technologies used by criminal justice institutions is to try to "open the black box" and scrutinise the inner workings of the knowledge machines that are central to surveillant assemblages (Haggerty and Ericson, 2000) – whether this is classic studies of the interpretative work of surveillance workers in the control room (Smith, 2015) or, more recently, investigations into the functioning of predictive policing assemblages (Lum and Isaac, 2016; Egbert and Leese, 2020). Besides marvelling at the complexity of socio-technological assemblages, the aim of this kind of research is, more or less explicitly, to unveil the political decisions inherent to the various steps of data production, analysis, and enactment of outcomes. This happens against a backdrop of a discourse that claims the objectivity of data and, by extension, the authority of decisions based on this data. The goal is to understand the politics of technologically produced visibilities. In this volume, Egbert and Heimstädt undermine the "objectivity" of predictive policing by pointing at the biases that feed the chain of translation, and Narayan points to the large chasm between the precision of digital crime maps and the haphazard, stereotyped recording patterns of crime incidents.

Objectivity, as Daston and Gallison (2010) have pointed out, relies heavily on the mechanical reproducibility of results. This mechanisation brings with it another concern beyond the authority of objectivity: artefacts are not only part and parcel of social relations but also act in stabilising them (Latour, 1994); infrastructure orders social life (Star, 1999). From the first public phone boxes to emergency call systems, from foot patrol to officers driving around in cars, and from unsystematic crime records to digital record management systems, technologies have long been part of efforts to transform policing and have shaped policing practice (Deflem and Chicoine, 2014). Already writing at the end of the 1970s, Colton (1979: 19) expressed the concern that the introduction of computers in US police departments would "[…] serve to reinforce the status quo, to lock in and substantiate our present approach, and to indirectly countermand other innovation". Policing researchers have continued to reflect on the degree to which information technology shapes policing. On the one hand, Manning (2008) highlighted the mere performativity of crime mapping and its lack of effect on frontline policing. On the other hand, Chan (2001), and Ericson and Haggerty (1997) have shown its role in enforcing the accountability of the police through reports and surveillance of police officers, and Harper (1991) has demonstrated how readily available information on computer systems has reshaped detective work.

The question of information technology's role in policing and its potential for stabilising problematic practices has become only more pertinent with the introduction of technologies like predictive policing and facial recognition. Maguire and Westbrook, in this volume, show concern about the prospect of the thin descriptions of terror incidents encoded in the *boxology* of counterterrorism training. These thin descriptions lend themselves to augmented reality training scenarios that have little to do with the thick "reality" of terror incidents described by their interlocutors. However, technology does not necessarily stabilise social relations. Other contributions in this volume demonstrate that socio-technical assemblies are fragile, rely on continuous maintenance, and may never come to be (see Diphoorn, Marciniak, Narayan).

Finally, a third concern relates to the balance between public values and private interests. As authors like Mel Hogan (2018) and Kate Crawford (2021) have made clear, the expansion of data-driven technologies is partially driven by companies seeking new customers for the products they have. Moreover, the field of surveillance studies and related research on security technologies have long been aware of what Hayes (2012) terms the surveillance-industrial complex", a revolving door between state and industry with private profit as a motivating force that provides evermore intrusive forms of surveillance. The overlap of private interests in worker and consumer surveillance and state interests in growing intelligence after the 9/11 terror attacks has consolidated a global surveillance society (Ball and Wood, 2013). In policing, increasing datafication has led not only to a transformation of surveillance relations but also to what Wilson (2021) refers to as "platform policing" – a managerial orientation in which constant analysis of data generated by officers structures their work in a feedback loop. More importantly, this has opened policing to the digital economy with a large number of private companies offering their cloud services. The analysis does not focus on the surplus value generated by surveillance capitalism (Zuboff, 2019). Rather than with surplus generated from extracting data (Zuboff, 2019), the concern in this market lies with questions of accountability and responsibility that have become fraught with new governance configurations in which private companies increasingly not only sell sensors that gather data – like cameras, IMSI-catchers, and digital forensics – but also process that data in a way that proposes particular interpretations, which then shape the way police act. As Marciniak's contribution to this volume makes apparent, a number of questions emerge from companies' involvement in shaping policing due to the outsourcing of cloud infrastructure production and maintenance: if particular technologies produce, or reproduce, inequalities is the onus on the companies themselves, or on the states who choose a particular service provider? How can we broaden the conversation about the role of policing and the technologies that structure its practices beyond private suppliers with vested interests and the state?

Approaches to the field

This volume brings together researchers with a variety of disciplinary backgrounds, including anthropology, sociology, and media studies, who focus their analysis on the socio-technical assemblages that underlie the daily workings of surveillance operations and the people who engage with or are the subjects of those operations. The different chapters show a diversity in *how* they approach the study of new technologies in surveillance and *what* they focus on. The kaleidoscope of perspectives is, on the one hand, an expression of the challenge to suitably define the object of study and, on the other hand, the perspectives collected in this volume help to bring into focus the diverse and ever-shifting field of technological change. In many ways, what the contributions in this volume show is how significant context is in determining how researchers approach the study of new technology and its effects.

Numerous scholars have demonstrated the challenges ethnographic approaches to understanding new technologies encounter, in particular in relation to access, technological opacity, and the heterogeneity of socio-technical assemblages dispersed in time and space (Kitchin, 2017; Seaver, 2017; Christin, 2020). Some of this heterogeneity relates to the question of who we study and some to which part of the "life" of a technology we study. Researchers can spend time with developers, bureaucrats, police officers, technicians, company representatives, those being policed, protestors, brochures, manuals, policy, and legislation – the list of entities that can be studied is endless. This relates to which part of the "life" of a new technology researchers attend to, whether this is development, marketing, deployment, or decommissioning. These different phases have consequences for the temporal orientation of research. For example, the chapters reflect on projects that have already been implemented and possibly failed (Diphoorn), analyse technological development as a process of iterative change (Marciniak), take apart the present functioning of a technology (Egbert and Heimstädt), or deal with the anticipation of technologies that are yet to arrive (Urtasun).

The entanglement of local contexts in global power relations poses a challenge to classic conceptions of a fieldsite. For example, Urtasun describes how the global market for facial recognition arrives in Argentina, Narayan encounters representatives of a Western mapping company that Indian institutions rely on for parts of the predictive policing system they are developing, and Avis describes how Israel leverages the sales of security technologies in diplomatic relations. The question of site and of how to study particular phenomena ethnographically, especially when they are globally entangled, has been of concern to ethnographers outside the field of technology for decades, leading some to highlight the necessity for multi-sited ethnography (Marcus, 1995; Holmes and Marcus, 2008; Feierman *et al.*, 2010).

In whichever way we intend to study surveillance our field can be shaped significantly by what we gain access to. Researchers who conduct their research within police departments and tech companies need to negotiate access with secretive institutions (Monahan and Fisher, 2015). Those who study the experiences and consequences of surveillance technologies encounter different difficulties with access, which might relate to difficulties in finding interlocutors who are aware of the technologies, show interest in discussing them, and are not afraid to talk about them. Even after successful initial access negotiations, a lack of trust, secrecy, or simply institutions or communities being unaccustomed to the presence of researchers may hamper research efforts.

Questions about what to study have been approached through spatial metaphors that ask about the direction of study and whether to study up, down, or sideways (Nader, 1972; Ortner, 2010). These directions relate both to issues of access discussed above and the politics of research. Characterised by the two perspectives on technology outlined in the previous sections, contributions to this volume reflect different directions of research. However, the research topic forces researchers to engage with similar political concerns. As Fassin (2017) has found, political concerns are all the more pressing when conducting research in the field of policing and technology. What changes is the amount of detail that is afforded to different perspectives on the same field. Accordingly, Maguire and Westbrook, in this volume, reflect on the often critical stance that ethnographers take in approaching technologies used in policing by highlighting the literal life-and-death stakes that are at play in counterterrorism training. Avis straddles the divide between studying up and studying down by considering the narratives she encounters at security conferences *and* the ways subjects resist or submit to power. Miller makes this relationship between research and its political implications explicit when they ask that we consider "what stories are told in our conversations with the technological objects and systems that enable and enact state violence?".

Despite the diversity of contexts and perspectives, the contributions to this volume deal with technologies that, when applied to the justice system, seem to raise similar issues and concerns. This provides an opportunity to study the "contemporary" (Rabinow, 2008) in its global dimensions and local adaptations. While in some contexts ethnographers find technologies already in action, in other contexts, like Urtasun's engagement with the anticipation of facial recognition technology in a small Argentinian town, global trends have yet to arrive. Concerns that emerge in this volume relate to the place of digital technologies in relationships of power, the role of tech corporations in shaping policies and laws, and the place automated decision-making has in the governance of today's world. In different settings the different aspects are more pronounced, which sharpens our sensibilities to these issues so that we can start identifying them even if they only appear as minute gestures like the "tear and the shrug" in Miller's contribution. This may also help with anticipating upcoming or underlying problems for other locations. Ethnography helps us to not take issues like bias for granted or fall into ready-made narratives around what the concerns with new technologies are. Examples of this are Marciniak's engagement with technical experts who have already considered some of the publicly voiced critiques, Narayan's reflection on the stereotypes that shape data collection in India in a completely different way from the potential for bias identified by Egbert and Heimstädt, and the contrast between the indifference encountered by Miller and the polarisation of the field that Avis engages with.

Instead of the more obvious comparisons between the global North and South; high-tech and low-tech; pre-modern, modern, and post-modern, contributions to this volume show that technological change is accompanied in all contexts by the promise of transformation. This transformation is often (still) depicted in the light of technological optimism even where there is a growing awareness of some of the impacts that arise from technology's encounter with the frictions of social contexts. To end then on a hopeful note, we cannot help but notice that we have come a long way from the worries of the 1990s about the unforeseen consequences of technological progress encapsulated in the risk society, and the crisis of objectivity in the science wars, as well as the various discussions of whether or not a new era of post-modernity had arrived. Indeed, the proponents of new technologies – the developers, the company representatives, the bureaucrats – that speak through the various chapters collected in this volume have not given up on modernity as a project of scientific-technological progress. Many are driven by hopes for a better world. Hopes that are shared beyond the area of security. While AI may just be the latest buzzword in a collection that includes Big Data, the cloud, machine learning, and Web 2.0, we get a sense of entering uncharted territory. Yet, at the same time, we do not enter blindly; experts are not dominant anymore just because they are experts, developers cannot hide behind the "objectivity" of their numbers, and regulators have started drafting legal texts to prohibit the well-intentioned from inadvertently causing harm. This has caused and will cause conflict, some of which may sit quite uncomfortably with us as we have learned during the pandemic, but it seems we have taken great strides in the direction of treating "matters of fact" as "matters of concern" (Latour, 2004). We believe that this volume provides two valuable insights for this journey: first, social sciences, and particularly ethnography, can provide valuable insight into the problematizations that those working at the coalface of innovation are impervious to, and second, relatedly, while we need to ask the questions of bias and social inequality, we also need to ask broader questions about the trajectory we are on as human beings. Perhaps our task then lies in rendering visible the paths we are taking and remaking surveillant assemblages with a Janus face (Lyon, 2001) that favours care over control and social trust over surveillance.

Overview of the volume

The volume begins with **Maya Avis**' contribution in which she analyses the logic of *security as technological domination* that drives the Israeli security industry and contrasts this with the forms of resistance it encounters. With a focus on drones and cybersecurity, she calls attention to how the production of new surveillance and military technologies serves as a symbol of Israel's drive to technological dominance in the region. This dominance is reflected in a constant stream of footage from "successful" security operations, which are reflected in accounts by protagonists in the security complex who position themselves as defenders of democratic values and a bastion against terrorism in narratives laced with religious imagery. Avis shows how this self-perception serves to justify the export of new policing technologies, which are a central part of Israel's foreign relations. She contrasts these imaginations of technologies that can produce near-total control, with detailed attention to how they are experienced by Palestinians. Pointing to a variety of confusion tactics and the destruction of surveillance technology such as cameras and drones, she highlights how the expansion of technologically mediated surveillance and control increases frustration and mobilises solidarity and resistance. Stressing the logic of dominance packaged in Israeli conceptions of security, her account forces readers to reflect on what kinds of technology are appropriate for democratic societies. The resistance that comes with the intensification of surveillance spurs some hope that these trends are not inevitable.

While Avis's fieldsite is overflowing with evidence of resistance to technologically mediated state violence, **Andrea Miller**'s contribution highlights the centrality of their initial dismay at not finding any immediately recognisable forms of organised resistance to a newly developed $100 million Georgia Cyber Center in Augusta in the United States. The Georgia Cyber Center which brings together the military, law enforcement agencies, Augusta University, local government, and private companies is part of a regional redevelopment project. They focus their chapter on the *tear and shrug* of their interlocutors to their provocations about the redevelopment ambitions of the centre and show how these gestures contain within them significant, if hard to understand, forms of resistance. Their account is a methodological provocation about the importance of engaging ethnographically with apparently banal technological objects and concepts, like cybersecurity, because their banality masks their role in facilitating state violence through the expansion of police powers.

Based on ethnographic material collected in Kenya in 2017/2018, **Tessa Diphoorn** traces a newly introduced digital system to file complaints about public officials including law enforcement officers. Funded by Western states and non-governmental organisations (NGOs), the new technology is part of a larger policy effort of police reform and increasing public sector transparency in accordance with global policy ideals. Her fieldwork demonstrates how *digitalisation alone cannot fix broken bureaucracies*. Funding problems impact the technical functioning of the system, and the work of bureaucrats is complicated by parallel reporting structures and mistrust between state institutions. Perhaps most importantly, citizens, the imagined users of the system, do not know about it, do not trust its promise of anonymity, and prefer personal interaction with a dedicated contact that guides them through the complaints process. Diphoorn thus highlights the discrepancies that emerge between a national narrative of modernisation through digitisation and the many people in Kenya who are still disconnected from digital services.

In his ethnography of a surveillance control room in Ensenada, a small city in Argentina, **Martín Javier Urtasun** attends to the hopes and fears of surveillance workers anticipating the arrival of facial recognition technology. His work highlights the relevance of *scale in surveillance* and its relation to global trends. The surveillance workers he engages with pride themselves on "surveillance with a human face" – their ability to recognise individuals in the video footage and, given their intimate knowledge of the context, provide an appropriate interpretation of their behaviour. While they engage with the same common, polarised narratives between dreams of technological progress and fears of authoritarian dystopia, their familiarity with the surveillant assemblage allows them to have a more practical discussion around the uses, effectiveness, morality, and power effects of the expected arrival of facial recognition technology. This is a discussion that raises doubts about the replacement of their role in the assemblage and foreshadows a field of struggle between the low-level surveillance workers and the technologists in management positions.

Simon Egbert and **Maximilian Heimstädt** observed the operation of the German place-based predictive policing software PRECOBS in 11 police departments in Germany and Switzerland. They examine the different elements of *predictive policing as a chain of translation*, an iterative socio-technical process of police patrol, data generation, data analysis, and dissemination of predictions. With different elements of this process occurring simultaneously in multiple locations, they reflect on the difficulties of observing its operation ethnographically and suggest a team-based approach to address this. In Egbert and Heimstädt's account, predictive policing is applied in the context of media attention to high burglary rates, which have turned burglary into a political problem. Supported by reliable reporting of burglaries that are incentivised by the necessity of a police report for making an insurance claim, the main source of concern they identify lies in the possibility of police patrols targeting ethnic minorities with the added confidence of being in an area of predicted crime.

By contrast, this problematisation of place-based policing becomes more pronounced in a different context. **Shivangi Narayan** provides a detailed analysis of the ways in which police data that underlies New Delhi's crime maps and future predictive policing system is shaped by preconceptions about people living at the margins of society as being "prone to crime". Following police officers, particularly those of New Delhi police's mapping division, she describes the complex relationship between the police and the marginalised for whom the emergency call centre is often the only way to gain attention from the state. This, together with the absence of an address database and the regular attribution of crime to areas that house the most marginalised, leads to crime maps reinforcing theories of the poor as criminals. Narayan's account insists on attending to pre-existing *conditions and histories of inequality* when considering new digital policing techniques. Moreover, it adds to the problematisation of objectivity by pointing to the entanglement of mechanical objectivity and frames of interpretation. She asks whether it is the map that locates crimes in poor areas that is the problem or whether the problem relates to the interpretative frame of those who record crimes and interpret the maps. The nuance of her ethnography prompts the reader to reflect on the entanglement of factors shaping the relationship between policing and poverty in New Delhi.

Staying with the subject of software that predicts likely locations for future crimes, **Daniel Marciniak** thematises the democratic deficits that come with an *infrastructure shortcut* when police departments rely on private companies to provide and maintain their technical infrastructure. He draws on conversations with technology leads in UK and US police forces and developers in companies developing predictive policing solutions, as well as visits to security trade fairs. Centring his analysis on the expansion of cloud infrastructure in policing during the COVID-19 pandemic, his analysis reveals how this change shifts the role of private companies from providing the tools of policing and surveillance (police cars, surveillance cameras, etc.) to creating software that generates the knowledge that shapes police actions (predictive policing, facial recognition, and data dashboards). He points to the often concealed work of iterative technological innovation and continued technical maintenance that makes a private provision of these tools attractive to police. The chapter illustrates how the technicality of maintenance and design of policing software contains ongoing normative deliberation around what policing should do and problematises that this happens behind closed doors. He highlights the need to consider how interpretative frames for police data evolve when the expertise is outsourced to software companies.

Mark Maguire and **David Westbrook** take us into the exclusive training settings of elite counterterrorism special forces in the UK, France, Ireland, and Kenya. Contrasting these with accounts given by survivors of terrorist incidents, they show how training programmes for elite counterterrorism units rely on styles of reasoning that reduce the chaotic reality of terror attacks into neat scenarios – a *boxology* of knowable actions and reactions. This (overly) simplified reasoning opens counterterrorism training to simulations in the experimental fields of AI and X-Reality technology. Acknowledging the utility of the simplifications of counterterrorism scenarios for the training of special forces to deal with the life-and-death situation of a terror incident, their work brings attention to the flawed data, poor-quality theories, and exaggerated expressions of human behaviour that underpin these technologies.

References

Amoore, L. (2006) 'Biometric Borders: Governing Mobilities in the War on Terror', *Political Geography*, 25(3), 336–351.

Ball, K.S. *et al.* (2006) 'A Report on the Surveillance Society. For the Information Commissioner by the Surveillance Studies Network', *Surveillance Studies Network*, 98. Available at: https://ico.org.uk/media/about-the-ico/documents/1042390/surveillance-society-full-report-2006.pdf (Accessed: 13 July 2023).

Ball, K.S. and Wood, D.M. (2013) 'Political Economies of Surveillance', *Surveillance & Society*, 11(1/2), 1–3.

Beer, D. (2016) *Metric Power*. London: Palgrave Macmillan.

Benjamin, R. (2019) *Race After Technology: Abolitionist Tools for the New Jim Code*. Cambridge: Polity Press.

Brayne, S. (2021) *Predict and Surveil: Data, Discretion, and the Future of Policing*. New York, NY: Oxford University Press.

Brayne, S. and Christin, A. (2020) 'Technologies of Crime Prediction: The Reception of Algorithms in Policing and Criminal Courts', *Social Problems*, 68(3), 608–624.

Broeders, D. (2007) 'The New Digital Borders of Europe: EU Databases and the Surveillance of Irregular Migrants', *International Sociology*, 22(1), 71–92.

Browne, S. (2015) *Dark Matters: On the Surveillance of Blackness*. Durham, NC: Duke University Press.

Chan, J.B.L. (2001) 'The Technological Game: How Information Technology is Transforming Police Practice', *Criminal Justice*, 1(2), 139–159.

Christin, A. (2020) 'The Ethnographer and the Algorithm: Beyond the Black Box', *Theory and Society*, 49(5), 897–918.

Colton, K.W. (1979) 'The Impact and Use of Computer Technology by the Police', *Communications of the ACM*, 22(1), 10–20.

Crawford, K. (2021) *Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence*. New Haven: Yale University Press.

Daston, L.J. and Galison, P. (2010) *Objectivity*. New York, NY: Zone Books.

Deflem, M. and Chicoine, C. (2014) 'History of Technology in Policing', in G. Bruinsma and D. Weisburd (eds.) *Encyclopedia of Criminology and Criminal Justice*. New York, NY: Springer, 2269–2277.

Deleuze, G. (1992) 'Postscript on the Societies of Control', *October*, 59, 3–7.

Egbert, S. and Leese, M. (2020) *Criminal Futures: Predictive Policing and Everyday Police Work*. Abingdon/New York: Routledge.

Ericson, R.V. and Haggerty, K.D. (1997) *Policing the Risk Society*. Oxford: Clarendon Press.

Espeland, W.N. and Sauder, M. (2007) 'Rankings and Reactivity: How Public Measures Recreate Social Worlds', *American Journal of Sociology*, 113(1), 1–40.

Eubanks, V. (2018) *Automating Inequality*. New York, NY: St Martin's Press.

Fassin, D. (2017) 'Ethnographying the Police', in D. Fassin (ed.) *Writing the World of Policing: The Difference Ethnography Makes*. Chicago/London: University of Chicago Press, 1–32.

Feierman, S. *et al.* (2010) 'Anthropology, Knowledge-Flows and Global Health', *Global Public Health*, 5(2), 122–128.

Ferguson, A.G. (2017) *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*. New York, NY: New York University Press.

Gandy, O.H. (1993) *The Panoptic Sort. A political Economy of Personal Information*. Boulder, CO: Westview.

Gandy, O.H. (2009) *Coming to Terms with Chance: Engaging Rational Discrimination and Cumulative Disadvantage*. Aldershot: Ashgate.

Gilliom, J. (2001) *Overseers of the Poor: Surveillance, Resistance, and the Limits of Privacy*. Chicago: University of Chicago Press.

Gilliom, J. and Monahan, T. (2012) 'Everyday Resistance', in K. Ball, K. Haggerty, and D. Lyon (eds.) *Routledge Handbook of Surveillance Studies*. Hoboken: Taylor & Francis (Routledge International Handbooks), 404–410.

Guilfoyle, S. (2012) 'On Target?–Public Sector Performance Management: Recurrent Themes, Consequences and Questions', *Policing*, 6(3), 250–260.

Haggerty, K.D. (2006) 'Tear Down the Walls: On Demolishing the Panopticon', in D. Lyon (ed.) *Theorizing Surveillance: The Panopticon and Beyond*. Cullompton: Willan Publishing, 23–45.

Haggerty, K.D. and Ericson, R.V. (2000) 'The Surveillant Assemblage', *The British Journal of Sociology*, 51(4), 605–622.

Harper, R.R. (1991) 'The Computer Game: Detectives, Suspects, and Technology', *British Journal of Criminology*, 31(3), 292–307.

Hayes, B. (2012) 'The Surveillance-Industrial Complex', in K. Ball, K. Haggerty, and D. Lyon (eds.) *Routledge Handbook of Surveillance Studies*. Hoboken: Taylor & Francis (Routledge International Handbooks), 167–175.

Hogan, M. (2018) 'Big Data Ecologies. Landscapes of Political Action', *Ephemera. Theory & Politics in Organization*, 18(3), 631–657.

Holmes, D.R. and Marcus, G.E. (2008) 'Collaboration Today and the Re-Imagination of the Classic Scene of Fieldwork Encounter', *Collaborative Anthropologies*, 1(1), 81–101.

Huey, K., Walby, A. and Doyle, L. (2006) 'Cop Watching in the Downtown Eastside: Exploring the Use of (Counter)Surveillance as a Tool of Resistance', in T. Monahan (ed.) *Surveillance and Security. Technological Politics and Power in Everyday Life*. New York: Routledge, 149–166.

Kazansky, B. (2021) '"It Depends on Your Threat Model": The Anticipatory Dimensions of Resistance to Data-driven Surveillance', *Big Data & Society*, 8(1), 1-12.

Kitchin, R. (2017) 'Thinking Critically about and Researching Algorithms', *Information, Communication & Society*, 20(1), 14–29.

Latour, B. (1994) 'Where Are the Missing Masses? The Sociology of a Few Mundane Artifacts', in W.E. Bijker and J. Law (eds.) *Shaping Technology/Building Society: Studies in Sociotechnical Change*. Cambridge, MA: MIT Press, 225–258.

Latour, B. (2004) 'Why Has Critique Run Out of Steam? From Matters of Fact to Matters of Concern', *Critical Inquiry*, 30(2), 225–248.

Lum, K. and Isaac, W. (2016) 'To Predict and Serve?', *Significance*, 13(5), 14–19.

Lyon, D. (2001) *Surveillance Society: Monitoring Everyday Life*. Buckingham; Philadelphia: Open University Press.

Lyon, D. (ed.) (2003) *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination*. Abingdon: Routledge.

Mann, S., Nolan, J. and Wellman, B. (2003) 'Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments', *Surveillance & Society*, 1(3), 331–355.

Manning, P.K. (2008) *The Technology of Policing: Crime Mapping, Information Technology, and the Rationality of Crime Control*. New York: New York University Press (New perspectives in crime, deviance, and law series).

Marcus, G.E. (1995) 'Ethnography in/of the World System: The Emergence of Multi-Sited Ethnography', *Annual Review of Anthropology*, 24, 95–117.

Marx, G.T. (2002) 'What's New About the "New Surveillance"? Classifying for Change and Continuity', *Surveillance & Society*, 1(1), 9–29.

Marx, G.T. (2003) 'A Tack in the Shoe: Neutralizing and Resisting the New Surveillance', *Journal of Social Issues*, 59(2), 369–390.

Marx, G.T. (2015) 'Surveillance Studies', in J.D. Wright (ed.) *International Encyclopedia of the Social & Behavioral Sciences (Second Edition)*. Amsterdam: Elsevier, 733–741.

Marx, G.T. (2016) *Windows into the Soul: Surveillance and Society in an Age of High Technology*. Chicago/London: The University of Chicago Press.

McCahill, M. (2021) 'Theorizing Surveillance in the Pre-Crime Society', in B.A. Arrigo and B.G. Sellers (eds.) *The Pre-Crime Society: Crime, Culture and Control in the Ultramodern Age*. Bristol: Bristol University Press, 227-248.

Merry, S.E. (2011) 'Measuring the World: Indicators, Human Rights, and Global Governance: with CA comment by John M. Conley', *Current Anthropology*, 52(S3), S83–S95.

Monahan, T. (2015) 'The Right to Hide? Anti-Surveillance Camouflage and the Aestheticization of Resistance', *Communication and Critical/Cultural Studies*, 12(2), 159–178.

Monahan, T. and Fisher, J.A. (2015) 'Strategies for Obtaining Access to Secretive or Guarded Organizations', *Journal of Contemporary Ethnography*, 44(6), 709–736.

Nader, L. (1972) 'Up the Anthropologist: Perspectives Gained From Studying Up', in Dell Hymes (ed.) *Reinventing Anthropology*. New York: Pantheon, 284–311.

O'Neil, C. (2016) *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. London: Allen Lane.

Ortner, S.B. (2010) 'Access: Reflections on studying up in Hollywood', *Ethnography*, 11(2), 211–233.

Porter, T.M. (1996) *Trust in Numbers: The Pursuit of Objectivity in Science and Public Life*. Princeton: Princeton University Press.

Rabinow, P. (2008) *Marking Time: On the Anthropology of the Contemporary*. Princeton: Princeton University Press.

Rottenburg, R. *et al.* (eds.) (2015) *The World of Indicators: The Making of Governmental Knowledge through Quantification*. Cambridge: Cambridge University Press (Cambridge Studies in Law and Society).

Sandhu, A. (2019) '"I'm Glad That Was on Camera": A Case Study of Police Officers' Perceptions of Cameras', *Policing and Society*, 29(2), 223–235.

Scheel, S. (2019) *Autonomy of Migration?: Appropriating Mobility within Biometric Border Regimes*. Abingdon, Oxon/New York, NY: Routledge.

Seaver, N. (2017) 'Algorithms as Culture: Some Tactics for the Ethnography of Algorithmic Systems', *Big Data & Society*, 4(2), 1–12.

Smith, G.J.D. (2015) *Opening the Black Box: The Work of Watching*. Abingdon, Oxon/New York, NY: Routledge, Taylor & Francis Group (Routledge advances in sociology).

Star, S.L. (1999) 'The Ethnography of Infrastructure', *American Behavioral Scientist*, 43(3), 377–391.

Stevens, A. *et al.* (2023) '"I Started Seeing Shadows Everywhere": The Diverse Chilling Effects of Surveillance in Zimbabwe', *Big Data & Society*, 10(1), 1-14.

Wilson, D. (2021) 'The New Platform Policing', in A. Završnik and V. Badalič (eds.) *Automating Crime Prevention, Surveillance, and Military Operations*. Cham: Springer International Publishing, 47–68.

Winner, L. (1993) 'Upon Opening the Black Box and Finding It Empty: Social Constructivism and the Philosophy of Technology', *Science, Technology & Human Values*, 18(3), 362–378.

Zuboff, S. (2019) *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. London: Profile Books.

Part 1

Navigating surveillance

Contending with promises of transformations

1 Shaping surveillance futures

Palestinian responses to Israeli surveillance technologies

Maya Avis

Introduction[1]

A detailed picture of the centrality of new technologies in the extensive Israeli surveillance apparatus in place across Palestine has been emerging as different parts of it are exposed through the cataloguing of the direct experience of Palestinians and in-depth investigations into the subject by civil society organisations, journalists, and researchers. For example, in May 2023, a report by Amnesty International uncovered a network of cameras used to extract biometric data from Palestinians at the countless Israeli checkpoints that exist throughout the West Bank, without their prior knowledge or consent (Amnesty International, 2023). Across the globe, digital technologies like these are increasingly being developed and used to manage not just protests but also other areas of life including work, leisure, retail, and movement. Recent years have seen the proliferation of new "smart" technologies and there is a multiplicity of possible roles and logics that can be embedded within them.

Most authors agree that the expanded affordances technological transformations have made available to the field of surveillance over the last decades are not neutral and include a certain degree of control and coercion even where the context is not one of military occupation (Marx, 2015; Monahan and Wood, 2018). Huang and Tsai (2022) explain how surveillance has become a "core function of modern nation-states" (p. 3). They note how the pre-emptive repression of actors and events that might seek to undermine the state became paramount to states' security to such an extent that public expenditure on policing in the 20th century increased "to match defence spending" (2022: 5). They explain that the significance of this is compounded by the way in which market incentives can lead to the overproduction of surveillance technologies.

Some existing research on new surveillance technologies calls to situate contemporary surveillance in longer histories of the control of populations. Despite the seemingly contemporary nature of the transformations taking place in surveillance, they argue that approaches to surveillance that centre the "novel" overlook the place of new technology in longer histories of the monitoring and control of marginalised populations (Zureik, Lyon and

DOI: 10.4324/9781003412908-3

Abu-Laban, 2010; Browne, 2015; Marx, 2015; Stevens *et al.*, 2023). Yet, regardless of how the topic is approached, there seems to be widespread consensus that our “world demands thoughtful and decisive action to assess and confront the emerging world of surveillance, which is everywhere and often discriminatory” (Lyon, 2022, p. 5). While an increasingly rich and diverse body of literature does consider how racism and bias are embedded in new digital technologies (Browne, 2015; O’neil, 2017; Noble, 2018; Benjamin, 2019a, 2019b), other authors have focused on the effect of technologies on the practice of surveillance and policing themselves (Brayne, 2020; Klauser, 2022). McCahill (2021) has suggested that an often overlooked subject in the literature on surveillance technology is “how data subjects experience and respond to being monitored by new surveillance technologies” (McCahill, 2021: 242). By “data subjects” he is referring to those who live under, alongside, and despite new and changing regimes of surveillance.

This chapter considers the development of new surveillance technologies in the context of Palestine/Israel, where they have become increasingly central to maintaining the Israeli occupation (Zureik, 2016a) as well as to Israel’s economic and geopolitical standing (Loewenstein, 2023). Israel has been increasingly positioned as a key global player in the field of security and relatedly of surveillance (Khalili, 2010; Grassiani, 2017, 2018, 2022; Machold, 2018; Sa’di, 2021; Loewenstein, 2023). The first part of the chapter situates Israel within the broader ecosystem of the development and marketing of what can be broadly defined as surveillance technology. It sheds light on the Israeli approach to security, which perceives security as a kind of technological arms race, in which technological domination and innovation are intrinsic to security. I call this logic *security as technological domination* and argue that it is embedded in the way new technology is conceptualised. The relationship of this logic to the Israeli military–industrial complex, exports of Israeli technologies, and Israeli diplomacy helps to explain the air of inevitability that haunts new surveillance technology.

The chapter goes on to examine “responses” to these technologies and, in particular, instances of Palestinian rejection of the expanding use of new digital technologies of control and surveillance. This second part of the chapter highlights how significant populations’ reactions to surveillance technologies are to their study. The focus is specifically on instances in which new technologies are destroyed or sabotaged. These instances contradict dominant paradigms, which imagine these technologies as contributing to state security. The chapter gives insight into how these technologies are being contested and considers what that means for the logic of *security as technological domination* and surveillance futures both in Palestine and beyond.

The chapter addresses a variety of Israeli technologies used in the control and surveillance of Palestinians and considers both how they project power and how that power and domination come to be opposed and rejected. The specific relationship between drones and domination has been explored by a number of authors who address the role of drones and their operators in projecting power and sovereignty (Williams, 2011; Weizman, 2012; Neocleous, 2013; Parks and Kaplan, 2017; Kaplan and Miller, 2019; Miller, 2019). Much of this literature considers large Reaper-style unmanned aerial vehicles (UAVs), which are different from the lightweight, often camera-fitted drones used by law enforcement today and which are one of the technologies included in this chapter.

I propose that surveillance futures can be shaped by responses and public pressure to new technologies as well as in boardrooms and closed meetings. I do not intend to flatten or overlook power asymmetries – in fact this chapter addresses technological asymmetry in great detail – but rather to argue that publics can and do refuse to live with or rely on the use of extractive and invasive new technologies promoted for their benefit and “safety”. Even momentary acts of the sabotage and destruction of new surveillance technologies can be read as demands for real and democratic solutions to the social and political problems the presence of technology is supposed to resolve. New surveillance technologies are often portrayed in showrooms as somewhat “frictionless”, but their impact on the lives of those who are their everyday targets is marked, and this has serious consequences for social order and state security. The chapter shows how, rather than strengthening Israel’s security, the use of powerful surveillance tools and the repression of protest can increase opposition to Israeli rule.

The chapter draws on extensive ethnographic research carried out primarily in Palestine/Israel between 2021 and 2023, as well as previous research in the region. The data collection comprised in-depth participant observation and digital ethnography conducted in a variety of online and offline research sites, including at trade fairs for advanced digital technologies and industry events often organised with and for law enforcement professionals. For example, I attended the *24th European Police Congress*, in Berlin, Germany, and *ISDEF 2022* and *Cybertech Global 2023*, which both took place in Tel Aviv, Israel. In addition to these fairs, other important research sites were professional workshops and tech demonstrations such as those organised by the Israel National Drone Initiative (INDI) (online and in Tel Aviv in 2021) and hybrid conferences like one that addressed the impact of the Pegasus Project affair (Herzliya, Israel, 2023). Palestinian-led protests and direct actions (such as the Great March of Return in 2018) were also central to the research as were interviews with industry personnel, lawyers, journalists, and Palestinian and Israeli activists and civilians, from Jerusalem, Haifa, Tel Aviv-Jaffa, the Naqab, Masafer Yatta, and the Jordan Valley. These various observations and interviews were complemented by the collection and analysis of secondary sources, including social media content, media reports, and commercial materials presenting Israeli technology to international customers.

Technological domination: from press release to product performance

During the 2018 Palestinian Great March of Return Palestinians used kites and balloons – which came to be known in Israel as *terror kites* and *arson balloons* – to set fire to Israeli agricultural fields. These kites were basic incendiary devices that had Molotov cocktails attached to them. At this time, I found one of these large, awkward hexagonal kites, nearly two metres wide and made from a clear plastic sheet stapled to narrow wooden beams. Its tail was comprised of small strips of paper with phrases and poems about flight and freedom written on them. The object was simple. Its materiality indicated the kite's role as both messenger and weapon. The poetic phrases on its tail spoke of particular hopes while the destructive element of its form caused significant damage to Israeli crops and vegetation on the Israeli side of the barrier built by Israel to separate it from Gaza.

According to the website of an Israeli drone manufacturer, these *terror kites* were the inspiration behind a product aptly named *Skylord*. The website explained that the company was founded in 2018, when the founder of the Israeli Drone Racing League "translated his passion [for drones] into meeting the incendiary balloons threat on the Israeli-Gaza border" (Xtend, no date). The company boasts that it came to produce drones that could be flown by means of a VR headset, significantly reducing the need for training. The drones could therefore quickly turn Israeli soldiers into kite and balloon-catching cyborgs. According to the company's website, the Skylord "puts human intelligence and machine autonomy together to superpower soldier's abilities". Part of the company's stated vision was to "break the limits of physical reality, so our lives will no longer be limited by our locations or our capabilities – only by our imagination". The hyperbole of this description of the drones' abilities and its name is characteristic of the language and mindset I encountered during my research into new digital technologies in Palestine/Israel. The drive to conquer, control, and exceed boundaries was not unique to this company or product, and many similar products exist and are characterised in comparable ways in marketing materials. The representation of the outstanding creativity of an individual, heroic, tech entrepreneur is also not confined to the marketing of this particular product. The narrative of triumph and conquest-through-ingenuity reflects a more general narrative about Israel's technological supremacy over the threats it faces. The so-called terror kites stand in stark opposition to these drones. In contrast to the low-tech, improvised technology of the makeshift kites, the sophisticated drones represent the epitome of what Miller has described as the "imperial fantasy of perfectly asymmetrical warfare" (Miller, 2019: 94), something which highlights the limited nature of political imagination beyond domination by technologically driven surveillance and policing tools.

This example depicts a single drone flown by an individual operating at a distance. This is a reality that changed during the course of my research, and by May 2021 the Israeli military boasted that it had deployed AI-operated swarms of drones in Gaza, tasked with collecting information that was then analysed and processed using machine learning. The bombardment of the Gaza Strip in May 2021 was described by the Israeli army in its aftermath as "the first AI war", in part because of the way in which swarms of drones operated in unison to collect data that was then processed by programs with mythical names like "Alchemist", "Gospel", and "Depth of Wisdom" (Ahronheim, 2021; Gross, 2021). Reports about the Israeli aggression focused on how machine learning had combined different kinds of intelligence data (from signal, visual, geographical, and human intelligence) in new operation rooms that were able to produce "hundreds of targets relevant to developments in the fighting, allowing the military to continue to fight as long as it need[ed] to with more and more new targets" (Ahronheim, 2021). Target selection is a difficult and time-consuming process for militaries, and this breakthrough in target selection is significant. The Israeli army publicly acknowledged many of these "breakthroughs" – such as its use of swarms of drones and automated target selection – for the first time in May 2021 (Hambling, 2021). Since May 2021, the use of AI by the Israeli military has been increasingly publicly acknowledged.

May 2021 was a significant period in Palestine/Israel and is referred to alternately as *Habat al Karama* (the Dignity Uprising), and the Unity Intifada, among other things. It is considered by many to be a watershed moment for a number of reasons. Characterised by intensified protest and repression in many Palestinian towns and cities inside Israel including Jerusalem, Akka, Haifa, and Lydda (known as Lod in Hebrew), this moment has been described as "one of the crucial events of the Palestinian struggle against Israeli settler colonialism" (Nasasra, 2022: 330) due to the unified nature of the Palestinian response to years of repression and occupation. The scope and intensity of the "unrest" marked this period as a significant historical moment.

The way new technologies were used and acknowledged during this heightened period of Palestinian uprising provides an insight into the Israeli security logic and its relationship to technological domination. At the height of the uprising, one of the statements put out by the Israeli police included a 49-second video that was sent to foreign press via a WhatsApp group set up by the police. The video was edited to tell a story of success: in a scene filmed from above, a man is seen running. He throws a stick into a burning bin before the video cuts to a new scene. Here we see the man inside a red circle as he walks down a street. The circle seems to mark the man as a suspect. The same view from above follows "the suspect" until he reaches a house. He enters the house and disappears out of sight. The video cuts again and now a police car arrives outside the house, and two policemen go into the house and the video ends. This short sequence was circulated together with the following caption:

> *"Police foreign press Spokeman [sic]*
> *Police units in the area of Jaffa use drone[s] to search track and assist Special patrol units on the ground to arrest a suspect involved in disturbances.*

> *Police units on the ground searched, chased and arrested the suspect who set fire wit [sic] property".*[2]

Viewers were provided with the drone's perspective of the arrest. The police soon gave a name to this wave of arrests they had been carrying out, in response to the uprising: *Operation Law and Order*.[3] Local newspaper reports indicated that the "operation [would] incorporate all the existing operational capabilities and technologies" (Senior and Morag, 2021).

Statements about Israeli technological capabilities are a routine part of how Israeli security forces operate and present themselves in the media. Footage like the video of the drone in Jaffa often accompanies the written statements put out by the different Israeli forces after their operations whether they are carried out in Gaza, the West Bank, or inside Israel. These visual materials, which can include photos and videos, serve as a kind of proof of Israeli (technological) capabilities and dominance. They are designed to tell a story about how Israeli technological dominance produces security, something which is not just related to the domination of Palestinians but also used to position this technology as a battle-tested product for sale and export (Loewenstein, 2023). The official output is part of an attempt to dominate both Palestinians and the security technology market, as this chapter will now explain.

Erella Grassiani has described the process by which "security experience becomes security capital" in the development of an *Israeli security brand* (Grassiani, 2017: 16). She explains how this capital is used to sell Israeli technology and expertise as high-quality and effective. She describes how "Israel" becomes a brand that ensures the quality of a particular technology. The public discourse that accompanies the use of new technologies of control and surveillance by Israeli law enforcement agents projects the success of the Israeli logic of *security as technological domination*. The Israeli state constantly *performs* the technological domination of Palestinians through the publication of information about the success of its advanced technology (such as in the example of the arrest above). Presenting operational accomplishments in this way plays an important part in Israel's self-representation as able to exist and dominate a "hostile region" through its technological sophistication.

Establishing and exporting the myth of technological domination

Israel's self-representation as a technological leader was especially pronounced at a three-day trade fair called *Cybertech Global 2023*. During a panel called *8200 Unit, Entrepreneurial Secrets,* I could see first-hand how Israeli security experience was translated into capital (Grassiani, 2017, 2018, 2022), and I understood more about how the myth of Israel's technological supremacy is constructed. The blurb for the event described Unit 8200 as "an elite intelligence unit strongly associated with priming Startup Nation's future tech entrepreneurs". The event promised to be "a lively and intimate discussion uncovering the secrets of Unit 8200 – secrets that allow its alumni to build Israel's most successful cybersecurity companies". The panel tied the unit's success to the urgency of the obligation for victory in Israel's fight against terror.

Towards the end of the session, someone asked about what elements the UK was missing for the establishment of a similarly successful technology industry. One of the panellists replied that the difference was that in the UK 18-year-olds do not go through a nationwide screening process that selects the brightest minds for a compulsory three-year training programme (i.e., the army). Everyone laughed. A second panellist continued that the difference between Israel and the UK was that "France doesn't want to conquer you!", at which the room erupted in laughter again. The same panellist went on to explain that Israel is small and that running from east to west takes less than an hour in some places. He noted that this lack of "strategic depth" meant that "tanks could be here, in Tel Aviv, in less than 40 minutes if Israel was invaded". The speaker painted an evocative picture of how this meant that the unit needed to develop the technical and intelligence advantage that would enable it to locate enemy tanks before they even switched on their engines, and isolate terrorists before they left their houses. His descriptive answer impressed upon the audience the necessity of a pre-emptive logic and technological superiority. He explained that strong cybersecurity and intelligence are how Israel defends itself. Throughout the discussion the focus was on the development of technological excellence, which the unit's alumni could then take with them into different parts of the extensive global security industry.

The military's importance in the development cycle of new technologies can indeed not be overstated. This is partly related to the revolving door between the industry and the military and is confounded by the prevalence of military reserve duty in fields related to the development of new technology. An article in an Israeli newspaper boasted that one industry professional was able to get his product "from the first concept, scribbled on paper" to it being "demonstrated to the first customer" in less than four and a half months because of the short development cycles that result from the army reserve duty that many Israelis perform (Lavallée, 2019). As the article made clear,

> *"In Israel all the people (in the industry) are ex-army soldiers, officers. The engineers who work on the development of the systems are actually operating the UAVs in the (military) reserves, in actual service. Then they come back to the office with actual and real-time feedback" (ibid).*

Many other links exist between the military and these industries, and this has been the subject of many fascinating accounts (Khalili, 2010; Zureik, 2016b;

Grassiani, 2017, 2018, 2022; Machold, 2018; Talbot, 2020; Adams, 2021; Sa'di, 2021; Who Profits, 2021, n.d.).

The comparison that was made between Israel and international superpowers, like France and the UK, distils the creation of the myth of Israel's technological supremacy, according to which the "brightest minds" protect a dramatically small country under constant threat of terrorism through pre-emptive vigilance and action, carried out by smart technology able to ensure the management of threats. This triumphant "tech victory" can then indeed be transformed into exportable capital. The Pegasus affair, which is the focus of the next section, exemplifies this myth further.

Diplomacy and the justification of technological domination

While the previous sections focused on hardware (like drones), the Israeli technology/security industry is also, and perhaps especially, famed for software. This is significant to the myth of security as technological domination because whereas hardware is often visibly violent, even when operated remotely, software has a more insidious relationship with domination because it is represented as a more moral, accurate, and inevitable path to security. By producing autonomous, precise, and fair prediction tools, technology is seen as the solution to biased and violent methods of policing and control.

In July 2021, the publication of the Pegasus Project investigation revealed that Pegasus spyware was being exported to countries around the world, often as part of a strategy for strengthening diplomatic ties. Pegasus is a software developed by the Israeli company NSO Group which can "infect" a person's phone and make its data (such as text messages, calls, passwords, locations, contacts, and even the device's camera and microphone) available to whoever installed the spyware, without the device's owner being aware. Many organisations and investigations have addressed the way in which Israeli technology has been used to "pave the way for diplomatic relations and international cooperation" (Who Profits, 2021: 4). An Israeli lawyer who brought a legal case against NSO in 2020 explained to me that this relationship between the development of Israeli technology and diplomacy has a precedent. He highlighted that this strategy of exporting technology for diplomatic gains builds on "a long history of water drip and weapons diplomacy" in which Israel exports its technological innovations for political benefit. He explained that historically, agricultural and irrigation technology were important components of this strategy, though he emphasised that weapons have also always played an important part in Israeli diplomacy.

A product designer responsible for the visual presentation of products at industry trade fairs confirmed that they had travelled to the Gulf for product demonstrations with spyware firms in advance of the 2021 Abraham Accords, which were a series of normalisation deals between Israel and a number of countries in the region. The agreement between the United Arab

Emirates (UAE) and Israel, on 13 August 2021, normalised relations between the two countries, and in the first six months after normalisation, Israeli exports to the UAE surpassed 500 million USD (Who Profits, 2021). On 14 November 2021, Elbit Systems, considered the largest Israeli military manufacturer, announced the opening of a new subsidiary, Elbit Systems Emirates (ESE), in the Gulf state (Zaken, 2021). Eilat Maoz has written compellingly about the role of economics and ideology in the context of the Abraham Accords (Maoz, 2020).

In January 2023, during a one-day event held at Reichmann University, Israel's only private university, the use and export of offensive spyware like Pegasus received attention from a host of speakers, some of whom bore direct responsibility for its development, use, and export. The event was called, *Between Pegasus and Predator: When Is It Allowed and How Is It Forbidden to Use Offensive Cyber?* It was framed as a moment of reckoning for the industry. The event asked how these "tools" should be regulated both "at home" and abroad and took place almost entirely in Hebrew. The tone of the discussion largely cemented an inevitability with respect to the development and deployment of new surveillance technologies, despite the presence of a number of more critical speakers, including a research fellow from Citizen Lab, involved in the Pegasus Project investigation.

Other notable individuals among the panellists included the CEO and founder of NSO, Shalev Hulio. He was part of a panel called, *Light to the nations? Ethics, democracy and national security in the export regulations for offensive cyber*. "Light to the nations" is a biblical term related to the idea of Jews as spiritual guides or mentors. Much of the discussion, especially in this panel, was about the need for offensive spyware now that the web had "gone dark" to law enforcement. The constant references to light and dark and the religious themes extended beyond the messianic touch of the session's title. When it was his turn to speak, Hulio jokingly said that where the Bible held that "from Zion shall come forth Torah", today it was not Torah but *toh-nah* (תוכנה), which means "program" in Hebrew. The audience tittered before a more critical speaker on the panel interjected *roglah (*רוגלה*),* which is Hebrew for "spyware". These biblical references reflect Zionist narratives which link today's Israel to the biblical period. This variable yet reoccurring theme of the inevitable progress and triumph of technology depicted as a biblical light over the darkness (and good over evil) gestures towards the tendency to imagine technological progress as an inevitable part of a divinely dictated "progress", leading to a more enlightened and "civilised" world. This reasoning bears a stark resemblance to colonial notions of progress and enlightenment as Adams (2021) has noted. Moreover, the accuracy of this technology in relation to its targets was emphasised with the justification that most of us "have nothing to hide". This technology was portrayed as necessary in the fight against terrorists, crime lords, and often also paedophiles.

Together these themes of the inevitability of technological progress and its inherent virtue and accuracy contribute to Israel's self-perception and diplomatic positioning of itself as a leader of technological progress in a civilised world. This is a paradigm to which subjects of surveillance respond when they break, disrupt, or evade new digital technologies of control and surveillance. These technologies are justified as inevitable, accurate, and "civilised" alternatives to violent histories of population control. However, to those exposed to these technologies, such a paradigm hides that this technology – whether it is spyware, drones, or face recognition systems – is a small part of a larger oppressive system trying to disguise its violence in objective target selection. It is perceived not as an alternative but as a continuation of violent practices of control and surveillance. As the next part of the chapter will show, claims of the inevitability of the development of this technology and its higher rates of objectivity and accuracy are rejected by populations exposed to these advanced technologies in ways that highlight the masked violence of these "breakthroughs" and the limits of its underlying paradigm of security.

Drones, phones, and stones: response and solidarity

This part of the chapter shifts the discussion to how these technologies affect Palestinian lives and their right to protest and, importantly, addresses one of a range of possible responses to this technology – its sabotage and destruction. In particular, this part of the chapter is concerned with attempts to hamper surveillance technologies from functioning correctly and the impulse to destroy Israeli surveillance capabilities entirely. There are of course other possible "responses" to new technologies as I explain but I focus on this because I propose that it best encapsulates the false economy of surveillance technologies. Rather than reducing "friction", I propose that these technologies are seen by many subjects of surveillance, especially in settings of pre-existing injustice, as the expansion of surveillance, repression, and control. This additional layer of technological domination can then further galvanise target populations to defend themselves and organise specifically against this new aspect of repression. Rather than a distinction between everyday and organised resistance (Gilliom and Monahan, 2012), I suggest that even seemingly "small" responses to surveillance technologies build solidarity among people locally and internationally and in so doing strengthen criticism of this form of governance and thus can shape surveillance futures.

Differing technological subjectivities

On 5 March 2021, in the rolling green hills of spring in the Jordan Valley in the northern West Bank, a Palestinian shepherd described how Israeli settlers had been regularly using drones to intimidate the communities in the area by scaring his flocks and harassing the communities with the drones. He explained that the settlers constantly spied on him and his flocks with small drones and summoned the army if the flocks strayed into one of the many areas designated as "closed military zones" as part of the Israeli strategy to clear Area C of the West Bank of Palestinian communities.[4] The shepherd recounted how, with the use of drones and the help of the army, a few settlers were able to control huge swathes of land outside their settlement, without being physically present themselves. In a vivid description of the scenario, he recounted how,

> the drone is used several times a week, though usually we do not see the settler. He operates it remotely from his home. The sheep are scared and run away because of the noise. They fly the drone at a height of 20–30 meters, so there is nothing we can do.

When I inquired further about the impact of the drone on the sheep, he clarified that,

> the sheep do not get used to the noise [of the drones]. They continue to run away every time it comes. They [the settlers] also take pictures of the land and with the noise, scare the herds. The sheep have suffered miscarriages because of the noise. Obviously, what they do is illegal, but they work with the military so there is nothing we can do.

The shepherd showed pictures and videos of the drones operated by the settlers. An investigation into the phenomenon revealed that the Israeli government had transferred some 20 million shekel to settlers in the West Bank for the monitoring and detection of Palestinian construction in Area C of the West Bank (Ziv, 2022). The investigation exposed that some of these funds were used to purchase at least 21 drones at a cost of approximately 25–36,000 shekel each (up to about 10,000 USD per drone), as well as providing funding for training the settlers to fly them. The specific drones that bothered the shepherds I interviewed may not have been these state-funded drones, but the practice of using drones to surveil and harass Palestinian communities intensified during the course of my research. The shepherd explained that this practice "allows the settlers in our area to control more and more land. They control more than a 1,000 *dunams*[5] so far and also go down and throw stones directly at the sheep". He clarified that the settlers "also fly the drones in the area of our houses and scare the kids". Another shepherd also present during the interview chimed in and emphasised that, "in recent years, settlers have come to five places nearby and from each one they are controlling thousands of dunams".

This relationship between the drones and daily life for one marginalised community illustrates how this specific technology has become part of the wider practice of surveillance and dispossession, which unites drones, the military, and the settlers in the West Bank. The settlers are no longer limited by their physical locations and can use the drones to extend the reach of their intimidation and control. The drones are one feature in a reality in which Israeli settlers in the West Bank systematically attack Palestinians and their property. Where these attacks were consistent, residents have left their homes and the settlers succeeded in their aim of the ethnic cleansing of whole areas comprising numerous villages (B'Tselem, 2021; Ziv, 2023). In the accounts provided by the shepherds, the drones reproduced and exacerbated the disruptive reality of the occupation by generating a particular subjectivity of domination, through the use of the airspace around the shepherds, their families, and their livestock. The settlers' use of the drones is intended to enforce the shepherds' compliance and resignation to the Israeli occupation, while also serving to de-personalise the violence and protect the settlers' identities. In the case of the West Bank, where the lines between settlers and the military are already somewhat blurred (B'Tselem, 2021), drones are used by settlers in service of expanding the domination and dispossession of Palestinians.

Subjectivities related to different technologies are obviously not universally applicable, and during my research, I also came across examples in which drones were ignored, accepted, or even welcomed. On 11 October 2021, the sky above Tel Aviv, and other urban areas in central Israel, hummed with the sound of drones delivering sushi, beer, and ice cream to curious beachgoers and other interested passers-by. These drone flights were part of demonstration flights run by the Israel National Drone Initiative (INDI) as part of a two-year pilot programme intended to develop "agile regulation and [the] supporting ecosystem to enable drones and UAM [unmanned air mobility] operations in Israel" (Israel Innovation Authority, n.d.). During an online workshop that followed this ice-cream-sushi spectacle, one of the experts on the INDI project explained how:

> People aren't excited by drones. It's a part of life. Nobody notices drones in a city. You don't see or hear them because of the other noise. And anyway, the drones fly above 50 metres. We own the sky, but we tell people anyway … On the radio and so on. There was only one complaint, and nobody even came up to take a look when we were doing the flights. It was a very nice surprise for us.[6]

Drones might be "a part of life", as the speaker suggested, but their roles in people's lives vary considerably, as these examples illustrate. It is perhaps unsurprising that when drones are used to deliver ice cream, the public finds this new technology unremarkable. It follows that when similar technology is used in occupied territory for surveillance, policing, and crowd control, the response might be decidedly different and the urgency of the concern around its use more pronounced. This urgency is magnified further still when unmanned aerial vehicles are larger, fitted with weapons, and connected to AI systems capable of producing hundreds of targets for aerial bombing. The possibility and scale of the response that publics are able to mobilise depend on many factors, including the specifics of the technology being used and who is operating it. For example, the tactics and access necessary to destroy face recognition cameras are different from those that would facilitate similar responses to AI programs used in military operations. Still, this part of the chapter considers some Palestinian responses I encountered during my research and asks what they can tell us about new digital technologies.

Smoke and mirrors

To begin with, I want to return to the Great March of Return I referred to above when describing the inspiration behind the development of the *Skylord* drone. During these protests, which were held regularly by Gazans between March 2018 and December 2019, tens of thousands of Palestinians demonstrated near the fence that surrounds Gaza. The demonstrations sought to centre and protest against a number of specific grievances as well as the Israeli occupation as a whole. The specific issues were the Israeli siege of Gaza, the American recognition of Jerusalem as the capital of Israel, and a demand for Palestinian refugees' *right of return*. I watched these protests from the Israeli-side of the fence. As a British-Israeli dual national, I am not able to enter Gaza. From a distance of about a kilometre and a half, I saw Gazan protestors use the smoke of huge fires, as well as lasers and mirrors, to shield themselves from Israeli soldiers and snipers. The lasers and mirrors were used to dazzle and confuse the Israeli snipers positioned along the fence. The smoke was intended to obscure the soldiers' vision and protect the protestors. I observed similar "confusion" tactics in Beita, a Palestinian town in the northern part of the occupied West Bank where protests were held regularly from May 2021 to oppose a new Israeli outpost settlement established earlier that month on land belonging to the town's residents, in contravention of Israeli and international law.[7] Both in Gaza and in Beita the literal smoke and mirrors did not obscure the Palestinians well enough to prevent them from being maimed and killed by Israeli forces. During the Great March of Return, despite the protestors' efforts, Israeli soldiers shot and killed some 223 Palestinians and injured over 13,000 more (Puar, 2017).[8] In Beita, in the five months between May and September 2021, the Israeli army killed seven demonstrators (Levy and Levac, 2021)

Tactics designed to hamper visibility can be traced from Gaza and Beita into online spaces. Social media plays a central role in the amplification of Palestinian defiance (Aouragh, 2016; Kuntsman and Stein, 2015; Tawil-Souri and Aouragh, 2014) and during the escape of Palestinian prisoners from a high-security prison in September 2021, as well as during a siege on the Shuafat refugee camp, a little over a year later, in October 2022, Palestinians used the names of those wanted by Israeli forces on social media and in their private communications with the intention of confusing the surveillance tools assumed to be programmed to identify particular words and phrases. These tools are the subject of fear, rumours, and jokes, after their increasingly public use since 2015, when a wave of what was described as "lone-wolf" attacks on Israelis was blamed on social media activity (Nashif, 2017). The theory that the attacks were related to social media use justified the arrest of hundreds of Palestinians for their social media activity, including in the well-known case of the detention of Palestinian poet, Dareen Tatour, who was charged with inciting violence for a series of Facebook posts, including a video of her poem, *Resist my people, resist them*. These arrests cemented a prevalent, collective assumption that spyware is in constant use. Stevens *et al.* (2023: 12) have discussed how the effects of surveillance extend far beyond individual harms and "impact wider society and the functioning of democratic processes". With this in mind, it is interesting to note that in the context of the Shuafat refugee camp in East Jerusalem in October 2022, an awareness of the prevalence of surveillance technology was capitalised on by its residents.

The refugee camp, which comprises some 140,000 individuals, was placed under siege while Israeli law enforcement forces searched for Udai Tamimi, a 22-year-old from the camp with a shaved head, responsible for the fatal shooting of an Israeli soldier at a checkpoint at the entrance to the camp. After the details of the suspect were released, viral videos began to appear on social media of Palestinians from the camp shaving their heads in order to "confuse" biometric recognition technology. This physical impersonation was in addition to the more common practice of using specific names and phrases in messages and voice notes. (For example, in one viral video a woman from the camp can be heard asking her partner if he changed Udai's diaper). An article in a local newspaper published at the time suggested that this was "an attempt to distort algorithms in the area that could potentially be used to track and locate" (Fayyad, 2022). These tactics and videos are a genuine attempt to mislead and confuse the tools used by Israeli law enforcement, *and* they operate as jokes that make light of the carceral nature of the Palestinian experience under Israeli rule. This ambiguity about how "real" the effects of different confusion tactics are on Israeli technology is important because in both cases it builds the collective awareness of Israeli surveillance practices and positions them as illegitimate, invasive, unjust, and demanding collective and individual forms of resistance. The sense of collective punishment described by residents of Shuafat during the siege and under the constant hum of Israeli surveillance drones seemed to strengthen opposition to Israeli governance and cause fear and unease among the residents.

Similarly, during the events of May 2021 the centrality of social media was particularly pronounced, Palestinians and their allies adopted various techniques for masking pro-Palestinian content online in order to evade the automatic censorship of social media platforms. Words like "Palestine" were purposely misspelled or omitted, and pictures of pets and selfies were interspersed with more "political" content to try and dilute the success of automatic censorship. A report by a Palestinian digital rights NGO also describes this ongoing phenomenon of attempts at the evasion of online censorship and arrest (Goodfriend, 2021). Literature addresses how social media users navigate automatic content moderation in relation to other "charged" topics given that social media platforms have become increasingly important sites of public discourse (Gillespie, 2018, 2020; Myers West, 2018; Heldt, 2019; Morrow *et al.*, 2022).

These tactics – such as the modification of language and appearance – carried out by Palestinians either online or offline are significant responses to expanding surveillance practices and the kinds of chilling effect described by Stevens *et al.* (2023). They differ significantly from individualistic responses to surveillance like the widgets designed to cover the camera on computers or phones, or counter-surveillance fashion or make-up projects that periodically emerge with the aim of camouflaging individuals from surveillance technologies (Monahan, 2015). By contrast, the tactics used by Palestinians are collective behaviours designed to shield individuals from surveillance. They represent more symbolic opposition to surveillance. The attempts described in this chapter (as in the case of the impersonation of Udai Tamimi through head shaving) act to literally "duplicate" a targeted individual in the hope that the multiplication of the aesthetic of the fugitive might make it marginally harder to identify him. There is a more collective approach toIsraeli surveillance. The sense of shared responsibility and mobilisation contributes to a more widespread rejection of the legitimacy of Israeli surveillance tools and practices and the kind of legibility they afford Israeli security forces, even among those who may not be actively involved in confusion, impersonation, or amplification. In interviews it emerged that Israeli surveillance is not conceived of as an individual problem, but as a common threat that should be opposed collectively through Palestinian solidarity (and humour). Rather than a concern with their own privacy, my interlocutors saw this technology as part of Israeli oppression. Even those who do not shave their heads to confuse face recognition technologies or produce "original" social media content that can withstand content moderation are often involved in sharing and amplifying a shared position about the legitimacy of the surveillance taking place and thus contribute to the mobilisation of a collective rejection of intensifying Israeli surveillance.

Surveillance as a mobilising force

My research cements that new surveillance technologies mean that clear-cut distinctions between online and offline spaces are no longer relevant – if they ever were – especially when the goal is the domination and elimination of particular political movements seen as threatening by states. Crosby and Monaghan, (2016) discuss the extensive surveillance of Idle No More, a movement which the authors describe as powerfully challenging Canadian settler colonialism. They depict how this indigenous movement was policed with increasingly more powerful tools precisely because it was seen to threaten the foundation of the Canadian state. In Palestine, this is also the case. In the aftermath of protests against an afforestation project in the southern Naqab region of what is today Israel, described as an "extrajudicial land grab" (Kremer and Thomas, 2022: 6), scores of Palestinian Bedouin youngsters were arrested for posts they made about the protest on social media (specifically Instagram and TikTok). The protest itself took place on 10 January 2022, near the Palestinian Bedouin village of Sa'wa, and was violently repressed by the Israeli police, who deployed tear gas drones, horses, stun grenades, and rubber bullets against the protestors. This led to a number of protestors being seriously injured.

One of the protestors' lawyers clarified that many of those who were arrested in relation to the protest had not joined the protest in person but merely expressed sympathy with it online, which points to this blurring of the distinction between online and offline surveillance and repression. The lawyer explained that the arrests were part of "an ongoing wave [of arrests]. It's not a wave that stopped around January. It's ongoing". He traced this wave back to the period of *Habat al Karama* in May 2021 and stated that in less than two years, more than 450 individuals from the region had been arrested, and "we haven't seen a wave of arrests like this in the Naqab for years".

The policing of this protest with the increasingly invasive use of surveillance, tracking, and policing tools adds a technological layer to the repression already felt by the Palestinian Bedouin in southern Israel and across the areas under intensifying Israeli control. One political organiser explained to me how this repression further fuels people's frustration and mobilises resistance. He laid out how as a political organiser he no longer has to convince people of their oppression. The arrest of their friends, siblings, or neighbours for as little as a post on social media is proof enough of their oppression. Resistance to land expropriation and home demolitions in the Naqab had once necessitated a more organised approach to activism but as the activist described that had now changed:

> what we see today is that there's no need for activists in the first place because the youngsters are fully frustrated, and they see what's happening everywhere to their people and what's happening in the Naqab – from demolitions and taking over the land – and people go to the streets to protest anyway. And, that's their right in a real democratic country, but what's happening here has no relationship with democracy.

Describing having been targeted by Israeli security forces for his political organising, he clarified how misguided he thought the repression and surveillance of particular individuals can be in the wider context of occupation and injustice:

> They would take us [arrest them] because we are activists, because they think we are dominant, because they think we are moving stuff, but the frustration of people and the punishment of people does not need anyone to move things. People are just moving because they are occupied and because they are assaulted in the streets, and because they [Israeli

> forces] are demolishing villages and because they see what is happening to their people everywhere.

New surveillance technologies are often portrayed in showrooms as frictionless, but their impact is felt in the lives of those who are their everyday targets, like the protestors in the Naqab, and this has serious consequences for social order. Rather than strengthening Israel's security, the use of these powerful online surveillance tools and the repression of protest mobilise more opposition to Israeli control. Moreover, as the activist made clear, attempts to single out "troublemakers" through advanced surveillance technologies are useless because the problem of "unrest" in Palestine, as elsewhere, is deeper and more systematic than a few "bad apples" *moving stuff* and causing trouble.

In a passage that echoes what the activist articulated empirically, Elia Zureik optimistically proposes that "as surveillance spreads from the colony to the metropole, and from the colonized population to the general population, resistance is gaining ground" (Zureik, 2016b: 28). This certainly holds true in the case of NSO's Pegasus spyware. As the use of Israeli spyware spread from Palestinians to Israelis and then on to "the general population" in much of the world, its legitimacy came to be called into question. Immediately after the Pegasus Project revelation in July 2021, a group of approximately 20 activists stood outside the Israeli company's headquarters in the city of Herzliya, 20 kilometres north of Tel Aviv, and chanted slogans against the company and surveillance practices more generally:

> *"One, two, three, four: we don't want your cyber war*
> *Five, six, seven, eight: abolish the surveillance state".*

Several months after this small protest in Herzliya, the United States placed NSO on the trade restriction "Entity List". Of course, there is no direct link between this small protest and the decisions of the US government, but the question about the future direction of new surveillance technologies *is* affected by how these technologies are used, navigated, and responded to by populations increasingly governed by similar technologies. The Pegasus Project revelation triggered global public outrage and gave urgency to the conversation around the lack of regulation of spyware technology and the difficulties in transparency around its use and sale because of its immateriality. Calls for a moratorium on the use and sale of spyware became commonplace, as the scope and impact of the use of this technology became increasingly obvious. Heads of state, journalists, and activists had been targeted. As Zureik makes apparent, it is not the use of surveillance on particular populations, or as in this case, the outcry of 20 individuals that will change things, but the expansion of these logics and practices to the general population which *can* mobilise more profound and effective resistance. As more of the world becomes implicated in these apparently inevitable systems of surveillance, it seems likely that more transparency and restraint around their use will be demanded.

Destroying objects as if they were systems of surveillance

The (often humorous) hampering of surveillant visibility is supplemented by the literal destruction of parts of the surveillance apparatus. One interviewee recounted how:

> A group of young men were throwing stones at the surveillance camera. One, two, three. Stones continued to be thrown at the camera, some hit it, others missed, until eventually it came down and everybody there was cheering and ran away before the army arrived.

The interviewee's account depicts the destruction of a camera and portrays the symbolic nature of this act. It is a gesture of opposition to the broader system of surveillance and repression that I saw echoed across Palestine, including in Beita, where protestors brought down one of the army's drones by throwing stones at it until it finally fell from the sky. The drone had been circling above the protest, dropping tear gas on the assembled protestors, and released the remaining canisters it was carrying when it hit the ground.

In a video widely shared online following an Israeli raid on the West Bank city of Jenin in March 2023, I saw this scenario of destruction and elation depicted with even more clarity. The video shows an Israeli drone hovering above the city until it is shot down by armed resistance fighters and comes tumbling out of the sky into the streets. The drone is carried through a jubilant crowd, held up high like a carcass in a funeral procession.

In both the vignettes above, the destruction of surveillance tools is celebrated. These are not isolated incidents, and the procession by which the drone is carried through the crowd in the video speaks to the significance of the destruction of this object. Both the camera and the drone represent the oppression and harm of Israeli surveillance on Palestinians' everyday lives. The individual objects – the camera and the drone – are symbols of Israeli aggression. As with the head-shaving videos and use (and omission) of specific words designed to "confuse" surveillance tools and automated content moderation, the social significance of such acts is more important than the practical effect of destroying a single drone or camera. However small and fleeting these moments of destruction and response may seem, they are also constitutive of collective rebellion. An activist I interviewed about the successful downing of the tear gas drone during the protest in Beita noted how the crowd was wild with excitement after the drone was brought down. These acts uplift and rally people. They make pushback and outright rejection of surveillance and oppression real possibilities. Drones and cameras are the protruding edges of what Elia Zureik has referred to as the surveillant assemblage of settler colonialism (Zureik, 2016a). They are the vulnerable "eyes" through which the surveillant assemblage sees.[9]

Conclusion

Theoretically, the chapter foregrounds the importance of considering the responses of "data subjects" to the experience of surveillance. By looking at the protest, pushback, and even destruction of surveillance technologies and simple (as in not high-tech) forms of evasion, we get a clearer picture of possible empirical and theoretical responses to these technologies and an understanding of the way in which global surveillance futures are not only shaped in the sterility of the spaces where new technologies and particular paradigms of security are developed, sold, and justified. Ethnographic commitment to those who experience and navigate the effects of these technologies shows critical scholars not only the fear and distress they generate but also other possible responses to new surveillance technology such as its outright rejection. The responses I encountered throughout my research show the incongruity and even perhaps the futility of the logic of *security as technological domination*. While this logic proposes the complete domination of populations as a security solution, the chapter shows how the unchallenged expansion of surveillance technologies into new settings and fields of life isn't one-sided. Populations can and do respond to and resist their domination.

These conclusions are drawn against the backdrop of a detailed description of the way in which new technologies in Palestine/Israel function both as a means to exert dominance over Palestinians and as important products in a marketing strategy designed to position Israeli security as a leading brand in global technology markets. Their role in Israel's diplomacy and self-perception is discussed in the first half of the chapter, which traces how the development, use, and global circulation of these technologies are grounded in a paradigm that centres on the objectivity, effectiveness, and inevitability of the expansion of new surveillance technologies. The stark contradiction of such narratives to Palestinian rejection of these technologies through sabotage, evasion, or destruction is apparent in the second part of the chapter.

Notes

1 This chapter was written before 7 October 2023 when Hamas fighters stormed through the multi-million dollar 'smart fence' between Israel and Gaza. The events of that day and those in Gaza in its aftermath would surely impact the findings of this chapter. Investigations into the Israeli military's use of technology in Gaza would also no doubt reshape some of the arguments made here - (see, for example, Abraham, 2023). Both technology and reality are changing rapidly in this and other contexts and this chapter should be read with this in mind. It captures a moment which will already have passed by the time these words reach the reader.

2 Sent on 16 May 2021 – video and messages on file with the author.

[3] These arrests almost exclusively targeted Palestinians living inside Israel. According to the Israeli Police there were 2,142 arrests nationwide, with 184 indictments filed during the operation, which officially lasted until 3 June 2021 (Israel Police, 2021). In practice the increase in arrests continued after this date with many Palestinians arrested after the uprising subsided. The police activities were presented as necessary to restore order after the “disturbances” that had taken place.

[4] During the Oslo Accords the West Bank was temporarily divided into three parts with different levels of Palestinian and Israeli control. Area C comprises Israeli military and civil control and has remained so despite the fact that the initial division was supposed to only have been temporary.

[5] A dunam is an Ottoman term still used to measure land in Palestine/Israel. It is equal to about 900 square metres.

[6] The quotes are reconstructed from notes taken during the workshop and not verbatim transcriptions.

[7] I had joined a number of Jewish–Israeli activists who regularly attended these Palestinian-led protests. As a British–Israeli dual national who has spent a lot of her life living outside the region, I am indebted to pre-existing networks of solidarity between Jewish–Israelis and Palestinians, built over many years through practices of joint struggle against the Israeli occupation. These networks facilitated my access and research and shaped my understanding of the systems of control, surveillance, and segregation.

[8] Puar (2017) has described how injury and disability are used by the liberal state in *The Right to Maim* which captures some of the horror of this particular moment of Palestinian resistance and annihilation.

[9] Thanks to Nataliya Tchermalykh for this formulation and other help with this chapter.

References

Abraham, Y. (2023) ‘“A Mass Assassination Factory”: Inside Israel’s Calculated Bombing of Gaza, +972 Magazine’. Available at: https://www.972mag.com/mass-assassination-factory-israel-calculated-bombing-gaza/ (Accessed: 25 January 2024).

Adams, R. (2021) ‘Can Artificial Intelligence Be Decolonized?’, *Interdisciplinary Science Reviews*, 46(1–2), 176–197.

Ahronheim, A. (2021) ‘Israel’s Operation against Hamas Was the World’s First AI War’, *The Jerusalem Post | JPost.com*, 27 May. Available at: https://www.jpost.com/arab-israeli-conflict/gaza-news/guardian-of-the-walls-the-first-ai-war-669371 (Accessed: 7 June 2023).

Amnesty International (2023) ‘Automated Apartheid: How Facial Recognition Fragments, Segregates and Controls Palestinians in the OPT’. Available at: https://www.amnesty.org/en/documents/mde15/6701/2023/en/.

Aouragh, M. (2016) ‘Hasbara 2.0: Israel’s Public Diplomacy in the Digital Age’, *Middle East Critique*, 25(3), 271–297.

Benjamin, R. (2019a) *Captivating Technology: Race, Carceral Technoscience, and Liberatory Imagination in Everyday Life*. Durham, NC: Duke University Press.

Benjamin, R. (2019b) *Race After Technology: Abolitionist Tools for the New Jim Code*. Medford, MA; Polity Press.

Brayne, S. (2020) *Predict and Surveil: Data, Discretion, and the Future of Policing*. Oxford: Oxford University Press.

Browne, S. (2015) *Dark Matters: On the Surveillance of Blackness*. Durham, NC: Duke University Press.

B'Tselem (2021) 'Settler Violence = State Violence, B'Tselem'. Available at: https://www.btselem.org/settler_violence (Accessed: 23 June 2023).

Crosby, A. and Monaghan, J. (2016) 'Settler Colonialism and the Policing of Idle No More', *Social Justice*, 43(2 (144)), 37–57.

Fayyad, H. (2022) 'Head-shaving, Humour and Hoax Calls: How Palestinians Are Rallying around Jerusalem's Shuafat', *Middle East Eye*, 18 October. Available at: http://www.middleeasteye.net/news/palestine-israel-rallying-jerusalem-shuafat-haircuts-voice-notes-humour (Accessed: 1 May 2023).

Gillespie, T. (2018) *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media*. New Haven, Connecticut: Yale University Press.

Gillespie, T. (2020) 'Content Moderation, AI, and the Question of Scale', *Big Data & Society*, 7(2), 2053951720943234.

Gilliom, J. and Monahan, T. (2012) 'Everyday Resistance', in Ball, K., Haggerty, K. and Lyon, D., *Routledge Handbook of Surveillance Studies*. Routledge, 405–411.

Goodfriend, S. (2021) 'Intensification of Surveillance in East Jerusalem and Impact on Palestinian Residents' Rights: Summer and Fall 2021', *7amleh*. Available at: https://7amleh.org/2021/11/08/intensification-of-surveillance-in-east-jerusalem-and-impact-on-palestinian-residents-rights-summer-and-fall-2021 (Accessed: 16 April 2023).

Grassiani, E. (2017) 'Commercialised Occupation Skills: Israeli Security Experience as an International Brand', in Leese, M., and Wittendorp, S., *Security/Mobility*. Manchester: Manchester University Press, 57–73.

Grassiani, E. (2018) 'Between Security and Military Identities: The Case of Israeli Security Experts', *Security Dialogue*, 49(1–2), 83–95.

Grassiani, E. (2022) 'Performing Politics at the Israeli Security Fair', *Policing and Society*, *34*(1-2), 10-26.

Gross, J.A. (2021) 'In Apparent World First, IDF Deployed Drone Swarms in Gaza Fighting', 10 July. Available at: https://www.timesofisrael.com/in-apparent-world-first-idf-deployed-drone-swarms-in-gaza-fighting/ (Accessed: 7 June 2023).

Hambling, D. (2021) 'Israel Used World's First AI-guided Combat Drone Swarm in Gaza Attacks', *New Scientist*, 30 June. Available at: https://www.newscientist.com/article/2282656-israel-used-worlds-first-ai-guided-combat-drone-swarm-in-gaza-attacks/ (Accessed: 7 June 2023).

Heldt, A.P. (2019) 'Upload-Filers: Bypassing Classical Concepts of Censorship', *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 10, 56.

Huang, J. and Tsai, K.S. (2022) 'Securing Authoritarian Capitalism in the Digital Age: The Political Economy of Surveillance in China', *The China Journal*, 88, 2–28. https://doi.org/10.1086/720144.

Israel Innovation Authority (n.d.) 'National Drone Delivery Network Program, English Innovation Site'. Available at: https://innovationisrael.org.il/en/programs/national-drone-delivery-network-program/ (Accessed: 31 January 2024).

Israel Police (2021) 'Summary of "Operation Law and Order" of the Israel Police', *Ministry of National Security*, 3 June. Available at: https://www.gov.il/en/departments/news/police-restoring-order-030621 (Accessed: 7 June 2023).

Kaplan, C. and Miller, A. (2019) 'Drones as "Atmospheric Policing" from US Border Enforcement to the LAPD', *Public Culture*, 31(3), 419–445.

Khalili, L. (2010) 'The Location of Palestine in Global Counterinsurgencies', *International Journal of Middle East Studies*, 42(3), 413–433. https://doi.org/10.1017/S0020743810000425.

Klauser, F. (2022) 'Policing with the Drone: Towards an Aerial Geopolitics of Security', *Security Dialogue*, 53(2), 148–163. https://doi.org/10.1177/0967010621992661.

Kremer, E. and Thomas, C. (2022) *Enforcing the Invisible Barrier: Police Violence during January 2022 Protests of KKL-JNF Afforestation Projects*. Negev Coexistence Forum. Available at: https://www.dukium.org/102283/ (Accessed: 16 April 2023).

Kuntsman, A. and Stein, R.L. (2015) *Digital Militarism: Israel's Occupation in the Social Media Age*. Stanford: Stanford University Press.

Lavallée, G. (2019) 'Flying High: Military Prowess Helps Israel Become Global Force in Drone Industry'. Available at: https://www.timesofisrael.com/flying-high-military-prowess-helps-israel-become-global-force-in-drone-industry/ (Accessed: 7 June 2023).

Levy, G. and Levac, A. (2021) 'If the Israeli Sniper Could See the Devastation He Caused, He Wouldn't Shoot Again', *Haaretz*, 1 October. Available at: https://www.haaretz.com/israel-news/twilight-zone/2021-10-01/ty-article-magazine/.premium/if-the-idf-sniper-could-see-the-devastation-he-caused-he-wouldnt-shoot-again/0000017f-e1be-d804-ad7f-f1fe77110000 (Accessed: 21 January 2024).

Loewenstein, A. (2023) *The Palestine Laboratory: How Israel Exports the Technology of Occupation Around the World*. Brooklyn, New York: Verso Books.

Lyon, D. (2022) *Beyond Big Data Surveillance: Freedom & Fairness*. Surveillance Studies Center. Available at: https://www.surveillance-studies.ca/beyond (Accessed: 27 April 2023).

Machold, R. (2018) 'Reconsidering the Laboratory Thesis: Palestine/Israel and the Geopolitics of Representation', *Political Geography*, 65, 88–97. Available at: https://doi.org/10.1016/j.polgeo.2018.04.002.

Maoz, E. (2020) '"Welcome to Capital's Utopia: Israel, The United Arab Emirates, and Racial Catastrophe Capitalism, מיכורב מיאבה היפוטואל לש ןוהה: לארשי, דוחיא
ןוסאה לש מזילטיפקהו תויורימאה', *Theory and Criticism*, 53, 181–195.

Marx, G.T. (2015) 'Surveillance Studies', *International Encyclopedia of the Social & Behavioral Sciences*, 23(2), 733–741.

McCahill, M. (2021) 'Theorizing Surveillance in the Pre-Crime Society', in B. Arrigo and B. Sellers (eds.) *The Pre-Crime Society Crime, Culture and Control in the Ultramodern Age*. Bristol: Bristol University Press, 227–248.

Miller, A. (2019) 'Shadows of War, Traces of Policing', in Benjamin, R. (2019) *Captivating help_outlineTechnology: Race, Carceral Technoscience, and Liberatory Imagination in Everyday Life*. Durham, NC: Duke University Press,85–106.

Monahan, T. (2015) 'The Right to Hide? Anti-surveillance Camouflage and the Aestheticization of Resistance', *Communication and Critical/Cultural Studies*, 12(2), 159–178.

Monahan, T. and Wood, D.M. (2018) *Surveillance Studies: A Reader*. Oxford: Oxford University Press.

Morrow, G. *et al.* (2022) 'The Emerging Science of Content Labeling: Contextualizing Social Media Content Moderation', *Journal of the Association for Information Science and Technology*, 73(10), 1365–1386. https://doi.org/10.1002/asi.24637.

Myers West, S. (2018) 'Censored, Suspended, Shadowbanned: User Interpretations of Content Moderation on Social Media Platforms', *New Media & Society*, 20(11), 4366–4383. https://doi.org/10.1177/1461444818773059.

Nasasra, M. (2022) 'From Damascus Gate to Shaikh Jarrah: The Palestinian Sovereignty Protests in East Jerusalem', *Protest*, 1(2), 329–345. https://doi.org/10.1163/2667372X-01020006.

Nashif, N. (2017) 'Surveillance of Palestinians and the Fight for Digital Rights', *Policy Brief, Al Shabaka*, 23, 1-10.

Neocleous, M. (2013) 'Air Power as Police Power', *Environment and Planning D: Society and Space*, 31(4), 578–593. https://doi.org/10.1068/d19212.

Noble, S.U. (2018) *Algorithms of Oppression: How Search Engines Reinforce Racism*. New York City: New York University Press.

O'neil, C. (2017) *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. New York City: Crown.

Parks, L. and Kaplan, C. (eds.) (2017) *Life in the Age of Drone Warfare*. Durham, NC: Duke University Press.

Puar, J.K. (2017) *The Right to Maim: Debility, Capacity, Disability*. Durham, NC: Duke University Press.

Sa'di, A.H. (2021) 'Israel's Settler-colonialism as a Global Security Paradigm', *Race & Class*, 63(2), 21–37.

Senior, E. and Morag, G. (2021) '"Law and Order": The Police Will Launch an Arrest Operation Across the Country Today', *Ynet*, 23 May. Available at: https://www.ynet.co.il/news/article/SyMVBVOKO (Accessed: 7 June 2023).

Stevens, A. *et al.* (2023) '"I Started Seeing Shadows Everywhere": The Diverse Chilling Effects of Surveillance in Zimbabwe', *Big Data & Society*, 10(1), 20539517231158631. https://doi.org/10.1177/20539517231158631.

Talbot, R. (2020) 'Automating Occupation: International Humanitarian and Human Rights Law Implications of the Deployment of Facial Recognition Technologies in the Occupied Palestinian Territory', *International Review of the Red Cross*, 102(914), 823–849.

Tawil-Souri, H. and Aouragh, M. (2014) 'Intifada 3.0? Cyber Colonialism and Palestinian Resistance', *Arab Studies Journal*, XXII(1), 102–133.

Weizman, E. (2012) *Hollow Land: Israel's Architecture of Occupation*. Brooklyn, New York: Verso Books.

Who Profits (2021) *Repression Diplomacy: The Israeli Cyber Industry*. Flash report. Who Profits. Available at: https://whoprofits.org/flash-report/repression-diplomacy (Accessed: 13 June 2023).

Who Profits (n.d.) 'Elbit Systems', in *Company Profiles*. Available at: https://whoprofits.org/company/elbit-systems (Accessed: 13 June 2023).

Williams, A.J. (2011) 'Enabling Persistent Presence? Performing the Embodied Geopolitics of the Unmanned Aerial Vehicle Assemblage', *Political Geography*, 30(7), 381–390. https://doi.org/10.1016/j.polgeo.2011.08.002.

Xtend (no date) 'About, XTEND'. Available at: https://defense.xtend.me/about/ (Accessed: 7 June 2023).

Zaken, D. (2021) 'Elbit Systems Establishes UAE Unit', *Globes*, 14 November. Available at: https://en.globes.co.il/en/article-elbit-systems-establishes-emirates-unit-1001390875 (Accessed: 13 June 2023).

Ziv, O. (2022) 'תימוקמ החיש ,םילחנתמ לש םירייס תוקלחמ הנידמה תנממ דכ :םיפשחנ םינותנה'. Available at: https://www.mekomit.co.il/תוקלחמ-הנידמה-תנממ-דכ-םיפשחנ-םינותנה/ (Accessed: 8 May 2023).

Ziv, O. (2023) '"It's Like 1948": Israel Cleanses Vast West Bank Region of Nearly all Palestinians, +972 Magazine'. Available at: https://www.972mag.com/area-c-ethnic-cleansing-settler-violence/ (Accessed: 28 January 2024).

Zureik, E. (2016a) *Israel's Colonial Project in Palestine: Brutal Pursuit*. Milton Park, Oxfordshire: Routledge.

Zureik, E. (2016b) 'Strategies of Surveillance: The Israeli Gaze', *Jerusalem Quarterly*, 66, 12.

Zureik, E., Lyon, D. and Abu-Laban, Y. (2010), 'Surveillance and Control in Israel/Palestine: Population Territory and Power',*London: Routledge*.

2 Encountering ethnographic gestures

Reflections on the banality of cybersecurity and STS ecologies of practice

Andrea Miller

Introduction

On a blustery day in January 2018, I took a walk down Augusta, Georgia's mostly boarded-up and vacant main thoroughfare, Broad Street. I had just concluded a meeting with an official from the $100 million Georgia Cyber Center in downtown Augusta, the centrepiece of a regional redevelopment project premised on cybersecurity. Capitalising on the recent relocation of US Army Cyber Command to nearby Fort Gordon, the development of the Georgia Cyber Center's campus brought together Augusta University with the Georgia Technology Authority, the US Army, the National Security Agency, the Georgia National Guard, the Georgia Bureau of Investigation, and private tech companies and contractors. For the Cyber Center official with whom I had just met, cybersecurity could be the key to subverting decades of failed urban redevelopment projects in Augusta – its goal, to "create an ecosystem that is self-sustaining".[1]

While my interlocutor brimmed with optimism about what the influx of cybersecurity capital and professionals would do for the city's historically Black downtown and toward his aim to create a self-sustaining cyber ecosystem, early evidence to support that optimism was not readily apparent. Walking along Broad Street on that January day, I passed a countless number of #StartUpLife flyers taped to the windows of occupied and unoccupied buildings alike, torn from end to end, loose paper fluttering and snapping against the glass in the brisk winter wind (see Figure 1). A programme run by theClubhou.se, a makerspace turned occupant of the Georgia Cyber Center, Startup Life is an incubator programme in which "participants learn about customers, finance, management, and marketing as well as automation tools".[2] Noticing that other flyers of various types were spared while no #StartUpLife flyers were left unscathed, I asked a few shopkeepers and a barista if they knew about the flyers or any organised resistance to the programme, theClubhou.se, or the Georgia Cyber Center and the kinds of redevelopment cybersecurity might portend for the downtown. All shrugged. I asked the same question of a journalist I met for coffee the next morning. He shrugged. I later asked a local activist I befriended. While he was concerned about accelerating and predatory redevelopment in the

DOI: 10.4324/9781003412908-4

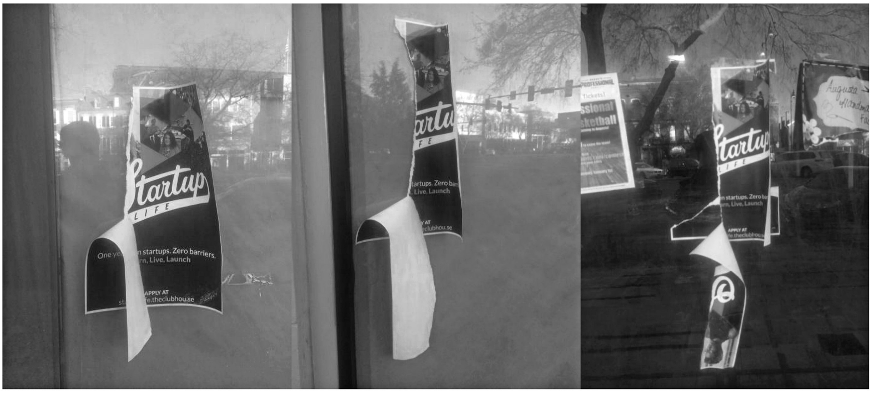


Figure 2.1 #StartUpLife flyers on vacant Broad Street storefronts in Augusta, GA, USA. 20 January 2018. Photographs taken by the author.

city, he likewise shrugged. Everyone I asked seemed only to shrug, sometimes offering accompanying anecdotes about Augusta's general capacity to rather obstinately withstand attempts to redevelop its downtown.

In this chapter, drawing from this ethnographic encounter, I turn my attention from interlocutors' narratives to the gestures of *the tear* and *the shrug* as themselves sites for ethnographic inquiry. Specifically, I argue that these ethnographic political gestures surrounding cybersecurity's relationship to the city of Augusta point toward and call into question cybersecurity's orderly and banal premises, which increasingly signal the operations of police power across all manner of digital platforms, media, and infrastructure for the US security state. Rather than discard these early ethnographic encounters as the absence of leads to pursue, I adopt a methodological approach that feminist science and technology studies scholar Isabelle Stengers calls "thinking in the minor key" to linger on the tear and the shrug as political gestures that draw my attention toward and respond, even if not in immediately recognisable ways, to what I will argue is the banality of police power in cybersecurity (Stengers, 2005). Here, the tear of the poster and the shrugs of my interlocutors function as examples of what Kemi Adeyemi has termed "microgestures of dissent and reformation that communities of colour, and black communities in particular have long practised" (Adeyemi, 2019a: 548).[3] As I will argue, these embodied and emplaced gestures signify not only insurgent political practices of critique via disinterest in the banality of cybersecurity-driven redevelopment and policing in Augusta but also methodological provocations for ethnographic engagements with technological objects and concepts that enact and facilitate state violence.

Prompted by the banality of the tear and the shrug as political gestures, I begin by charting how police power operates through banality within cybersecurity and – historically and more broadly – the data- and digitally driven warfare of the US war on terror. I refer to police power here, in keeping with scholars such as Mark Neocleous, Micol Seigel, and Tyler Wall, as the proliferating security practices of the state that produce and maintain the perceptual and material boundaries between police and war, civilisation and disorder, and the nation and its others (Neocleous, 2014; Wall, 2019; Wall, 2016; Seigel, 2018; Miller, 2019; Kaplan and Miller, 2019). Situated thusly, cybersecurity comes to enshrine an increasingly expansive and not altogether immediately legible modality of governance for the US security state. Emergent forms of cybersecurity-driven police practices correspond to changes in cybersecurity policy currently unfolding across the US security state, wherein cybersecurity provides the logic and charge to a shift from securing objects and assets, to one of securing state and industry *practices* through the nascent category of National Critical Functions (NCFs). After charting the conceptual development of NCFs via cybersecurity in US policy and practice, I return to the ethnographic gestures of the tear and the shrug to ask how an STS *ecologies of practice* invites a politically and ethically attuned engagement with the politics and policing that surround cybersecurity and its expansive manifestations. Here, the tear and the shrug function as indices of an insurgent and illegible archive of place-making, critique, and methodological incitement, inviting an ethnographic encounter with the murmurs, flutters, and silences of a disavowing politics.

The banal police power of cybersecurity

Indeed, cybersecurity has manifested as one of the most banal of US security practices, though no less insidious. As Louise Amoore and Marieke de Goede articulated in 2008, the dangers of "the banal face" of a doctrine of preemption central to the US war on terror form the basis for contemporary practices and conceptions of cybersecurity. Through preemption, cybersecurity enjoins the everyday, transactional, and purportedly objective data-driven infrastructures that make possible ostensibly more spectacular practices of war-making such as torture, the use of drones, facial recognition software, and other yet-to-be-implemented technologies of future war (Amoore and de Goede, 2008). As Amoore and de Goede warned, these "relatively unacknowledged" forms of violence in the war on terror are especially pernicious precisely because they are imagined to be so utterly quotidian, thus "in danger of being accepted as ubiquitous features of contemporary life" (Amoore and de Goede, 2008: 174). Through the power attributed to transactional and associational data, the security state asserts its preemptive capacity to identify and thwart future terrorist threats that have yet to cohere in an uncertain present. This doctrine of preemption that has underwritten US war-making and policing following 11 September 2001 proclaims that the perceived threat of future terror is so grave that it requires preventive action in the present, a racialised ontology that I have argued identifies terrorist threat as "immanent and imminent" to Muslims and other mostly Black and Brown persons ensnared in US counterterrorism (Miller, 2017b: 115). Following Amoore and de Goede, I likewise assert that while preemption may take the form of drone warfare and other data-driven and hypervisible state practices, it just as readily manifests in mundane and surreptitious forms of data collection and policing – such as cybersecurity – which may, *or may not*, result in direct encounters with the security state (Miller 2017b; Amoore and de Goede, 2008; Wall, 2016).[4] And in each case, these banal modes of preemptive practice and temporalities emerge in no small part through the sanitising force of objectivity and supposed fairness attributed to data-driven processes and technologies, as feminist scholars such as Caren Kaplan, Lucy Suchman, and Ruha Benjamin have pointed out (Kaplan, 2006; Benjamin, 2019; Chandler, 2020).

It is within this context that cybersecurity emerges as an intensifying preoccupation by and for the United States, notably in a moment marked by a purported shift by the Biden administration in its approach to the war on terror as it claims to move away from "boots on the ground" and direct interventions in Southwest Asia and the African continent. The catastrophic project of the war on terror has grown increasingly untenable for a United States grappling with a deteriorating image and strategic position within a global geopolitical and economic order, complicated by its failed response to the COVID-19 pandemic, the twin crises of uprisings against racialised state violence and the threat of a growing and active political Right, and a series of embarrassing and costly cyberattacks in the early months of the Biden presidency. Against this backdrop, and capitalising on cyber investments by the Trump administration as well as those precipitated by the US response to the 2021 Russian invasion of Ukraine, the US security state presents cybersecurity as a necessary and underinvested project, simultaneously signifying glaring insecurities and enticing economic opportunities.

Interestingly, cybersecurity is also a project of the security state that has by and large flown under the radar of explicit political critique. Even as the 2020 uprisings across the United States generated and mainstreamed calls to abolish institutions of racialised state violence and drew attention to their technical and algorithmically driven infrastructures – such as biometric surveillance technologies, consumer credit rating systems, and the database logics of Child Protective Services – cybersecurity itself has thus far evaded such explicit critiques.[5] To be clear, this is not a critique of abolitionist and anti-imperial politics and discourse. Rather, this absence is curious to me. *Why and how* does cybersecurity in particular evade political critiques that other digitally and data-driven technologies of governance do not?

I thus propose what may seem at first an obvious possibility: cybersecurity is tedious, highly technical, and incredibly *boring*. However, I suggest that cybersecurity's boring procedural veneer conceals not only the banal work of cyber police power but also cybersecurity as a technique of governance whose very mundanity provides a useful conduit by which to enact more pervasive policies and practices of US police power and state violence. To untangle the banal exercises of police power within cybersecurity, I draw from recent work by Shiloh Krupar to situate cybersecurity as a technology of "*operational banality*" (Krupar, 2020).[6] For Krupar, these especially boring and quotidian techniques of governance are animated folklorically and constitute "the messy and ambiguous terrain of banal norms, narratives, and their techno-procedural implementations":

> A system that demonstrates FOOB [folklore of operational banality] is reductive, tautological, and iterative … [its] operations are relentlessly optimized and/or moralized and take on a life of their own, in ways that are simultaneously unremarkable/banal and absurd/grotesque. These qualities all require that FOOB systems demonstrate *affect* – of objectivity, passivity, disinterestedness … The ordinary appearance of a FOOB system is therefore *contrived*. "Banality" describes not its ubiquitousness (though it may be ubiquitous), nor its regularity of occurrence (though it may be constant), but rather its affect. FOOB phenomena are characterized by an "affect plateau": everything is presented with the same affect or through the same channel, making it difficult to differentiate levels of degree. For instance, an impending heat wave occupies the same register as threat of war.
>
> (Kupar, 2020: 432 emphasis in original)

While Krupar (2020: 438) theorises operational banality through an analysis of the Health Coach App and its impacts on discourses of health and personal responsibility, the medical hotspotting Krupar (2020: 445) analyses relies on the very same logics of preemption that characterise data-driven practices of the war on terror. Further, this logic reflects discourses of digital hygiene that have historically inflected both industry and personal computing practices, such as those which Jussi Parikka (2007) traces to the moral, and I would add racial, panics surrounding HIV/AIDS in the 1980s and 1990s.

The "affect plateau" that Krupar (2020: 432) attributes to technologies of operational banality is particularly potent for examining the banality of police power within cybersecurity, whereby intensities of feeling undifferentiated by kind and degree emerge and merge within an atmosphere of security itself as everyday and mundane in the context of the ongoing war on terror.[7] Of course this affective plateau is one differentially experienced by and meted upon those targeted by the security state, particularly those persons racialised through ontologies of terrorist threat. However, in the context of cybersecurity, specified threats most typically take the form of nation-state actors – Russia, North Korea, China, and Iran – or evasive hacker collectives and figures whose murky subjectivities, as Kriss Ravetto-Biagioli (2013: 186) has argued through the case of Anonymous, emerge memetically and less oriented around conventional notions of identity and identification.

The simultaneity of fear and disinterest that has so characterised the "affect plateau" of the post-9/11 United States coheres through cybersecurity. A Pew Research Center Poll from 2017 found that "most Americans do not express profound worries about cybersecurity in their personal lives or in their public expectations for various institutions", while a 2021 poll by The Pearson Institute and The Associated Press-NORC Center for Public Affairs Research found "about 9 in 10 Americans are at least somewhat concerned" about threats posed by hacking and cybersecurity to financial institutions and personal data, national security and defence systems, energy infrastructures, health care, and government services.[8] Notably, unlike the 2017 Pew study, the 2021 Pearson-AP-NORC poll does not provide data about whether Americans' *worries* about cybersecurity attacks, which the study notes are markedly correlated by age (less than half of those polled between 18 and 29 indicated concern that the study identified as "extremely" or "very concerned"), translate into modifications of personal computing habits, or correspond to faith in the US government to address cybersecurity vulnerabilities. While this data is absent, the poll does show that by and large those polled, about seven in ten, believed the Chinese and Russian governments pose the gravest threats to US cybersecurity, while less than half were concerned with the threat posed by individual hackers.[9]

There is much to say about what it means that cybersecurity discourse has helped to reanimate China and Russia as the villainous enemies of the United States, a repetition of Cold War–era narratives that, of course, never truly dissipated, as well as much to say about how this corresponds to amplified Sinophobic and more broadly anti-Asian racism and violence within the United States. However, I focus on how circumscribing cybersecurity threat and practice to the realm of state actors obscures the mundane and much more expansive police powers of cybersecurity, which increasingly preoccupy not only the US federal government but also state and local police agencies of all sizes. For instance, in the case of Augusta, Georgia, the Georgia Cyber Center brings cyber operations for the US Army and National Guard, intelligence services, and the Georgia Bureau of Investigation and local police together with cybersecurity education through Augusta University and private industry within a single campus, the largest to date in the United States. As the resident Georgia Cyber Crime Center (G3C) of the Georgia Bureau of Investigation states,

> The mission of G3C is to assist local and state law enforcement agencies with complex investigations involving cyber-related criminal activity. This includes but is not limited to online fraud, computer and network intrusion, *and the proliferation of digital media* (the Internet of Things/IoT) as they relate to criminal activity and organised crime.[10]

G3C's reference to "the proliferation of digital media" here is both troubling and telling, pointing toward a much broader conceptualisation of cybersecurity. Specifically, while popularly and often publicly presented as the exercise of state power as it is concerned with network security and data privacy, in application, cybersecurity increasingly appears to simply mean the exercise of police power within and through digital spaces and media more broadly.

Thus, the *Cyber Center* operates much like intelligence *fusion centres*, wherein intelligence-gathering and social media monitoring practices and agencies converge. As Brendan McQuade identifies, these sites act as "a central component of mass supervision, a state strategy to pacify surplus populations in our nascent post-neoliberal world of low growth and soaring inequality" (McQuade, 2019: 16). I join McQuade (2019) in suggesting that whether framed as cybersecurity or intelligence fusion, these data-driven practices of policing do not evince an altogether *new form* of police power but, rather, function as sites through which police power as pacification cohere. In this way, the operational banality and bureaucratic veneer of geopolitical maneuvering attributed to cybersecurity – a matter of *states* – conceals how cybersecurity continues to grow more conceptually expansive and useful for the exercise of security practices at a variety of scales. Thus, I locate this analysis of cybersecurity as police power within and alongside articulations of war power and police power as co-constituting, where both are forged through histories of colonial violence and pacification (Neocleous, 2014; Siegel, 2018; Wall, Saberi, and Jackson, 2017; Kaplan and Miller 2019; Miller, 2019). As Caren Kaplan and I have argued in conversation with Mark Neocleous (2014) and Micol Seigel (2018): "This perceived gap between the military and the police … evacuates everyday manifestations of power and renders banal the persistent violence of policing, in favour of the spectacularisation of war at a distance" (Kaplan and Miller, 2019: 420). Further, Tyler Wall, situating the use of drones in the US war on terror in relation to everyday racialised police violence within the United States, contends police power traffics historically and explicitly in the banal. Police power is in fact, according to Wall, "the most insidious and 'ordinary' of all emergency powers" (Wall, 2016: 1124). In other words, the very banality of police power functions as itself a tried and true technique of the security state. This banality is, I argue, amplified through police power's coupling with cybersecurity, whereby the banal commandment of cybersecurity proclaims the mundanity of technical bureaucracy and statecraft while concealing the increasingly expansive exercise of police power with which cybersecurity is charged.

Further still, these banal exercises of police power that emerge through cybersecurity constitute those that Achille Mbembe identified as characteristic of the postcolony – the ludic, grotesque, and utterly mundane *simulation* of having transcended coloniality in which the dominating and dominated persist in a state of "mutual "zombification" much like the "affect plateau" theorised by Krupar (2020: 432). According to Mbembe (1992: 3), the simulation of postcoloniality operates through the reinscription of the colonial "*commandement*", which constitutes "the authoritarian modality *par excellence*" and "a fantasy that it presents to its subjects as a truth that is beyond dispute, a truth that has to be instilled into them in order that they acquire a habit of discipline and obedience" (Mbembe 1992:12). In the settler-colonial and imperial context of the United States, as Wall instructs, the *commandement* emerges through "the mystical power of police discretion" and manifests in "its resistance to any legal definition" (2016: 1132). Thus the banal *commandement* of police power within cybersecurity proclaims the mundanity of technical bureaucracy and statecraft alongside individual worry and disinterest as civic obligations in order to propel the United States" efforts to deter cyber threats from illiberal state enemies.

It is the banal *commandement* of police power in cybersecurity that subtends its legal and applied expansion, particularly through the state's emphasis on cyber threats as "National Critical Functions", or NCFs. As a mundane realm of the NCF, cybersecurity takes on an additive even if more invisibilised dimension as those practices necessary to secure critical infrastructure, a national security designation of all manner of physical and information systems and processes that enable the functions of state and capital. In the section that follows, I examine how the growing emphasis on cybersecurity has marked a shift in US national security policy from critical infrastructure governance away from objects and assets toward NCFs. A shift in critical infrastructure governance to an emphasis on security practices invites, in turn, an ethnographic attunement not only to those practices but also to the modalities of political attention and inattention that inform embodied and emplaced critiques of the banal project of cybersecurity.

From critical infrastructure to critical national function

In an October 2021 statement on Cybersecurity Awareness Month, US President Joe Biden beseeched Americans, "We must lock our digital doors". Citing a multiscalar cyber threat impacting individuals as well as businesses and communities of all sizes, Biden proclaimed that nothing short of a "whole-of-nation" approach to cybersecurity would be necessary to combat emergent dangers to the nation's digital infrastructure.[11] This language echoed that of the Biden administration's June appeal to private industry leaders: "Much as our homes have locks and alarm systems and our office buildings have guards and security to meet the threat of theft", so too must we "match the threat" of cyberterrorism through a personal and industry commitment to cyber fortification and security.[12] These recent statements anticipated the much-lauded introduction of the bipartisan HR 5491 Securing Systemically Important Critical Infrastructure Act, introduced by Congress on 5 October 2021, to "designate certain elements of critical infrastructure as *systemically important*". Notably, HR 5491 marshals the emergent category of National Critical Function, a public or private function so critical "that the disruption, corruption, or dysfunction of such function would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof".[13] A term that has quietly suffused the discourse of critical infrastructure via cybersecurity in recent years, National Critical Functions marks the growing centrality of cybersecurity as a mode of liberal governance for the United States, where the very banality that makes cybersecurity so uninteresting is the very same that makes it an opportune site for the legal and applied expansion of police power.

Introduced in 1996 by the Clinton administration, critical infrastructures were defined as those "so vital that their incapacity or destruction would have a debilitating impact on the defence or economic security of the United States".[14] The Bush administration vastly expanded this definition following 11 September 2001, and critical infrastructure has remained an organising concern of the US national security state throughout the now 20 years of the war on terror. In this context, everything from factory farms to sports stadiums to Confederate statues and energy grids figure as vital components of the national security state. Increasingly framed around securing the Internet of Things (IoT),[15] critical infrastructure policy and governance have further emerged as a primary legal mechanism through which to strengthen the scope and investment of cybersecurity as a sphere of US police power. Notably, this focus on cybersecurity has engendered a shift in critical infrastructure policy from assets and objects to functions, a shift that I argue reflects the everyday machinations of colonial police power *through practice* that cohere through cybersecurity (Coleman, 2016).

While critical infrastructure has generated particular legal architectures and applications that have corresponded to US expansionism and national security in the war on terror, the security-infrastructure relation has a much longer history that can be traced through the reorganisation of colonial geopolitical order following World War II.[16] Here, I draw from the genealogy of infrastructure charted by Ashley Carse, who notes that engineers adopted the term infrastructure into English in the early 20th century to connote "supranational military coordination and international economic development" following World War II (Carse, 2018: 31). Infrastructure, Carse argues, became "world-making", a reflection of the political and economic geopolitical reality instituted through supranational projects like the International Monetary Fund (IMF), the Bretton Woods agreement of 1944, and the formation of the United Nations in 1945 (Carse, 2018: 31).

The security-infrastructure relation has been further expanded through the designation of "critical infrastructures" by the US security state in laying the groundwork for and now throughout the ongoing US war on terror. Nonetheless, "critical infrastructure" as a national security concept remains somewhat undertheorised in its US context and specifically through its applications in the US war on terror, even as studies of infrastructure and what is often referred to as "critical infrastructure studies" (in other words, critical studies of infrastructure) have received much scholarly attention in recent years. Some notable exceptions include Peter Gallison's 2010 "Secrecy in Three Acts", Joseph Masco's ""Sensitive but Unclassified"" from the same year (2010), and Masco's treatment of critical infrastructure in his 2014 *The Theater of Operations*. More recently, Shiri Pasternak and Tia Dafnos (2018), Tia Dafnos (2020), and Andrew Crosby (2021) have analysed critical infrastructure as it has been mobilised in Canada to police Indigenous land and water protector movements, and Kai Bosworth and Charmaine Chua (2023) have addressed the concept in the US context of infrastructural blockades at Standing Rock.

As both Masco (2014: 31) and Galison (2010) point out, critical infrastructure as deployed by the Bush administration emerges as an expansive, totalising, and reductive concept that absents scale, context, place, and specificity in order to generate simply more objects of national security. As Masco has usefully argued, the "concept of critical infrastructure flattens risk across radically different objects and domains … [to] allow for radical new forms of policing at home and abroad". In particular, these objects and domains primarily cohere in the form of *private assets*. As Galison (2010: 968) notes, approximately 85 percent of critical infrastructures comprise private rather than public assets. The ascendance of critical infrastructure as a national security concept likewise informs the recent spate of legislations criminalising acts of protest that interfere with or damage critical infrastructure like pipelines and interstates.[17] As Bosworth and Chua argue, these moves belie "the fundamental anxiety that motivates state power and settler subjects to continually protect critical infrastructure has its sources in an economic project of securing flows that takes shape as a racial-colonial project of reaction and extermination" (Bosworth and Chua, 2023). In this way, critical infrastructure emerges as another site of Mbembe's *commandement*, one that posits the everyday flows of capital and commodities as a realm of "truth that is beyond dispute" and one that requires honing an unquestioning "habit of discipline and obedience" (Mbembe, 1992: 12). The *commandement* of critical infrastructure posits the nation as only a nation insofar as the infrastructural flows of capital, goods, and energy defy interruption, a colonial common sense that, as Bosworth and Chua (2023) point out, is challenged through Indigenous blockades "as an exercise of countersovereignty". Thus, the colonial common sense of critical infrastructure is at once so banal that it seems not worth mentioning yet so *critical* that its very disruption belies the instability and incoherence of the colonial security state.

Further, the flattening, threat-generating common sense of critical infrastructure offers a fertile terrain through which the state seeks to expand the banal workings of police power within the context of cybersecurity in particular. While laws criminalising protest and disruption or destruction of critical infrastructure following Standing Rock and the ongoing protests against racialised police violence in the United States have drawn critical attention, critical infrastructure laws premised on fortifying cybersecurity prove much less interesting and, so far, more insulated from public scrutiny. It is in this context that I address an emergent move within current national security policy that shifts critical infrastructure governance away from objects and assets toward what are being termed “National Critical Functions” or NCFs. First coined in a 2019 Trump Executive Order, NCFs are defined as “the functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on national security, economic security, public health or safety, or any combination thereof” (Executive Order 13865). This definition, which hews closely to the definition of critical infrastructure itself, was then expanded by the Cyber and Infrastructure Security Agency in policy documents from April 2019 and July 2020 that also define what they term the “National Critical Functions Set”, which designates 55 functions across four areas: supply, distribute, manage, and connect. The CISA determines a focus on function as a “more holistic approach” and refers to “the National Critical Functions construct” as “a new ‘language’ that we can use to talk about critical infrastructure risk management” (CISA 2019: 1, 2). Elsewhere in July 2020, the CISA states that “NCFs effectively reset the critical infrastructure risk management framework” and that the introduction of the NCF set “represented a nested, hierarchical, and bi-directional network” that “involves a complicated series of process composed of sub-processes and dependencies” (CISA 2020: 1, 9–10).

Notably, this language figures prominently in the Biden administration’s early emphasis on critical infrastructure vis-à-vis cybersecurity, showing up in his May Executive Order on Improving the Nation’s Cybersecurity, two June memos, and his October statement on Cybersecurity Awareness Month. In that October statement, as I mentioned briefly in this section’s introduction, Biden tells Americans “We must lock our digital doors”, building on his June assertion to private industry leaders that “much as our homes have locks and alarm systems and our office buildings have guards and security to meet the threat of theft”, so too must Americans rely on personal and business security measures to “match the threat” of cyberterrorism (WH June 2021 Memo). These statements notably serve as a policy basis for the bipartisan HR 5491 Securing Systemically Important Critical Infrastructure Act, introduced by Congress on 5 October 2021, to “designate certain elements of critical infrastructure as *systemically important*”. Of note for this essay, HR 5491 marshals the emergent category of National Critical Function, a public or private *practice* so critical “that the disruption, corruption, or dysfunction of such function would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof”.[18]

As an adaptation of the definition of critical infrastructure operationalised by the United States for more than two decades, the designation of NCFs appears to mark a shift in critical infrastructure governance from a concern with assets and objects to one of *practices*. On the one hand, this certainly reflects an increased governmental anxiety regarding the perceived risks of cyberterrorism emanating from state actors such as Russia, China, and Iran, an anxiety marked in no small part by the United States’ incapacity to meet those perceived threats both in military cyber-readiness and through a pronounced shortage of cybersecurity workers, with estimates ranging from 367,000 to 477,000 cybersecurity job openings in the United States as of October 2021.[19] However, this anxiety is subtended by a great deal of enthusiasm for a perceptibly vast market of exponential growth – economically and, I would add, as a route by which to fortify and expand US police power for local and municipal police agencies as well as for counterterrorism operations more broadly. Specifically, this fortification and expansion of police power is facilitated through the banality attributed to cybersecurity policy, which is seen as simply an arena of everyday bureaucratic practices *and* privacy-protecting functions.

This shift in governance, from a concern with objects and assets to practices, also marks an epistemological shift for the security state, as critical infrastructure encounters conceptual limitations when attempting to account for the extensivity of cybersecurity and toward a cybernetic algorithmic model of statehood that leans into networked notions of protocol and circulation (notably, a shift that also corresponds to the deterioration of the objects and assets previously centred in critical infrastructure policy in the United States).[20] However, I suggest that this reorganisation of national security discourse is simply that – a reorganisation of national security discourse. Further, it is a reorganisation of national security discourse that reflects the longstanding operations of colonial police power, which I previously argued have historically functioned through data-driven, taxonomizing practices of "protocological violence", whereby algorithmic practices such as biometric data collection "emerge through and alongside historical techniques of colonial dispossession, extraction, and governance that pervade the management of persons, populations, and territory" (Miller, 2017a)[21] Placing biometric data collection programmes in the US war on terror in conversation with the database logics that organise the warehousing of Native remains at University of California, Berkeley's Phoebe A. Hearst Museum of Anthropology, I suggested that it is useful to examine colonialist algorithmic practices through what Isabelle Stengers terms "ecologies of practice", an analytic approach that entails thinking "through the middle" and "with the surroundings" (Strangers, 2005: 187). In other words, locating cybersecurity practice within STS ecologies of practice would entail a *situated* engagement with the banal practices and emplacements of cybersecurity. If cybersecurity policy is itself attuned to processes and protocols, how are those lived? How are they enacted and mediated through the contours of place-based, historical, and political specificity? With what other worlds and practices do they collide, disagree, evade, and are evaded by?

Ethnographies of practice and how not to be a cop

In closing, I offer a methodological reflection on STS ecologies of practice and the banal practices of cybersecurity. Locating ethnography as the primary scholarly method to engage with STS ecologies of practice, I ask what ethical and political considerations ensue when we locate cybersecurity and police power as ethnographic concepts that are not evidentiary and discoverable – the stuff of investigations – but, rather, situated and partial concepts that emerge through constellations of practices that do not exclude scholarly praxis (Mol, 2003). To this end, I draw from Mario Blaser and Marisol de la Cadena's proposal to "think of ethnography as a scholarly genre that conceptually weaves together those sites (and sources) called the theoretical and empirical so that they cannot be pulled apart". As a "*concept-making genre*", ethnography generates concepts that "signal their connections to place, for they are not without it" (Blaser and de la Cadena, 2018: 5, emphasis added). Following Blaser and de la Cadena (2018: 5), practices of fieldwork enact concepts through and in relation to other historically situated and place-based practices of being, doing, and knowing. Together, these entanglements of practices constitute "worlding tools" that are also, as Kathleen Stewart (2012: 520–521) suggests, tools of "*un*worlding".[22] Whether framed in dualistic terms of construction and destruction, recognition and nonrecognition, or invocation and excommunication, the simultaneity of ethnographic worlding and unworlding is, if we follow de la Cadena, not only an inevitability but also an invitation (De la Cadena, 2015: 212–214). The meeting of worlds and words generates "misunderstandings", which becomes "a problem" only insofar as "the intention is for the understanding to be *one*". By "avoiding the univocal" and inhabiting misunderstanding, de la Cadena asserts, the ethnographer can "make the conversation just that – a conversation" (De la Cadena, 2015: 214, emphasis added). The potential for harm and undoing that suffuses ethnographic misunderstanding is not, then, inherent to the misunderstanding itself but, rather, depends on our ethnographic and political practices as we engage in conversations with, and in the making of, concepts.

What might this entail for those of us working as ethnographers of police power and technologies of state violence such as cybersecurity, artificial intelligence, and algorithms? What does it mean to undertake the ethnographic proposal of concept-making when our concepts are deeply overdetermined by historical and persistent harm? What worlds meet, what misunderstandings emerge, and what stories are told in our conversations with the technological objects and systems that enable and enact state violence? I conclude by suggesting that if, as Tyler Wall argues, police power defines the very order of humanity itself – a world in which "police is civilisation and civilisation is police" – the world-making and unmaking capacity of cybersecurity emerges as a site of dense and potent political obligation (Wall, 2019: 322). Do we wish to make and remake the worlds forged through the civilisational crucible of police power within our ethnographic storying, that gumshoe impulse that seeks only accumulative and evidentiary accounts in our concept-making? Put plainly, we must ask ourselves: do we want to be cops?

I propose that STS ecologies of practice, informed by feminist and decolonial anthropological methods, offer a methodological model to think differently with concepts, even those concepts with which the ethnographer might fervently disagree and wish to dismantle. For Isabelle Stengers, what she terms "an ecology of practice is a tool for thinking through what is happening, and a tool is never neutral" (Stengers, 2005: 185). Rather, an ecology of practice, as Stengers conceptualises it, is a decidedly anti-capitalist orientation to the study and making of concepts – not least of all scientific concepts – that requires resisting the seductions of teleological storytelling, progress, and truth, what Stengers terms thinking in the "major key" (Stengers, 2005: 185–186). Instead, Stengers outlines "thinking in the minor key" as one step to a non-neutral ecology of practice, where thinking, ethics, and politics manifest relationally through ethnographic practice with the aim to "create a different practical landscape" (Stengers, 2005: 186–187).

For this chapter, thinking in the minor key invited me to begin with and remain provoked by my ethnographic encounter with torn posters and disinterested shrugs as political gestures. It is the eventfulness of these uneventful gestures, what de la Cadena would describe as the "eventfulness of the ahistorical", that prompted me to consider the very uneventfulness of cybersecurity and its practical landscape rather than the other way around (De la Cadena, 2015: 150–151). The tear and the shrug, then, resonate with Adeyemi's conceptualisation of "microgestures of dissent", which Adeyemi (2019a) develops to think through queer Black modalities of slow politics and place-making that critique and exceed the pace of neoliberal gentrification in Chicago. Just as Adeyemi argues that microgestures of dissent "demonstrate fundamental ambivalences … less intelligible and codified, but no less powerful" political assertions, so too do I suggest that the tear and the shrug function in the case of Augusta and as provocations to ethnographic practice (Adeyemi, 2019a: 548).[23] Casual, disorderly, and subjectless contestations to the banal and orderly project of cybersecurity, the tear and the shrug certainly signify insurgent responses to datafication and a "right to opacity" in the spirit of Simone Browne's "dark sousveillance" (2015: 21–2, 68, 164); Kara Keeling's politics of "unaccountability" (2019: 41–51) and opacity, drawing from Glissant (1997); and Clare Birchall's "experimenting with secrecy" (2016: 159). As the banal commandment of police power within cybersecurity conceals its desire to make knowable, enumerable, and, thus, containable beneath a veneer of the boring and everyday, the political gestures of the tear and the shrug respond in kind as assertions of incalculability and illegibility against the smooth, functionary order of cybersecurity. Further, these gestures point toward a politics of disavowal and disinterest that is methodologically instructive – an ethnographic provocation to think "through the middle" and "with the surroundings" (Stengers, 2005: 186–187). What these banal and uneventful gestures of political critique may very well offer, then, is a methodological reflection on how not to be a cop.

Notes

[1] For an in-depth examination of cybersecurity-driven redevelopment in Augusta, Georgia, and the urban ecosystem, see Miller (2022).

[2] "theClubhou.se Launches their Second Startup Life Program", *Augusta CEO*, 19 March 2019, http://augustaceo.com/news/2019/03/theclubhouse-launches-their-second-startup-life-program/.

[3] On the relationship between Bartleby, Blackness, and opacity, see Keeling (2019). On Bartleby and "the minor key", see Stengers (2005), Deleuze (1998).

[4] see also Center for Constitutional Rights, "Court Dismisses No-Fly Retaliation Case", 3 September 2015, https://ccrjustice.org/home/press-center/press-releases/court-dismisses-no-fly-retaliation-case;

[5] Dorothy Roberts, "Abolishing Policing Also Means Abolishing Family Regulation", *The Imprint*, 16 June 2020, https://imprintnews.org/child-welfare-2/abolishing-policing-also-means-abolishing-family-regulation/44480; Molly Schwartz, "Do We Need to Abolish Child Protective Services?", *Mother Jones*, 10 December 2020, https://www.motherjones.com/politics/2020/12/do-we-need-to-abolish-child-protective-services/; for a capacious account of the digital and abolition, see J. Khadijah Abdurahman, ed. "Beacons", *Logic* 15 (2015). Of note, recent calls have been made to apply abolition to *security* more broadly. As Brendan McQuade has recently argued, "*Abolition is the foil of bourgeoisie security*. Where security discourses are concerned with fabrication of capitalist forms of social order, abolition is a way of thinking about producing social order outside of the logic of capital and private property, state violence, and racialized subjectivity" McQuade (2018: 5). See also Machold and Chiniara Charett (2021).

[6] I have italicised the text to note that for future uses I do not employ quotation marks but nonetheless attribute this term to Krupar. Also on banality, see Mbembe (1992), Katz (2007), and Arendt (2006).

[7] See also Masco (2014), Amoore and de Goede (2008), Massumi (2015), Kaplan and Miller (2019), Kaplan (2017), Kaplan (2021), Kaplan (2020), Parks (2018), Adey (2014), and Stewart (2011).

[8] Aaron Smith, "Americans and Cybersecurity", Pew Research Center, 26 January 2017, https://www.pewresearch.org/internet/2017/01/26/americans-and-cyber-security/; Alan Suderman, "Cyberattacks Concerning to Most in US: Pearson/AP-NORC poll", AP News, 11 October 2021, https://apnews.com/article/joe-biden-technology-business-china-russia-c9a698542ed95bfa49f9cee0e96ef9a6. For full report, see the Pearson Institute and the Associated Press-NORC Center for Public Affairs Research, "The Public is Highly Concerned About Cyber Attacks on the United States", October 2021, https://apnorc.org/wp-content/uploads/2021/10/cybersecurity_final.pdf.

[9] The Pearson Institute and the Associated Press-NORC Center for Public Affairs Research, "The Public is Highly Concerned About Cyber Attacks on the United States".

[10] "Georgia Cyber Crime Center (G3C), "Georgia Bureau of Investigation", accessed November 2021, https://investigative-gbi.georgia.gov/investigative-offices-and-services/specialized-units/georgia-cyber-crime-center-g3c, emphasis added.

[11] White House, "Statement by President Joe Biden on Cybersecurity Awareness Month", 1 October 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/01/statement-by-president-joe-biden-on-cybersecurity-awareness-month/, accessed 12 October 2021.

[12] White House, "What We Urge You to Do to Protect Against the Threat of Ransomware", 2 June 2021, https://www.whitehouse.gov/wp-content/uploads/2021/06/Memo-What-We-Urge-You-To-Do-To-Protect-Against-The-Threat-of-Ransomware.pdf, accessed 14 November 2021.

[13] Securing Systemically Important Critical Infrastructure Act, H.R. 5491, 117th Cong. (2021), emphasis added.

[14] Exec. Order No. 13010, 61 C.F.R. 138 (1996). On critical infrastructure, see Galison (2010), Masco (2014).

[15] Cybersecurity and Infrastructure Security Agency, "Security Tip (ST17-001): Securing the Internet of Things", 14 November 2019, https://us-cert.cisa.gov/ncas/tips/ST17-001.

[16] On the relationship between infrastructure and state power and violence, see Easterling (2014), Star (1999), Star and Ruhleder (1996), Bowker (1994), Bowker and Star (1999), Starosielski (2015), Parks and Starosielski (2015), Carse (2014), and Harvey and Knox (2015).

[17] See, for instance, Dan Shea, "Balancing Act: Protecting Critical Infrastructure and Peoples" Right to Protest", National Conference of State Legislatures, 21 July 2020, https://www.ncsl.org/research/energy/state-policy-trend-protecting-critical-infrastructure-and-peoples-right-to-protest-magazine2020.aspx; Kaylana Mueller-Hsia, "Anti-Protest Laws Threaten Indigenous and Climate Movements", March 17, 2021, https://www.brennancenter.org/our-work/analysis-opinion/anti-protest-laws-threaten-indigenous-and-climate-movements.

[18] Securing Systemically Important Critical Infrastructure Act, H.R. 5491, 117th Cong. (2021), emphasis added.

[19] Mark Pomerleau, "Russia and China Devote More Cyber Forces to Offensive Operations than US, Says New Report", *C4ISRNET*, 13 February 2022, https://www.c4isrnet.com/cyber/2022/02/14/russia-and-china-devote-more-cyber-forces-to-offensive-operations-than-us-says-new-report/;Joseph Marks, "The U.S. Cyber Workforce Gap is Getting Bigger", *The Washington Post*, 26 October 2021, https://www.washingtonpost.com/politics/2021/10/26/us-cyber-workforce-gap-is-getting-bigger/.

[20] See, for example, Galloway (2004), Galloway and Thacker (2007), Castells (2012), Hardt and Negri (2000), and Hardt and Negri (2004).

[21] https://radicalantipode.files.wordpress.com/2017/05/6-andrea-miller.pdf. This is very much in line with Ruha Benjamin's articulation of race itself as a technology that precedes the introduction of digital technologies and constitutes "the sorting, establishment and enforcement of racial hierarchies with real consequences". See Benjamin (2019: 53). See also Coleman (2019), Browne (2015), and TallBear (2013).

[22] See also de la Cadena (2015); de la Cadena (2010), and Mol (2003).

[23] See also Adeyemi (2019b).

References

Adey, P. (2014) 'Security Atmospheres or the Crystallisation of Worlds', *Environment and Planning D: Society and Space,* 32(5), 834–851.

Adeyemi, K. (2019a) 'The Practice of Slowness: Black Queer Women and the Right to the City', *Journal of Lesbian and Gay Studies,* 25(4), 545–567.

Adeyemi, K. (2019b) 'Beyond 90°: The Angularities of Black/Queer/Women/Lean', *Women & Performance: A Journal of Feminist Theory,* 29(1), 9–24.

Amoore, L. and de Goede, M. (2008) 'Transactions after 9/11: The Banal Face of the Preemptive Strike', *Transactions of the Institute of British Geographers,* 33(2), 173–185.

Arendt, H. (2006) *Eichmann in Jerusalem: A Report on the Banality of Evil*, with an introduction by Amos Elon. New York: Penguin Books (1963).

Benjamin, R. (2019) *Race After Technology: Abolitionist Tools for the New Jim Code*. Medford, MA; Polity Press.

Birchall, C. (2016) 'Managing Secrecy', *International Journal of Communication,* 10, 152–163.

Blaser, M. and de la Cadena, M. (2018) 'Introduction: Pluriverse: Proposals for a World of Many Worlds', in M. de la Cadena and M. Blaser (eds.) *A World of Many Worlds*. Durham, NC: Duke University Press, 1–22.

Bosworth, K. and Chua, C. (2023) 'The Countersovereignty of Critical Infrastructure Security: Settler-State Anxiety versus the Pipeline Blockade', *Antipode,* 55(5), 1345-1367.

Bowker, G.C. (1994) *Science on the Run: Information Management and Industrial Geophysics at Schlumberger, 1920–1940*. Cambridge, MA: MIT Press.

Bowker, G.C. and Star, S.L. (1999) *Sorting Things Out: Classification and Its Consequences*. Cambridge, MA: MIT Press.

Browne, S. (2015) *Dark Matters: On the Surveillance of Blackness*. Durham, NC: Duke University Press.

Carse, A. (2014). *Beyond the Big Ditch: Politics, Ecology, and Infrastructure at the Panama Canal*. Cambridge, MA: MIT Press.

Carse, A. (2018) 'Keyword: Infrastructure – How a Humble French Engineering Term Shaped the Modern World', in P. Harvey, C. Bruun Jensen, and A. Morita (eds.) *Infrastructures and Social Complexity: A Companion*. London: Routledge, 27–39.

Castells, M. (2012) *Networks of Outrage and Hope: Social Movements in the Internet Age*. Malden, MA: Polity Press.

Chandler, K. (2020) *Unmanning: How Humans, Machines and Media Perform Drone Warfare*. Rutgers, NJ: Rutgers University Press.

CISA (2019) 'National Critical Functions: An Evolved Lens for Critical Infrastructure Security and Resilience'. US Department of Homeland Security Cybersecurity and Infrastructure Agency. 30 April 2019. https://www.cisa.gov/sites/default/files/publications/national-critical-functions-overview-508.pdf.

CISA (2020) 'National Critical Functions: Status Update to the Critical Infrastructure Community'. US Department of Homeland Security Cybersecurity and Infrastructure Security Agency. July 2020. https://www.cisa.gov/sites/default/files/publications/ncf-status-update-to-critical-infrastructure-community_508.pdf.

Coleman, M. (2016) 'State Power in Blue', *Political Geography,* 51, 76–86.

Coleman, B. (2019) 'Race as Technology', *Camera Obscura,* 70, 24(1), 177–207.

Crosby, A. (2021) 'The Racialized Logics of Settler Colonial Policing: Indigenous 'Communities of Concern' and Critical Infrastructure in Canada', *Settler Colonial Studies,* 11(4), 411–430. http.doi.org/10.1080/2201473X.2021.1884426.

Dafnos, T. (2020) 'Energy Futures and Present Threats: Critical Infrastructure Resilience, Accumulation, and Dispossession', *Studies in Political Economy,* 101 (2), 114–134.

Deleuze, G. (1998) 'Bartleby; Or, The Formula', in G. Deleuze (ed.)*Essays Critical & Clinical*. New York: Verso, 68–90.

de la Cadena, M. (2010) 'Indigenous Cosmopolitics in the Andes: Conceptual Reflections Beyond Politics', *Cultural Anthropology,* 25(2), 334–370.

de la Cadena, M. (2015) *Earth Beings: Ecologies of Practice Across Andean Worlds*. Durham, NC: Duke University Press.

Easterling, K. (2014) *Extrastatecraft: The Power of Infrastructure Space*. New York: Verso.

Galison, P. (2010) 'Secrecy in Three Acts', *Social Research,* 77(3), 941–974.

Galloway, A. (2004) *Protocol: How Control Exists After Decentralization*. Cambridge: Massachusetts Institute of Technology Press.

Galloway, A. and Thacker, E. (2007) *The Exploit: A Theory of Networks*. Minneapolis: University of Minnesota Press.

Glissant, É. (1997) *Poetics of relation*. Ann Arbor: University of Michigan Press.

Hardt, M. and Negri, A. (2000) *Empire*. Cambridge, MA: Harvard University Press.

Hardt M. and Negri, A. (2004) *Multitude: War and Democracy in the Age of Empire*. New York: Penguin.

Harvey, P. and Knox, H. (2015) *Roads: An Anthropology of Infrastructure and Expertise*. Ithaca, NY: Cornell University Press.

Kaplan, C. (2006) 'Precision Targets: GPS and the Militarization of Consumer Identity',*American Quarterly* 58 (3), 693–713.

Kaplan, C. (2017) *Aerial Aftermaths: Wartime from Above*. Durham, NC: Duke University Press.

Kaplan, C. (2020) 'Atmospheric Politics: Protest Drones and the Ambiguity of Airspace', *Digital War,* 1, 50–57.

Kaplan, C. (2021) 'Eyes in the Skies: *Repellent Fence* and Trans-Indigenous Time-Space at the US–Mexico Border', in A.I. Graae and K. Maurer (eds.) *Drone Imaginaries: The Power of Remote Vision*. Manchester: Manchester University Press, 203–224.

Kaplan, C. and Miller, A. (2019) 'Drones as "Atmospheric Policing": From US Border Enforcement to the LAPD', *Public Culture,* 31(3), 419–445.

Katz, C. (2007) 'Banal Terrorism: Spatial Fetishism and Everyday Insecurity', in D. Gregory and A. Pred (eds.) *Violent Geographies: Fear, Terror, and Political Violence*. New York: Routledge, 349–361.

Keeling, K. (2019) *Queer Times, Black Futures*. New York: New York University Press.

Krupar, S. (2020) 'The Folklore of Operational Banality: Medical Administration and Everyday Violence of Health', *Environmental Humanities,* 12(2), 431–432.

Machold, R. and Chiniara Charett, C. (2021) 'Beyond Ambivalence: Locating the Whiteness of Security', *Security Dialogue,* 52(S), 43–44.

Masco, J. (2010) 'Sensitive but Unclassified': Secrecy and the Counterterrorist State', *Public Culture,* 22(3), 433–463.

Masco, J. (2014) *The Theater of Operation: National Security Affect from the Cold War to the War on Terror*. Durham, NC: Duke University Press.

Massumi, B. (2015) *Ontopower; War, Powers, and the State of Perception*. Durham, NC: Duke University Press.

Mbembe, A. (1992) 'The Banality of Power in the Postcolony', *Public Culture,* 4(2), 1–30.

McKittrick, K. (2011) 'On Plantations, Prisons, and a Black Sense of Place', *Social & Cultural Geography,* 12(8), 947–963.

McKittrick, K. (2014) 'Mathematics Black Life', *The Black Scholar,* 44(2), 16–28.

McQuade, B (2018) 'Histories of Abolition, Critiques of Security', *Social Justice,* 45(2/3) (152/153), 1–24.

McQuade, B. (2019) *Pacifying the Homeland: Intelligence Fusion and Mass Supervision*. Oakland: University of California Press.

Miller, A. (2017a) 'Protocological Violence and the Colonial Database', *Antipode*, 19 May.

Miller, A. (2017b) '(Im)Material Terror: Incitement to Violence Discourse as Racializing Technology in the War on Terror', in L. Parks and C. Kaplan (eds.) *Life in the Age of Drone Warfare*. Durham, NC: Duke University Press, 112–133.

Miller, A. (2019) 'Shadows of War, Traces of Policing: The Weaponization of Space and the Sensible in Preemption', in R. Benjamin (ed.) *Captivating Technology: Race, Carceral Technoscience, and Liberatory Imagination in Everyday Life*. Durham, NC: Duke University Press, 85–106.

Miller, A. (2022) 'Cyber-Insecurities and Racialized Threat in the Embattled Urban Ecosystem', in R. Grusin (ed.) *Insecurity*. Minneapolis: University of Minnesota Press, 139–164.

Mol, A. (2003) *The Body Multiple*. Ontology in Medical Practice. Durham, NC: Duke University Press.

Neocleous, M. (2014) *War Power, Police Power*. Edinburgh: Edinburgh University Press.

Parikka, J. (2007) *Digital Contagions: A Media Archaeology of Computer Viruses*. New York: Peter Lang.

Pasternak, S. and Dafnos, T. (2018) 'How Does a Settler State Secure the Circuitry of Capital?' *Environment and Planning D: Society and Space*, 36(4), 739–757.

Parks, L. (2018) *Rethinking Media Coverage: Vertical Mediation and the War on Terror*. New York: Routledge.

Parks, L. and Starosielski, N. (eds.) (2015) *Signal Traffic: Critical Studies of Media Infrastructures*. Urbana, Chicago/Springfield: University of Illinois Press.

Ravetto-Biagioli, K. (2013) 'Anonymous: Social as Political', *Leonardo Electronic Almanac,* 19(4), 178–195.

Seigel, M. (2018) *Violence Work: State Power and the Limits of Police*. Durham, NC: Duke University Press.

Star, S.L. (1999) 'The Ethnography of Infrastructure', *American Behavioral Scientist,* 43(3), 377–391.

Star, S.L. and Ruhleder, K. (1996) 'Steps Toward an Ecology of Infrastructure: Design and Access for Large Information Spaces', *Informations Systems Research,* 7(1), 111–134.

Starosielski, N. (2015) *The Undersea Network*. Durham, NC: Duke University Press.

Stengers, I. (2005) 'Introductory Notes on an Ecology of Practices', *Cultural Studies Review,* 11(1), 186–187.

Stewart, K. (2011) 'Atmospheric Attunements', *Environment and Planning D: Society and Space,* 29, 445–453.

Stewart, K. (2012) 'Precarity's Forms', *Cultural Anthropology,* 27(3), 518–525.

TallBear, K. (2013) *Native American DNA: Tribal Belonging and the False Promise of Genetic Science*. Minneapolis, MN: University of Minnesota Press.

Wall, T. (2016) 'Ordinary Emergency: Drones, Police, and Geographies of Legal Terror', *Antipode,* 48(4), 1122–1139.

Wall, T. (2019) 'The Police Invention of Humanity: Notes on the 'Thin Blue Line', *Crime, Media, Culture*, 16(3), 319–336.

Wall, T., Saberi, P. and Jackson G. (2017) *Destroy, Build, Secure: Readings on Pacification*. Ottawa, ON: Red Quill Books.

3 "The server is always down!"

Digitalised complaints systems to monitor public service (mis)conduct in Kenya

Tessa Diphoorn

Introduction

In March 2018, I attended a meeting organised by the Complaints Handling and Referral Partners Network, a network established to handle and refer complaints made by citizens against public officials in Kenya. It was one of their quarterly network meetings, and in addition to discussing general affairs, the primary focus was the collective signing of the Memorandum of Understanding (MoU). The MoU had been in the making for a while and needed to be signed by the 45 state and non-state partners involved in this network. As underlined by many participants, the MoU was crucial because it would enable the organisations to collaborate more efficiently and thus enhance complaint management. As one of the female leading representatives stressed: "It is time to formally consolidate our efforts and to create a framework", so that "we can serve our communities". She repeatedly emphasised that their goal is to serve the public and that "the complainants are counting on us!"

This network meeting was one of a few that I attended during my ethnographic fieldwork in Kenya between 2017 and 2018 on the broader police reform project that the National Police Service (NPS) of Kenya had undergone since the political transformation of 2010. In addition to larger structural changes, a key component of the broader political transformation dealt with complaints against the police, and the Kenyan state in general. In Kenya there are numerous state and non-state bodies, such as specific state commissions, independent oversight bodies, and human rights organisations, that collect, document, and manage complaints from the public. In addition, there are other state institutions and commissions that manage complaints about public service delivery more generally. Combined, there is an extensive state bureaucratic apparatus aimed at managing and handling complaints against public officials, with the state police receiving the most attention.

In my research, I was interested in unpacking these "complaint biographies", as Sara Ahmed (2021) calls them, and understanding how complaints against public officials "provides a lens, a way of seeing, noticing, attending to a problem in the effort to redress the problem" (24). To understand these biographies, my interlocutors included a wide range of people that

DOI: 10.4324/9781003412908-5

were somehow involved in, or connected to, the police reform project, such as police officers, state officials working for various oversight bodies and commissions, human rights defenders, lawyers, prosecutors, and victims of police violence. As was evident during the network meeting, there are ongoing initiatives to streamline the numerous mechanisms and efforts across institutions so that, as one of the representatives voiced, the complainants can be assisted. One method of streamlining is through the creation and use of digitalised systems to gather, process, and address complaints raised by the public. These digital systems include internal ones managed within organisations and inter-institutional ones aimed at harnessing endeavours across the various state and non-state bodies. According to my interlocutors, these digitalised initiatives are primarily geared towards collaboration, more efficient complaint management, and ultimately, better public service delivery.

This increased focus on digitalisation matches a global trend of the digitalisation and computerisation of state services and the establishment of e-governance systems. Such digitalised bureaucracies are implemented within global paradigms of efficiency, transparency, and inclusivity, whereby citizens will gain easier access to key public services. Digitalised systems are habitually framed as neutral and technical solutions that will solve administrative and logistical problems. In this chapter, I problematise this technocratic vision of neutrality and show how such digitalised systems consolidate, and perhaps even exacerbate, existing inequalities and fragmentations within state institutions in Kenya. I will discuss several digitalised systems that have been implemented in Kenya to receive complaints against public officials to enhance state accountability, and more specifically police accountability, in Kenya. By drawing from and combining anthropological studies on bureaucracy (Hull, 2012; Gupta, 2012; Herzfeld, 1992), transparency (see Ballestero, 2012, 2018; Strathern, 2000; Hetherington, 2011, 2012; Mazzarella, 2006; Levine, 2004), and Sara Ahmed's (2021) analysis of complaints, I will show how such digital systems fail to address the structural problems that lie at the basis of their inadequacy and tend to reproduce existing political hierarchies and inequalities. Although digitalised systems are heralded as vehicles of structural change, I show that they are a part of the "non-performativity" (Ahmed, 2021) of procedures that institutions enact. However, like Mazzarella (2010: 784), it is not my intention to provide some kind of "functionalist explanation" and assess whether such digitalised systems are (un)productive. Rather, in concurrence with others, I argue that we need to understand the "politics of technological failure" (Jaffe and Pilo, 2023: 78) and move beyond the "technological determinism perspective" (Odote and Karuti, 2021: 560).

To unpack this argument, I will first briefly discuss the literature on digitalised bureaucracies and show how these are based on three key pillars of efficiency, transparency, and inclusivity that are housed within global development paradigms. I will then analyse the broader political transformation that has taken place in Kenya over the past two decades and the role of digitalisation therein, thereby simultaneously highlighting Kenyan specificities as well as global patterns and trends. The aim is to show how complaints systems play a prominent role in this transformation. In the three sections that follow, I describe the different digitalised complaint systems that have been implemented in Kenya and analyse how they have been experienced by the creators and users to show that these technological systems are not neutral solutions to deeper underlying structural problems. I conclude this chapter with some remarks about the need to maintain a critical stance towards increasing digitalisation and to recognise the politics of digitalisation, especially in the public sector, for both Kenya and beyond.

Digital bureaucracies

Within political anthropology, there has been a growing interest in the notion of bureaucracy (see Bear and Marhur, 2015; Hull, 2012). Rather than solely seeing bureaucracies as administrative systems that order, sort, and organise rules and procedures, anthropologists have extended the literal gaze of the "bureau", i.e., "desk or office", to examine how bureaucracies operate as organisational and institutional structures that reflect the larger structures of inequalities through which societies operate (see Kleinman, Das, and Lock, 1997). Bureaucracies largely uphold and maintain state systems rather than enhance state-society relations (Gupta, 2012; Graeber, 2015). According to Michael Herzfeld (1992), state bureaucracies should be considered as mechanisms responsible for "the social production of indifference". Furthermore, much of the work has also exposed the excessive amount of red tape (Gupta, 2012) and complex webs of bureaucracy that citizens must navigate (see Hoag, 2011).

With the increasing digitalisation of all aspects of life, we have also seen the emergence of "new bureaucratic worlds" (Mathur, 2017: 4), where certain bureaucratic procedures and systems are digitalised, such as identity management systems, smart ID cards, and biometric registration systems (Debos, 2021; Maguire, 2009; Rao, 2013: Hobbis and Hobbis, 2017; Sananes, 2021; Thiel, 2020). Across the globe there is an increase in the digitalisation of government documents, such as birth certificates, drivers' licenses, and landholding records, and the use of digital systems in elections, health care, and much more. Much of this has been encapsulated in the term e-governance, which broadly refers to "the computerised streamlining of bureaucracy" (Mazzarella, 2010: 788). In the field of public administration, a common distinction is made between e-government and e-governance (see Calista and Melitski, 2007), whereby the former refers to "government services that are electronically provided to citizens" while the latter "assumes an interactive dynamic between government elites and the citizenry" (D'Agostino et al., 2011). E-governance is often presented in opposition to non-computerised forms of bureaucracy and rests on several key pillars.

The first is efficiency: e-governance includes "the deployment of Internet-powered computing to bring about, in one fell swoop, more efficient administration and more directly democratic forms of public life" (Mazzarella, 2006: 475). Rather than waiting endlessly in lines and being transferred from one desk to the other, e-governance entails a promise that services and documents are available "just one-click away" and that, in turn, the provision of certain services will thus be expedited. In this regard, long lines and lengthy forms are framed as logistical problems that can be solved through technical and digital, solutions.

The second key feature of the e-governance paradigm is transparency. This chapter draws from a growing body on transparency in anthropology (see Ballestero, 2012, 2018; Strathern, 2000; Hetherington, 2012; Mazzarella, 2006; Levine, 2004) that highlights how transparency is essentially about making the invisible become visible. Transparency is a quality that renders an actor, object, relation, or process as knowable and accessible and thereby limits the potentiality for arbitrariness (Hetherington, 2012). Public services are described as entities that lack transparency and accountability and provide far too much space for corruption and nepotism (see Gupta, 2012). In contrast, digital systems and technologies are viewed as "magical vectors of transparency" (Poggiali, 2016: 399). An underlying premise is that once data and information become digital or computerised (and thereby accessible, see Ratner and Ruppert, 2019), they somehow carries "the stamp of incorruptibility" (Mazzarella, 2006: 485). This is strengthened by the idea that once citizens comprise certain information, i.e., become knowledgeable about a certain process, they will become more empowered. This notion frames public servants as technical experts who allow citizens to fully participate within democratic, and often neoliberal, regimes (Hetherington, 2011).

The third pillar of e-governance is accessibility and inclusivity. E-governance systems allow those who were previously disconnected and thus "invisible" to the state to become connected to the "wired world" (Mazzarella, 2010: 783). This argument is especially used in contexts such as Kenya, where large parts of the country remain inaccessible and are regarded as "the bush" and "out there". By eliminating literal physical space between a government official and a citizen through a digital system, space is created for interactions and encounters. Combined with guiding principles of efficiency, transparency, and inclusivity, e-governance systems are framed as technical and neutral solutions that essentially depoliticise state relations and practices.

These logics of transparency, efficiency, and inclusivity largely stem from global development paradigms within the "post-neoliberalism" era (Hetherington, 2011). Kregg Hetherington analyses how notions of transparency, which he describes "as a bureaucratic virtue" (3), derive from international reform discourses and projects that are largely rooted in World Bank–propagated notions of good governance, where democratic principles and procedures are coupled with civic participation and transparency. Transparency is showcased as a universal good within anti-corruption campaigns and reform projects that have been implemented on the African continent (see Lawson, 2009). In addition, transparency is seen as a vehicle for eradicating a bureaucratic evil, namely, politics (Hetherington, 2011). This resonates with several anthropological studies (see Bierschenk, 2008; Ferguson, 1994; Li, 2007; Mosse, 2013), that have demonstrated how development in the post-Cold-War era focused on depoliticisation, i.e., to "take political problems and render them technical and bureaucratic" (Hetherington, 2011: 7). In her evocative book on *The Will to Improve* in Indonesia, Tanya Li (2007) uses the term "rendering technical" to highlight the expertise that is used and defined in a variety of programmes and how "questions that are rendered technical are simultaneously rendered non-political" (7). Yet studies, such as Li's, have demonstrated that development projects are inherently political and create new political subjectivities. James Ferguson's (1994) classic analysis of development as an "anti-politics machine" explicitly argues that development centres on "depoliticizing everything it touches, everywhere whisking political realities out of sight, all the while perfuming, almost unnoticed, its own pre-eminently political operation of expanding bureaucratic state power" (xv). This claim has been supported by others, and scholars such as Bierschenk (2008: 10) have emphasised how African elites have politicised the "antipolitics" of aid programmes to their own advantage.

The increased focus on digitalisation is a part of this technical rendering, to use Li's (2007) words. Digitalisation is a component of the "technical game" (Rottenburg, 2009) of development and progress. Digital transformation and infrastructures are framed as specific sets of expertise that are heavily promoted and invested in by development organisations and financial institutions, such as the World Bank (see Mazzarella, 2010). According to Donovan and Park (2022: 122) the growth of techno-capitalism in Kenya has unleashed "a new style of development, defined by its careful attention to everyday practices – a modality they contrast with the clumsier, distant approaches of traditional aid". For many decades, Kenya has acted as a "donor darling": in addition to hosting UN headquarters, Kenya has received substantial financial support from the United States in the fight against terrorism (see Brass, 2016) and has developed into a regional hub for the development and aid industry (see McNamara, 2017).

Digital transformation in Kenya

Alongside this hub for humanitarian aid, Kenya has also undergone a major digital transformation. Kenya has received the status of a digital technological epicentre (see Poggiali, 2016; Moore and Smith, 2020; Ndemo and Weiss, 2017), has acquired the nickname "Silicon Savannah" (Poggiali 2016: 390), and is defined as "a central node in the global FinTech industry" (Donovan and Park 2022: 121). According to Poggiali (2016), this started in the early 2000s after the telecommunications sector was deregulated and the main wireless provider, Safaricom, was privatised. Since then, Safaricom has morphed into a major economic and political player (Breckenridge, 2019; Donovan and Park, 2022; Park, 2020). This has resulted in various state-corporate relationships and "ensured that ICT would become a major political focus" (Poggiali 2016: 391). Amidst this expansion of techno-capitalism, a range of digital systems were established, such as the well-known SMS-based money-transfer system of M-Pesa (see Kusimba, 2021; Park, 2020; Morawczynski, 2009) and the establishment of the IHub, a technological epicentre in the heart of the capital city of Nairobi. In tandem with this technological expansion in the financial and commercial sectors, various public services were also increasingly digitalised. Similar to other countries on the African continent, in Kenya elections are managed through digital systems (see Barkan, 2013; Cheeseman, Lynch, and Willis, 2018)

At the same time, alongside these technological changes, the Kenyan state also underwent a constitutional and political transformation with its new constitution of 2010. The constitution transformed day-to-day state governance, from the level of the country to the county to the municipality. Spearheaded by devolution and decentralisation, the constitution was heralded as a beacon of hope and transformation to enhance state-citizen relations (see Ghai, 2008; Kindiki and Ambani, 2005; Kanyinga, 2016). A crucial component of this was the improvement of public service delivery, and this occurred through all levels of state institutions and often with digitised systems. One example is the creation of various Huduma centres across the country to act as a "one stop shop service that provides services from a single location" and has the "aim to turn around public service delivery by providing efficient and accessible Government services at the convenience of citizens through various integrated service delivery platforms".[1] Another key dimension of Kenya's state transformation was the monitoring of the everyday conduct of state officials for better public service delivery. Article 59(4) of the constitution focused specifically on the establishment of several commissions that each also has the mandate to receive complaints from citizens against public officers, and several have the mandate to investigate such complaints, such as the Commission on Administrative Justice (CAJ).

In line with these mechanisms targeted for state institutions more broadly, there was also a key focus on transforming the state police and several bodies explicitly focused on police misconduct. As highlighted during the interviews that I conducted with various state officials working for these constitutional commissions, the state institution that receives most complaints from citizens is the state police. The state police in Kenya has been notorious for corruption, nepotism, and acting as a political instrument of control by and for the political elite (see Anderson, 2002; Akech, 2005; Auerbach, 2003; Hills, 2007; Osse, 2016). These structural changes were encapsulated within a larger police reform project that has been undergoing since the Kibaki government in 2002, where various government programmes aimed to transform the security and justice sector (Ruteere, 2011).

Police reform efforts really took shape with the establishment of the new constitution in 2010 and the National Police Service (NPS) Act of 2011. This Act entailed, among many things, transforming command structures of the police, introducing new training curricula, and implementing new community policing programmes (see Diphoorn and van Stapele, 2021; Hope, 2015; Kivoi and Mbae, 2013; Osse, 2016; Skilling, 2016). Additionally, another fundamental legislative change was the setting up of two oversight agencies to oversee police (mis)conduct. For external civilian-led oversight, the Independent Policing Oversight Act of 2011 was decreed, and an oversight agency, the Independent Policing Oversight Authority (IPOA), was established. IPOA is an independent state institution that is required to investigate police misconduct, especially deaths and serious injuries caused by the police, review the functioning of internal disciplinary process, monitor and investigate policing operations and deployments, and conduct inspections of police premises. Between 2013 and 2018, IPOA received and processed 9,878 complaints, of which 5,085 were classified for investigations, and 64 cases have come before the courts. On a global level, IPOA is regarded as highly progressive, having an extensive mandate that exceeds oversight authorities established elsewhere. For internal oversight, the Internal Affairs Unit (IAU) was set up under Section 87 of the National Police Service (NPS) Act. The IAU is responsible for handling police (mis)conduct internally and it receives and investigates complaints against police officers that come from members of public and police officers (Osse, 2016). In 2017, the unit received a total of 522 complaints (NPS, 2017) and in 2020, this increased to 1,043 (NPS, 2020). Combined, both oversight bodies have the mandate to investigate such cases and are seen as key actors in dealing with complaints against police officers (see Diphoorn, 2020).

Throughout my fieldwork, I spoke to individuals working within these diverse institutions and attended several meetings to understand how police reform was envisioned and experienced. One shared sentiment was that complaints against public officials, especially police officers, were not managed and addressed properly. This last part, i.e., the police not being targeted by these complaints, was a pressing concern considering the high levels of police and extrajudicial killings, especially in the larger urban centres. For many urban inhabitants, everyday life is marked by violence, crime, fear, and insecurity, and the police are widely considered to be implicated in all these phenomena (Omenya and Lubaale, 2012; Musoi et al., 2013; Price et al., 2016; Van Stapele, 2016; Jones, Kimari, and Ramakrishnan, 2017). Within the larger structures of social exclusion and stigmatisation, policing in these parts of the city is very often defined by corruption, criminality, and the illegal use of (lethal) force. State police officers are often regarded by residents as the prime perpetrators of violence, and this police violence has been extensively documented by numerous non-governmental organisations (KNCHR, 2008; MSJC, 2017).

To combat the prominence of police (mis)conduct, an extensive apparatus has been set up in Kenya as part of the broader political transformation project. This apparatus comprises state and non-state institutions that collect and document cases of police (mis)conduct and act as vehicles for citizens to voice complaints against police officers, and public officers more broadly. Yet most of the complaints directed against the police are insufficiently addressed. This is not only experienced as such by the complainants, but also a sentiment that is widely shared by the individuals working for these organisations, both state and non-state. Many shared their frustration that they can receive and document complaints, but that this often stops there. Complaints regularly do not end up with the right institutions, fail to enter the system properly, and essentially, are not dealt with adequately.

This failure to deal with complaints is addressed head-on by Sara Ahmed (2021) in her provocative and inspirational book, *Complaint!* Based on extensive work on complaints in universities, Ahmed analyses the power structures and hierarchies that are unearthed when analysing complaints and shows how a complaint "provides a lens, a way of seeing, noticing, attending to a problem in the effort to redress the problem" (24). She introduces the idea of a "complaint biography" to not only understand how complaints travel but to comprehend "a complaint in relation to the life of a person or group of people" (20). She further describes how "The path of a complaint, where a complaint goes, how far it goes, teaches us something about how institutions work" (6). She narrates how complaints are hard work; dealing with them is exhausting and emotionally taxing. One of the reasons lies with the numerous "blockages" (34), and the "complaints often end up being about the system" (27).

This clearly resonates with the sentiments of my interlocutors: when discussing the difficulties of managing and addressing complaints, most of the individuals working in the system, especially the state officials, focused on the system itself, particularly the manual systems. During numerous conversations, the faults of the manual systems were stressed, and there were urgent calls for more efficient mechanisms. Many stressed the need for further collaboration between the various institutions. In these conversations, these problems of the so-called system were framed as technical and logistical ones, such as the forms that were used, the distance (often physical) between organisations, the lack of expertise of officials, and so forth. As a result, digitalised systems have been implemented as technical solutions for technical problems. The digitalisation of the complaint biography, to use Ahmed's words, is thus geared towards eliminating potential blockages and simplifying the institutionalisation of a complaint. In the following section, I discuss the various digital systems that have been established in Kenya to provide more efficient, transparent, and inclusive mechanisms to address complaints against public servants, especially the state police, and to enhance public service delivery.

Digital complaint systems

The first type of digital systems are those that are established internally among organisations. Previously, all state institutions used manual systems (i.e., paper files) and in recent years, many state bodies have set up digitalised systems to manage their own record keeping and complaints. The Independent Policing Oversight Authority (IPOA), for example, prides itself on its internal system that it has created to manage cases against police misconduct.

The second type of digital systems are those between organisations and citizens, and it is increasingly common for state institutions to use online portals to establish and facilitate contact with citizens. The Internal Affairs Unit (IAU), which still uses paper files for their own investigations, invested heavily in their Anonymous Reporting Information System (ARIS), an online system set up in 2019 to allow people to file complaints against police officers anonymously. In July 2018, I attended a session organised by the Internal Affairs Unit to share the preliminary phase of the online system and to receive feedback from key partners and stakeholders. This entailed IT experts presenting the dashboard and showing the actual interface. It was interesting to see how "technical" the meeting was: the conversations primarily centred around the aesthetics of the system and technical issues, such as where to click "proceed" and which sections had to be filled in and how. Although it was stressed, at the beginning and end of the meeting, that all of this was done to ensure that police misconduct is tackled, this theme was rarely mentioned. And when police misconduct, such as corruption and intimidation, was discussed, it was done in a hypothetical manner, despite the very real impact this has on many Kenyan citizens.

The third type of digital systems are those that exist across institutions and are "referral systems" that focus on referring complaints between institutions. The main one that most of my interlocutors referred to is the Integrated Public Complaints Referral Mechanism (IPCRM), which was established in 2013 among five government institutions, namely, the Ethics and Anti-Corruption Commission (EACC), the Commission on Administrative Justice (CAJ), the Kenya National Commission on Human Rights (KNCHR), the National Cohesion and Integration Commission (NCIC), and the National Anti-Corruption Campaign Steering Committee (NACCSC), and one non-governmental organisation, Transparency International-Kenya (TI-K). In Swahili, this referral system is called *Sema! Piga Ripoti* – which translates as: Speak out! Submit your complaint! The most important part of the mechanism is the digital referral tool, which is "an internal tool that enables participating organisations to re-route complaints that are submitted to them to the body with the appropriate mandate".[2] According to the policy brief of the IPCRM, the main objective was to "strengthen partnerships between state oversight institutions in the handling, management and disposals of received complaints/reports as well as feeding back to the members of the public handling complaints" (2). In addition, specific objectives were outlined, namely, (1) facilitating "efficient and effective access to the agencies' services", (2) "establishing functional and accountable linkages" between the various agencies, and (3) creating "a reliable source of data".

Previously, referrals were managed manually, primarily in the form of formal letters that were sent between organisations and often, literally, entailed an extensive journey. One of the female interviewees working at one of the institutions estimated that previously, 70–80 percent of the complaints received had to be transferred to another institution. She described the frustration that accompanied this, i.e., spending so much time on cases that weren't meant for them. It was extremely time-consuming, and citizens experienced it as a nuisance. Furthermore, there was not a proper means of checking whether the complaint had arrived at the appropriate institution and whether this had been handled. This created space for delay and miscommunication, and Michael, one of the employees working for the Commission on Administrative Justice (CAJ), explained the following to me during an interview:

> So we used to go out into the field for advocacy and sensitization sessions, and we would conduct these "social audits" on projects that were funded by the government, such as the building of a school … While doing this, we often received complaints by people, almost always about corruption and maladministration. When we came back, we would bring these complaints to the relevant offices and distribute them … Yet often, when we would go back into the field, sometimes a year later or so, we would be told that their complaints had never been handled. So the system wasn't working … and there was no way for us to have any idea on what was happening with a complaint.

IPCRM was thus set up to enhance coordination among the different state agencies and ensure that complaints were handled in a more efficient way. It centred around state cooperation and coordination, and essentially about extending the scope and reach of the Kenyan state. For example, many state bodies did not have a physical presence (i.e., an office) in all the counties and were thus not accessible. With this new digital system, all state institutions would become accessible. For example, if the Ethics and Anti-Corruption Commission (EACC) does not have representation in one region, the complaint can be filed with another organisation that does have a physical office there, which will then be diverted to the Ethics and Anti-Corruption Commission (EACC). For many of the involved parties, it was a way of unifying state efforts and presenting a unified notion of the Kenyan state. As mentioned by an employee working for an international organisation that funded the initiative: "Eventually it's all the same, the same government".

In addition to the IPCRM, there is also the Complaints Handling and Referral Partners Network, which I discussed in the introduction. Unlike IPCRM, this is, as one described it to me, "referral without a system": complaints are referred, but not within a proper digital system. In fact, the referrals are often done by complainants themselves, who move from one organisation to the next. Interestingly, the lack of a digital system was often provided as the main clarification for why this referral system was not operating as it could be. It missed, as one of the administrators called, "the technological finesse".

Technological solutions?

The administrators and makers of the various systems described them as an advancement to address the technical problems. During our interviews, the systems were praised and initially pronounced as successes that were imperative for further progress. This was especially the case with those affiliated with IPCRM: they described how IPCRM provided a more efficient platform that allowed complaints to be managed in a much more effective manner. Yet, at the same time, when I was conducting fieldwork in 2017–2018, I also came to know that the system had apparently been down since November 2017. After operating for just over two years, the entire system could no longer be accessed by all the organisations involved. With the "server always being down!", it became more difficult to restart it.

Similarly, with the Anonymous Reporting Information System in the IAU, there was initially a lot of optimistic chatter. IAU officers talked about a "rush of complaints" that would come in once the system was up and running. Like other schemes, this revolved around an inclusivity rhetoric: many citizens were currently disconnected from the system and the Anonymous Reporting Information System would act as a bridge. Recent figures show, however, that the system has not delivered what IAU officers had anticipated. From the 1,043 complaints that the IAU received in 2020, 80 of them were received through the Anonymous Reporting Information System (a mere 7.7 percent). Furthermore, from these 80 complaints, 16 came in through the web form and 10 through the mobile-app system, while the remaining were called in or received through the SMS system (NPS, 2020).

When inquiring why the systems were not working or had not worked as anticipated, the primary and dominant response centred around the notion of technical failure: there was either a problem with the required software and its maintenance, or the personnel didn't have the adequate training to deal with the software, and so forth. IPCRM, for example, was no longer operating due to the server, and the Anonymous Reporting Information System had not yet delivered on its promises because the connection was often poor and officers were not sufficiently trained with the right amount of "technical expertise". For many, the solution to these issues was, interestingly, further technological advancement. In their most recent Annual Report, the IAU indicates that the creation of an "integrated complaints management system" is one of their objectives for 2021, and that this will act as a system to link all sections within the Unit and thereby "enable investigators fast-track" and a "timely completion of assigned tasks" (NPS, 2020: 36).

In line with the focus on technical gaps, another key focus was the lack of funding. It is crucial to emphasise that the design, implementation, and working of these systems were largely facilitated by funding from foreign donors, further attesting to the way in which global discourses and trends shape national policies. The IAU reporting system was, for example, largely supported by the United Nations Office on Drugs and Crime (UNODC) and Transparency International (NPS, 2020). Transparency International was asked to join due to their international reputation as one of the leading organisations in the field of transparency and anti-corruption. Furthermore, one government employee highlighted how it was crucial to have a non-state institution on board as an additional way of monitoring the state institutions and ensuring accountability. IPCRM was primarily financed by the German development agency (GIZ), which also had several projects that focused on strengthening public institutions within their Good Governance Programme. One of their key goals, as several of their employees explained, was to create technical solutions for some of these governance-related problems.

The financial support of these organisations made these systems possible but was also a part of the reason why they stalled. This was particularly so with IPCRM: when the server was down, financial support was needed, yet the German development agency only wanted to continue with financial support if the organisations displayed more commitment, both financially and operationally. This was, after all, one of the key problems for IPCRM: although it was discussed as a revolutionary system, many of the people involved were not committed and often experienced the system as extra work. Much of this revolved around issues of ownership and responsibility: during my interviews, it became apparent that potential users of the system often did not know which person or institution was responsible for a complaint and thus responsible for maintaining contact with the complainant. For some members, ownership lay with the institution that had the mandate to address the case, while others felt that it belonged to the institution that received the complaint to start with. Due to these differences in ideas, complaints were registered, but not adequately dealt with.

It also became evident that competition among state bodies played a key role, and that this occurred at various levels. The larger organisations often, for example, felt that they were largely driving the project and that others were not contributing. At the same time, larger organisations had more offices spread across the country and were thus in less need for a broader scope; the idea was that IPCRM largely benefited organisations that had fewer offices and thus less reach. Some organisations were described by others as lazy and not putting their part into it, while others were described as bullies and aggressive in their approach. As one of the employees of the German development agency said to me: “IPCRM is a nice project to talk about, but it is not followed by institutional commitment”. This resonated with the statement provided by one of the female state officials working for one of the smaller organisations:

> The problem with this system is not the members of the public and how we deal with them, but about how we compete with each other. It is

> this mistrust that means that I, as a state official, cannot perform my duty to serve my country.

This mistrust was echoed by several other members, who also highlighted that this is inherent to government bodies. As one of the employees stated:

> Once something is government information, it remains an endless process of seeking authority. Although things have changed now, this perspective in government is still holding on, and we are still hesitant to share and release information.

He further stressed, and this was echoed by others, that this also has to do with the nature of the information: these were complaints that often dealt with serious issues, such as human rights violations and corruption:

> These matters of investigations … they are all very sensitive and you cannot let information out just like that, this can jeopardize matters and bring issues of legal battles … For example, a false accusation of corruption … if this comes out, it can lead to a legal battle. And people can destroy evidence if it gets into the wrong hands … Because of this, there is a lot of suspicion.

Such claims of suspicion and mistrust go against the idea of the government as a unified and integrated entity, and the claim that "eventually it's all the same, the same government".

In addition to this sense of mistrust between organisations, the system actually produced more work, rather than minimised it. The result was that many institutions ended up engaging in a degree of "parallel record holding", i.e. maintaining parallel forms of record-keeping. One employee described it to me as: "The system we have here [name institution] is the mother system, and the IPCRM is something extra". Although there were many attempts to link the various systems together, here too emerged the dimension of mistrust: how could you permit those not working within the organisation to look into your system? Furthermore, organisations used different categories to compile their systems. For example, the Kenyan National Commission on Human Rights (KNCHR) had numerous categories for complaints related to human rights (civil, political, economic, social, etc.), while the IPCRM system used the generic category of "human rights". The result was that many organisations used IPCRM for receiving and referring complaints but used their own databases for their own cases. As a result, rather than eliminating potential steps of "red tape", it eventually produced more red tape. According to one of the employees of the German development agency, "IPCRM is extra work for most officers". This resonates with Hetherington's (2012: 243) reflection on Mathur's analysis of how paperwork inherently implies "a kind of labour whose only obvious end is the documents themselves".

In addition to the dimension of competition, the issue of membership was also a contested one within IPCRM. Various members felt that more NGOs should be involved, especially those focusing on human rights, while others felt that this should primarily be a government-centred initiative. According to some of the members, the limited membership of five government institutions was the problem, and this largely centred around the police. Many complaints were directed against the police, but they could not be used as both oversight bodies – IPOA and IAU – were not a part of the system. This was a contested domain. For some, IPOA was seen as an outsider – although a government body, it was seen as an ally of civil society. In contrast, IAU was seen as being "too close" to the police by some members and therefore problematic to include them (see Diphoorn, 2020). As a result, IAU and IPOA were not members and thus not linked to the system. Considering that police misconduct was identified by most participants as the most prominent and urgent issue with regards to public service delivery, it was problematic (and telling) that these two institutions were excluded from the system. This issue of membership unearths the suspicion and mistrust between and among state institutions and the problematic process to define which institutions co-constitute the state.

"A face for my case": the prominence of trust

In a rather contrasting fashion to the perceptions of the bureaucrats from my research, for many ordinary Kenyan citizens, much of this praise for digitalisation was missing, at least from the Nairobians that I spoke to during my fieldwork. Let me underline that my main interlocutors were individuals somehow involved in the broader policing reform project, such as human rights defenders, prosecutors, investigators, police officers, and victims of police violence. These were thus people who were likely to have encountered or interacted with one of the public institutions dealing with complaints and thus using one of these digitalised systems. Based on my discussions with them, I want to highlight three issues, namely, awareness of the systems, confidence in the state police, and trust.

The first is that many people are simply unaware of these systems. Despite the growth of the "dotcom generation" (Moore and Smith, 2020), where mobile phones are readily accessible and used, many Kenyans are still disconnected from digital services. Furthermore, many are unaware of the institutions behind the digitalised systems. I often asked people whether they had heard of, for example, the Commission on Administrative Justice (CAJ), and many interlocutors had not. The second is that the vast majority do not have confidence in police reform, or state transformation more broadly. As has been highlighted by scholarship conducted across the globe (see Goldsmith, 2005; Schaap, 2021; Prenzler and Den Heyer, 2016; Torrible, 2018), complaint management systems for the police, and police reform more broadly, are often directed towards enhancing police legitimacy and building relationships of trust between state police officers and citizens. As highlighted by Goldsmith, "those concerned with police reform, I shall argue, are interested largely with establishing trustworthy police agencies" (2005: 445).

In Kenya, although most people applaud the existence of organisations such as the IAU and IPOA, there is very little confidence in their work and in the notion that oversight will have an impact (see Diphoorn, van Stapele, and Kimari 2019; Osse 2016). For many citizens, filing a complaint is a waste of time and something that they are not inclined to do. In addition to the reigning fear of reporting a case of police abuse, many people do not believe in the system, i.e., have confidence that their complaint will be addressed, that the system will change, and even worse, fear that there will be repercussions. Numerous studies and surveys have shown that trust in the police in Kenya is low (see Kamau, Onyano, and Salau, 2022; Elfversson, 2024). During my fieldwork, numerous people shared with me how speaking up against the police is life-threatening, and how participating in an ongoing case by, for example, acting as a witness can act as a death sentence. Anonymous systems aim to address this fear, yet many people still fear that the system is not completely anonymous and that their identity will be known. Filing complaints – digitally or manually – is thus not a viable option for most people. This lack of confidence in the system is not a technical problem, but a deeply politicised one that cannot be fixed by technical solutions but requires a fundamental transformation of relations between citizens and police officers. The digitalised systems discussed here do have the aim to enhance trust, yet they do not address the underlying reasons for the lack of trust.

The third and perhaps most interesting dimension is that individuals who do want to file a complaint prefer to do so through a manual system. Although some did voice the benefits of an anonymous system, most people highlighted the preference for personalised contacts. This became explicitly apparent to me during the several interviews that I had with Edward, who had filed a case with the IAU. He did this on behalf of his brother, who had been unlawfully arrested and beaten in prison. Although released without charges, his brother had suffered from the injuries long after the incident. Edward had gone to the IAU to file his case because he wanted the case to be documented formally with an institution. During our conversations, he spoke rather highly of the male IAU investigator who had helped him and managed his complaint. He especially highlighted how he appreciated the personal interactions and that he had "a face for my case", i.e., a person who he could contact directly. This was, he later suggested, also due to potential future cases. Although the officer had been disciplined internally for his wrongdoings, Edward still feared potential future interactions with the police officer in question and felt reassured that there was someone at the IAU, i.e., someone he knew, whom he could contact if such a situation would arise.

This sentiment, of preferring personal contact, was echoed by several other complainants who specifically went to certain institutions, especially human rights defenders working for community-based organisations, because they trusted these individuals. With complaints in general, but especially when they deal with issues of violence and abuse, trust is crucial, and for many, this trust does not come from institutions more broadly, but from individuals working for institutions who can help them navigate this complex system of police accountability. In a context where police violence is an everyday reality and confidence in the system is shockingly low, trust is a fragile affair, and digital systems cannot overcome this structural problem. In fact, although digital systems aim to bring forth more transparency and reduce the potentiality for negative interactions, they also eliminate the possibilities to establish relationships of trust. While some studies present more optimistic analyses of how digital complaint systems enhance public trust (see Indiahono, 2021; Odeyemi and Obiyan, 2018), this research shows that digital systems further complicate trust, as the systems themselves are also framed as being untrustworthy (see Keymolen, 2023).

Concluding remarks

In this chapter, I have demonstrated the increasing digitalisation of systems that manage and handle complaints against public officials in Kenya. These systems, which range from internal mechanisms to referral systems across institutions, are based on the premise that digitalisation will result in more efficiency, transparency, and inclusivity. Yet, as has been documented elsewhere, this has not necessarily been the result. Rather, such systems have had the tendency to reproduce opacity (Mazzarella, 2006) and expose hierarchical relations among state institutions (Garson, 2006).

Furthermore, it is highly questionable whether these systems have resulted in an enhanced perception, practice, and experience of state accountability, and especially in a more efficient manner to deal with police (mis)conduct. With persisting high levels of police violence and a reigning perception that the police is untouchable, it seems that these systems have not addressed the main issue at hand, but have rather diverted their gaze. Although optimistic sentiments are still to be heard, many research participants have indicated that these systems have “failed”. Interestingly, when explaining the failure, the reasoning relies on the same technical jargon, namely, that there is a technical problem within the system. Technical solutions are thus plagued by technical problems, which is a common discourse in explaining the failure of security technologies (see Jaffe and Pilo, 2023). Combined, this diverts focus on the real problem at hand, namely, the violent structures of inequality that allow police misconduct to occur and the prominent lack of trust in both state institutions as well as police organisations. The reality is that the manual systems are not only plagued by technical problems, but they are beleaguered by a system that will not allow them to work, regardless of their nature. And in Kenya, this system is rather extensive and includes numerous state and non-state organisations that focus either specifically on police misconduct or on public service delivery more broadly. As stated by Ahmed (2021), to really understand the “life of a complaint" (20), we cannot only look at the process, but need to recognise that "a complaint, in being lodged somewhere, starts somewhere else" (20).

The failure of these complaints systems is due to broader political and social mechanisms at play, namely, a deep lack of confidence and fear towards the state police. As highlighted by Jaffe and Pilo (2023: 78), failure is not an objective state of being, but it should be approached "as a contingent outcome of ongoing, contested processes of valuation". This is also not solely a Kenyan reality. Across the globe, the notion of "techno-solutionism" has been criticised (see Jaffe and Pilo, 2023), and studies are unearthing the value of analysing the politics and subjectivities of technological advancements. By focusing on the role of digitalisation in the broader political transformation of Kenya, especially in the digitalisation of complaints systems to address public service delivery more broadly and police (mis)conduct more specifically, this chapter aims to contribute to wider discussions on digitalisation and reliance on technological advancements in the field of policing, security, bureaucracy, and statehood.

Notes

[1] From Huduma website: https://www.hudumakenya.go.ke/, accessed 4 November 2021.

[2] An online portal was also created (www.sema.go.ke), but this website was not in operation for the duration of my research project (2017–2020).

References

Ahmed, S. (2021) *Complaint!* Durham: Duke University Press.

Akech, M. (2005) 'Public Law Values and the Politics of Criminal (in)Justice: Creating a Democratic Framework for Policing in Kenya', *Oxford University Commonwealth Law Journal,* 5(2), 225–256.

Anderson, D.M. (2002) 'Vigilantes, Violence and the Politics of Public Order in Kenya', *African Affairs,* 101(405), 531–555.

Auerbach, J.N. (2003) 'Police Accountability in Kenya', *African Human Rights Law Journal,*3(2), 275–313.

Ballestero, A. (2012) 'Transparency in Triads', *Political and Legal Anthropology Review,* 35(2), 160–166.

Ballestero, A. (2018) 'Transparency', in H. Callan (ed.) *The International Encyclopaedia of Anthropology*. https://doi.org/10.1002/9781118924396.wbiea1505

Barkan, J.D. (2013) Kenya's 2013 Elections: Technology is not Democracy. *Journal of Democracy,* 24(3), 156–165.

Bear, L. and Mathur, N. (2015) 'Introduction: Remaking the Public Good: A New Anthropology of Bureaucracy', *The Cambridge Journal of Anthropology,* 33(1), 18–34.

Bierschenk, T. (2008) *Anthropology and Development. An Historizing and Localizing Approach*. Working paper 87, Department of Anthropology and African Studies, Mainz: University of Mainz.

Brass, J.N. (2016) *Allies or Adversaries: NGOs and the State in Africa*. Cambridge: Cambridge University Press.

Breckenridge, K. (2019) 'The Failure of the "Single Source of Truth about Kenyans": The NDRS, Collateral Mysteries and the Safaricom Monopoly', *African Studies,* 78(1), 91–11.

Calista, D.J. and Melitski, J. (2007) 'E-government and E-governance: Converging Constructs of Public Sector Information and Communications Technologies', *Public Administration Quarterly,* 31(1/2), 87–120.

Cheeseman, N., Lynch, G. and Willis, J. (2018) 'Digital Dilemmas: The Unintended Consequences of Election Technology', *Democratization,* 25(8), 1397–1418.

D'Agostino, M., Schwester, R., Carrizales, T. and Melitski, J. (2011) 'A Study of E-government and E-governance: An Empirical Examination of Municipal Websites', *Public Administration Quarterly,* 35(1), 3–25.

Debos, M. (2021) 'Biometrics and the Disciplining of Democracy: Technology, Electoral Politics, and Liberal Interventionism in Chad', *Democratization,* 28(8), 1406–1422.

Diphoorn, T. (2020) 'The "Pure Apples": Moral Bordering within the Kenyan Police', *Environment and Planning D: Society and Space,* 38(3), 490–509.

Diphoorn, T. and van Stapele, N. (2021) 'What is Community Policing? Divergent Agendas, Practices, and Experiences of Transforming the Police in Kenya', *Policing: A Journal of Policy and Practice,* 15(1), 399–411.

Diphoorn, T., van Stapele, N. and Kimari W. (2019) 'Policing for the Community? The Mismatch between Reform and Everyday Policing in Nairobi, Kenya', in S. Howell (ed.) *Policing the Urban Periphery in Africa: Developing Safety for the Marginal*. Pretoria: APCOF, 24–40.

Donovan, K. and Park, E. (2022) 'Algorithmic Intimacy: The Data Economy of Predatory Inclusion in Kenya', *Social Anthropology,* 30(2), 120–139.

Elfversson, E. (2024) 'Why Kenya's Urban Residents Don't Trust the Police', *African Liberty*. Available at: https://www.africanliberty.org/2024/01/22/why-kenyas-urban-residents-dont-trust-the-police/#:~:text=We%20analysed%20data%20from%20four,limited%20trust%20in%20the%20police (Accessed: 22 January 2024).

Ferguson, J. (1994) *The Anti-Politics Machine: Development, De-politicisation and Bureaucratic Power in Lesotho*. Minneapolis: University of Minnesota Press.

Garson, D. (2006) *Public Information Technology and E-Governance: Managing the Virtual State*. London: Jones and Bartlett Publishers.

Ghai, Y.P. (2008) 'Devolution: Restructuring the Kenyan State', *Journal of Eastern Africa Studies,* 2(2), 211–226

Goldsmith, A. (2005) 'Police Reform and the Problem of Trust', *Theoretical Criminology,* 9(4), 443–470.

Graeber, D. (2015) *The Utopia of Rules: on Technology, Stupidity, and the Secret Joys of Bureaucracy*. New York: Melville House.

Gupta, A. (2012) *Red Tape: Bureaucracy, Structural Violence, and Poverty in India*. Durham: Duke University Press.

Herzfeld, M. (1992) *The Social Production of Indifference: Exploring the Symbolic Roots of Western Democracy*. London: Routledge.

Hetherington, K. (2011) *Guerrilla Auditors. The Politics of Transparency in Neoliberal Paraguay*. Durham: Duke University Press.

Hetherington, K. (2012) 'Agency, Scale, and the Ethnography of Transparency', *Political and Legal Anthropology Review,* 35(2), 242–247.

Hills, A. (2007) 'Police Commissioners, Presidents and the Governance of Security', *Journal of Modern African Studies,* 45(3), 403–423.

Hoag, C. (2011) 'Assembling Partial Perspectives: Thoughts on the Anthropology of Bureaucracy', *PoLAR: Political and Legal Anthropology Review,* 34(1), 81–94.

Hobbis, S.K. and Hobbis, G. (2017) 'Voter Integrity, Trust and the Promise of Digital Technologies: Biometric Voter Registration in Solomon Islands', *Anthropological Forum,* 27(2), 114–134.

Hope, K.R. Sr. (2015) 'In Pursuit of Democratic Policing: An Analytical Review and Assessment of Police Reforms in Kenya', *International Journal of Police Science and Management,* 17(2), 91–97.

Hull, M.S. (2012) 'Documents and Bureaucracy', *Annual Review of Anthropology,* 41, 251–267.

Indiahono, D. (2021) 'Bureaucratic Reform by Building Trust in Citizens: Best Practices from Local Online Complaints', *Policy & Governance Review,* 5(2), 146–163.

Jaffe, R. and Pilo, F. (2023) 'Security Technology, Urban Prototyping, and the Politics of Failure', *Security Dialogue,* 54(1), 76–93.

Jones, P., Kimari, W. and Ramakrishnan, K. (2017) 'Only the People Can Defend This Struggle: The Politics of the Everyday, Extrajudicial Killings and Civil Society in Mathare, Kenya', *Review of African Political Economy,* 44(154), 559–576.

Kamau, P., Onyano, G. and Salau, T. (2022) 'Kenyans Cite Criminal Activity, Lack of Respect, and Corruption among Police Failings', *Afrobarometer Dispatch No. 522*. https://www.afrobarometer.org/wp-content/uploads/2022/09/AD552-Kenyans-cite-criminal-activity-and-corruption-among-police-failings-Afrobarometer-16sept22-1.pdf (Accessed on 22 January 2024).

Kanyinga, K. (2016) 'Devolution and the New Politics of Development in Kenya', *African Studies Review,* 59(3), 155–167.

Kenya National Commission on Human Rights (KNCHR) (2008) *The Cry of Blood: Report on Extra-judicial Killings and Disappearances*. Nairobi: KNCHR

Keymolen, E. (2023) 'Trustworthy Tech Companies: Talking the Talk or Walking the Walk?', *AI and Ethics,* 4(2), 1–9.

Kindiki, K. and Ambani, O. (eds.) (2005) *The Anatomy of Bomas: Selected Analyses of the 2004 Draft Constitution of Kenya*. Nairobi: Claripress.

Kivoi, D.L. and Mbae, C.G. (2013) 'The Achilles' Heel of Police Reforms in Kenya', *Social Sciences,* 2(6), 189–194.

Kleinman, A., Das, V. and Lock, M. (1997) 'Introduction', in Arthur Klienman, Veena Das and Margaret Lock (eds.) *Social Suffering*. Berkeley: University of California Press, ix–xxv.

Kusimba, S. (2021) *Reimagining Money: Kenya in the Digital Finance Revolution*. Stanford: Stanford University Press.

Lawson, L. (2009) 'The Politics of Anti-Corruption Reform in Africa', *The Journal of Modern African Studies,* 47(1), 73–100.

Levine, A. (2004) 'The Transparent Case of Virtuality 2003 APLA Student Paper Prize Winner: Runner-Up', *PoLAR: Political and Legal Anthropology Review,* 27(1), 90–113.

Li, T. (2007) *The Will to Improve: Governmentality, Development, and the Practice of Politics*. Durham: Duke University Press.

Maguire, M. (2009) 'The Birth of Biometric Security', *Anthropology Today,* 25(2), 9–14.

Mathare Social Justice Centre (2017) *Who Is Next? A* Participatory Action Research Report Against *the Normalization of Extrajudicial Killings in Mathare*. Nairobi: MSJC. Available at: http://www.matharesocialjustice.org/ who-is-next (Accessed: 18 November 2021).

Mathur, N. (2017) 'Bureaucracy', in F. Stein, S. Lazar, M. Candea, H. Diemberger, J. Robbins, A. Sanchez and T. Stasch (eds.) *The Cambridge Encyclopedia of Anthropology*. Cambridge: Cambridge University Press, 1–12.

Mazzarella, W. (2006) 'Internet X-Ray: E-Governance, Transparency, and the Politics of Immediation in India', *Public Culture,* 18(3), 473–505.

Mazzarella, W. (2010) 'Beautiful Balloon: The Digital Divide and the Charisma of New Media in India', *American Ethnologist,* 37(4), 783–804.

McNamara, J. (2017) 'Digital Media, Development, and Political Creativity - Between Utopia and Digital Disruption in Urban Nairobi', *Critical African Studies,* 9(3), 268–280.

Moore, H.L. and Smith, C. (2020) 'The Dotcom and the Digital: Time and Imagination in Kenya', *Public Culture,* 32(3), 513–538.

Morawczynski, O. (2009) 'Exploring the Usage and Impact of "Transformational" Mobile Financial Services: The Case of M-PESA in Kenya', *Journal of Eastern African Studies,* 3, 509–525.

Mosse, D. (2013) 'The Anthropology of International Development', *Annual Review of Anthropology,* 42, 227–246.

Musoi, K., Muthama, T., Waiya, N. and Kitiku J. (2013) *Nairobi Region Annual Crime Observatory Report 2011/2012.* Nairobi: Security Research and Information Centre.

National Police Service (NPS) (2017) *Internal Affairs Unit. Annual Report 2017.* Nairobi: NPS.

National Police Service (NPS) (2020) *Internal Affairs Unit. Annual Report 2020.* Nairobi: NPS.

Ndemo, B. and Weiss, T. (eds.). (2017) *Digital Kenya: An Entrepreneurial Revolution in the Making.* London: Palgrave Macmillan.

Odeyemi, T.I. and Obiyan, A. (2018) 'Digital Policing Technologies and Democratic Policing: Will the Internet, Social Media and Mobile Phone Enhance Police Accountability and Police–citizen Relations in Nigeria?', *International Journal of Police Science & Management,* 20(2), 97–108.

Odote, C. and Karuti, K. (2021) 'Election Technology, Disputes, and Political Violence in Kenya', *Journal of Asian and African Studies,* 56(3), 558–571.

Omenya, A. and Lubaale, G. (2012) *Understanding the Tipping Point of Urban Conflict: The Case of Nairobi, Kenya. Urban Tipping Point.*Working Paper No. 6, Manchester: University of Manchester.

Osse, A. (2016) 'Police Reform in Kenya: A Process of "Meddling Through"', *Policing and Society,* 26(8), 907–924.

Park, E. (2020) '"Human-ATMs": M-Pesa and the Expropriation of Affectvie Work in Safaricom's Kenya', *Africa,* 95, 1–20.

Poggiali, L. (2016) 'SEEING (FROM) DIGITAL PERIPHERIES: Technology and Transparency in Kenya's Silicon Savannah', *Cultural Anthropology,* 31(3), 387–411.

Poggiali, L. (2017) 'Digital Futures and Analogue Pasts? Citizenship and Ethnicity in Techno-Utopian Kenya', *Africa,* 87(2), 253–277.

Price, M., Albrecht, P., Colona, F., Denney, L. and Kimari, W. (eds.) (2016) *Hustling for Security: Managing Plural Security in Nairobi's Poor Urban Settlements.* The Hague: Clingendael Conflict Research Unit.

Rao, U. (2013) 'Biometric Marginality: UID and the Shaping of Homeless Identities in the City', *Economic and Political Weekly,* 48(13), 71–77.

Projecting DataPGovernmentDataPortals *y,*

Rottenburg, R. (2009) *Far-Fetched Facts. A Parable of Development Aid.* Cambridge, MA: MIT Press.

Ruteere, M. (2011) 'More than Political Tools', *African Security Review,* 20(4), 11–20.

Sananes, V. (2021) *From the Social Production of Indifference to the Digital Production of Invisibility.Experiencing the Digitalization of Bureaucracy in the Netherlands through the DigiD Interface.* Unpublished MA Thesis: Sustainable Citizenship, Department of Anthropology, Utrecht University.

Schaap, D. (2021) 'Police Trust-building Strategies. A Socio-institutional, Comparative Approach', *Policing and Society,* 31(3), 304–320.

Skilling, L. (2016) 'Community Policing in Kenya: The Application of Democratic Policing Principles', *The Police Journal: Theory, Practice and Principles,* 89(1), 3–17.

Strathern, M. (2000) 'The Tyranny of Transparency', *British Educational Research Journal,* 26(3), 309–321.

Thiel, A. (2020) 'Biometric Identification Technologies and the Ghanaian "Data Revolution"', *Journal of Modern African Studies,* 58(1), 115–136.

Torrible, C. (2018) 'Reconceptualising the Police Complaints Process as a Site of Contested Legitimacy Claims', *Policing and Society,* 28(4), 464–479.

Van Stapele, N. (2016) 'We Are Not Kenyans': Extra-Judicial Killings, Manhood, and Citizenship in Mathare, a Nairobi Ghetto', *Conflict, Security and Development,* 16(4), 301–325.

4 Surveillance with a human face

Imaginaries, debates, and resistance to facial recognition implementation among CCTV workers in Argentina

Martín Javier Urtasun

Introduction: facial recognition and its imaginaries

> There is a threshold point in urban surveillance beyond which quantitative change – the addition of devices used and areas watched – becomes qualitative change. It follows that we might not recognize the facial recognition society.
>
> (Gray, 2003: 315)

Pervasive surveillance has become a main feature of our social life, and video surveillance has played a key role both as a driver and as an emblem of this process. Originated to cope with petty crimes in English-speaking countries, and then boosted by the anti-terrorist agenda, Close Circuit Television (CCTV) has turned into a "fifth utility" taken for granted in almost every cityscape (Graham, 1999). Technological innovations and the massive increase in the production, storage, and processing of personal data have recently led to enhanced algorithmic surveillance powered by the use of artificial intelligence. The resulting next generation of Facial Recognition Systems (FRS) has developed into a global trend. In the Global South, many local governments have not hesitated to import turnkey solutions to secure and manage their urban spaces.

This chapter contributes to the situated study of global trends in surveillance by focusing on the case of Ensenada, Argentina, which is presently going through an early stage of debate and implementation. FRSs in Ensenada are still far from being established technologies in the surveillant assemblage – for the time being, their presence remains a mere imaginary. This case selection might seem odd, since most research being done in surveillance studies is usually aimed at disclosing the social effects of the most cutting-edge innovations, taking place in big cities and metropolises all over the world. However, I propose that understanding what lies behind the relative "backwardness" of Ensenada's surveillance assemblages is worth close consideration. Much existing work lacks an adequate account of the local dynamics of global surveillance trends. Surveillant workers are frequently deemed irrelevant to the analysis of new technologies, and the issue of city scale is too often overlooked. Smaller cities' surveillance devices not only vary

DOI: 10.4324/9781003412908-6

in size but also feature different power dynamics that affect the entanglement between policing, social control, and community bonds. In Ensenada, as in other similar places, FRS implementation relies on pre-existing surveillance assemblages that play a key role as mediators, in both enabling and resisting their implementation and functioning. As I show, facial recognition was already part of the surveillance capacities of CCTV in Ensenada, albeit not done algorithmically but by human recognition. I will develop this insight to address how FRS and pre-existing surveillance practices in Ensenada stage power struggles regarding who should be able to decide what is worth watching through the surveillance cameras.

I draw on ethnographic research conducted in the Municipality Operational Center (MOC) of Ensenada to approach these questions. The standpoints of camera operators, supervisors, police officers, and computer experts are considered in order to explore the "human element" at the core of an existing surveillance network. Importantly, this sheds light on the negotiations that take place during the initial phases of FRS implementation, thus avoiding the usual disregard for the local assemblages in which new devices are deployed. This idea is supported by another already well-established empirical finding: traditional CCTV heavily relies on the careful orchestration of both "human" and "nonhuman" elements that partner to form the networks that enable its daily functioning. This approach has been the flagship idea of a growing number of CCTV "control rooms" ethnographies that share a common rejection of "technical overdetermination" (Smith, 2012) and borrow analytical tools from actor-network theory (Gad and Lauritsen, 2009), especially Bruno Latour's call to "open the black boxes" and ensure symmetry in our accounts of "human and nonhuman" actions (Latour, 2008). I apply this theoretical and methodological frame to understand current tensions related to global trends in surveillance.

Surveillance has a dual nature, swinging between control and care, protection, and repression. This triggers two opposite sets of imaginaries (Lyon, 1994): on the one hand, enthusiastic discourses depict FRS as powerful but rather neutral tools that can overcome human constraints and biases and render traditional video surveillance a more accurate, fast, and impartial sorting device. On the other hand, worried commentators claim that the "facial recognition society" could leave our democracies unrecognisable (Gray, 2003), dangerously pushing societies onto an authoritarian path in which privacy, freedom, and human rights may be limited or even vanish altogether. Scholars' attempts to assess these technologies do justify some of these bleak forecasts. It has been proved that FRSs are often inaccurate, gender and racially biased, and vulnerable to "surveillance creep" from their supposedly legitimate targets to more mundane aspects of city management (Introna and Wood, 2004; Melgaco and Hildebrandt, 2013). Scholars have also pointed to the obscure nature of the technical facade that covers algorithmic surveillance, concealing the prejudices, biases, and arbitrariness embedded in the code of these "weapons of math destruction" (O'Neil, 2016). Proof of FRS's biases, specifically against dark-skinned women, has led to campaigns against their implementation,[1] with some governments directly banning their use for law enforcement purposes (INCLO, 2021), and major tech companies withdrawing their sales of FRS to police forces.[2]

Although being at the centre of ongoing controversy, FRS advocates have successfully spread the technology from massive surveillance systems in the metropolises of the world to small- and medium-sized cities' governments. Rather than assuming a uniform global trend, a Latourian approach to the study of these innovations calls for an in-depth account of the local embeddedness of each "surveillant assemblage" in which FRSs are deployed. The concept of surveillant assemblages highlights the heterogeneity, rhizomatic, and decentralised nature of the networks formed by horizontal trades of information between different surveillance actors (Haggerty and Ericson, 2000). From this theoretical standpoint, one major challenge in surveillance studies is to strike a balance between recognising global trends and paying attention to variations in the regional and local settings where they unfold (Green and Zurawski, 2015). High-resolution case studies have recently exposed the affordances involved in "assisted" rather than "automated" surveillance, which "opens a discretionary space in which agency is enacted and techno-social interactions become negotiated" (Fussey, Davies, and Innes, 2020: 341). Consequently, any particular attempt to implement an FRS will still be affected by the results of the interactions between new technologies, previous surveillance devices, and the workers that operate them.

The chapter is organised into three parts. First, I briefly frame recent national developments in FRS within Argentina's wider security and surveillance policies. This overview offers useful clues to understanding the case of Ensenada and the debates and specificities related to the naturalisation of state surveillance in Argentina. In the second part, I introduce Ensenada's video surveillance system, focusing on how images, cameras, and workers are assembled to form "electronic surveillants" (Cardoso, 2011), and why this affects the relationship between the watchers, the watched, and the community bonds they all share. Human-driven surveillance, as opposed to FRS, brings workers' personal knowledge and interpretative skills to the foreground. In Ensenada, this enables camera operators to approach surveillance as a "recognition experience". This insight into the daily functioning of "traditional" CCTV sets the stage to analyse the local imaginaries triggered by FRS. Ethical assessments on surveillance automatisation usually question the alleged effectiveness of algorithmic surveillance (does it work?), its cost–benefit equation (is it worth it?), and raise moral concerns (does it entail any prejudices or authoritarian danger?) (Macnish, 2012). Surveillance workers provide a unique perspective in the broader FRS debate because their intimate knowledge and concerns often lead to a more practical stance. The conclusions will address the power dynamics inside the surveillance assemblage: who gets to say who is who and what is worth watching? Local municipality workers or international software companies?

Surveillance trends in Argentina

> It would appear that Argentina's intelligence services and police do not possess advanced technical capabilities required to carry surveillance and there is no way that Argentina could be fairly described as 'a surveillance state'. Indeed, it should be emphasised that this is very far from being the case.
>
> (United Nations Special Rapporteur on the right to privacy, J. Cannataci, 2019)

Latin America is among the most violent regions in the world (UNODC, 2019), and crime and violence usually rank high among public issues. Regrettably, security policies devised to face these challenges have usually proved to be short-sighted and misguided, with a strong emphasis on tough-on-crime and police-centred measures that produce high imprisonment rates, regardless of the ruling party's political orientation (Sozzo, 2016). This also applies to the recent spread of mass surveillance devices in Latin American cities, a relatively delayed process in comparison to their early adoption in the Global North. CCTV advocates were successful in introducing it as an indispensable tool in the "fight against crime", overcoming possible criticism regarding burdensome public investments, little international evidence of its efficiency, and arguable risks to human rights.

Far away from concerns about international terrorism, Argentina's discourse on the introduction of CCTV differs from that of the most violent countries in the region. In the last decade, CCTV in Argentina has emerged as a political response to the "insecurity" associated with street crime perpetrated by young amateurs living in poor neighbourhoods (Pegoraro, 2001), a major public issue since the economic and political crisis in 2001 (Kessler, 2009). Local governments played a key role in this development (Galvani, Ríos, and Cañaveral, 2015). Pressed simultaneously from below by demands from the voters and from above by national authorities, city mayors aligned their security policies according to the situational crime prevention paradigm (Sozzo, 2009). Municipality Operational Centers (MOCs) have mushroomed in almost every city since 2010, from big metropolises like Buenos Aires to the medium and small cities scattered in the countryside.

As stated by Joseph Cannataci, Argentina could not fairly be described as a "surveillance state". This could be rather "disappointing" if we trace the national history of ground-breaking technical innovations like the police's use of dactylography in the late 19th century and the early implementation of unified identity documents equipped with biometric data. After a decade of expansion, there is still no public debate in Argentina about a national act to regulate "traditional" CCTV, with only a few provinces enforcing low-level regulations (Cejas and Gonzalez, 2015) that leave any further innovation in a state of anomie (Pérez Esquivel, 2021).

The introduction of artificial intelligence into surveillance has also experienced a significant delay in Argentina. Apart from some pilot schemes, the first relevant use of FRS for law enforcement was the Fugitive Facial Recognition System launched by the Autonomous City of Buenos Aires (CABA) in April 2019. The measure was announced as an attempt to bring the best technology available to improve an already fully developed video surveillance system connecting more than 10,000 cameras. A Russian search engine was selected to perform automated facial recognition of people passing by 300 designated cameras in the city subway and compare them with CONARC (Consulta Nacional de Rebeldías y Capturas), the national database of individuals with arrest warrants. The biometric data needed by the FRS to match passers-by's identities was in turn provided by the National Persons Register, the institution in charge of producing and managing national ID cards. Interestingly, most of the key elements gathered by the new device were already there given the legacy of longstanding evolutions in personal identification policies by the national government. The Federal System of Biometric Identification for Security Purposes (SIBIOS) was created in 2010 under the scope of a brand-new National Security Ministry (Abreu and Gómez Barrera, 2016). The SIBIOS biometric database holds personal information on every citizen or legal resident in the country. This was actually implemented for identity validation processes in border control, something intended to turn Argentina into an example for neighbouring countries (Santi Pereyra, 2018). Therefore, smart CCTV could rightfully be positioned as another step on this path of enlarged surveillance capacities driven by biometric devices.

The local government's announcement of the facial recognition scheme aroused great interest in the media, and soon enough, there were reports detailing the first 1,000 matches that led to the arrest of 174 alleged criminals. Yet, there were also warnings about the low accuracy rate of the system which was producing many false positives that led to individuals being wrongfully detained.[3] Further investigation also revealed the inversion of the presumption of innocence, leading to the universalisation of suspicion over the entire population, the incompatibility of the system with national constitutional guarantees, and concerns over the security of the personal data gathered and its possible market value.[4] Official data acquired by researchers showed that the system was configured to run at a 95% confidence rate, delivering poor figures of positive matches (9%) that were almost comparable to the number of false positives (4%) (Pérez Esquivel, 2021). Some commentators also underlined the fact that Buenos Aires was accepting devices that were already restricted or totally banned in several cities in European countries and the United States.[5] FRSs were being implemented under low-level regulation and with no detailed legislation and no initial legislative debate.[6] The criminal database was also a subject of debate, with organisations like Human Rights Watch arguing that children's rights were endangered by the disclosure of their personal data and exposure to biased systems that perform poorly when applied to them.[7]

Two years after its implementation, CABA's use of FRS to capture fugitives overcame the initial wave of resistance. Human rights advocates and technology experts campaigning against FRS did achieve some influence over the general debate, and complaints about flaws in the criminal database put an end to this dataset's public availability.[8] However, there are currently FRSs in at least four provinces (Salta, Mendoza, Córdoba, and Santa Fe), with many local governments explicitly voicing plans to set up their own systems in the near future.

Whether (and where) this kind of surveillance will continue to permeate urban spaces, or will rather be subject to strong regulation, is still to be decided. As an imported turnkey solution for security issues, its evolution will express global trends in the surveillance arena – one also characterised by resistance and setbacks. Europe, Canada, and the United States have recently seen heated debate over the risks involved in the use of these largely ungoverned technologies (Richardson, 2021). At the regional level, Eduardo Ferreyra has claimed that inequality, political unrest, and the authoritarian culture inherited from past dictatorships render any further deployment of devices capable of political oppression strongly inadvisable (Ferreyra, 2020). Calls like his for a ban on facial recognition echo current debates among social movements against surveillance in Brazil (Souza and Zanatta, 2021). These simultaneous global trends are mediated by their roots in earlier surveillant assemblages. It is in this respect that surveillance workers' practices and imaginaries are useful for understanding the interplay between the global and the local.

Ensenada, a place where "nothing happens"

> Nothing happens here. I mean, it does, but nothing serious. It's not like in La Plata.
>
> (MOC's supervisor. Field notes, 26/04/2017)

Ensenada has approximately 60 000 inhabitants. It is characterised by strong community bonds and a common history of union movements and industrial development. The city has been recently incorporated into the Buenos Aires Metropolitan Area – an urban sprawl that has come to include some 15 million inhabitants, approximately one-third of the country's population. This increased proximity to the so-called "*Conurbano*", the codename for a vast array of urban realities usually associated in mainstream media with poverty, underdevelopment, and crime, has strained the local assumption of Ensenada as a safe and quiet place. This makes Ensenada an interesting place to analyse the local embeddedness of surveillance assemblages and their reaction to technological innovations.

Strong links with the metropolis have been present in the city since its foundation in 1801 as an alternative port to Buenos Aires. Ensenada is located on the Río de la Plata, a wide river that has been the main route for international commerce since colonial times, and thus shipping has been one of its main activities, followed by the manufacture of exportable goods produced by meat and hide factories, a shipyard, a steel mill, and a large petrochemical hub (Ursino, 2015). Despite its proximity to La Plata City – the centre of provincial administration – there are important differences between the localities. The foundation of La Plata near Ensenada in 1889 momentarily took away Ensenada's autonomy until it was restored in 1957. Ensenada's relationship with its bigger neighbour has been one of economic and political subordination, but also competition. Due to its industrial development, Ensenada's population was shaped by a growing working class that shares a flourishing labour movement with the nearby city of Berisso, a breeding ground for both Peronist and radical left political movements.

In contrast to La Plata's sophisticated middle-class and white-collar state employees, the people of Ensenada forged social identities as industrial workers living in a small town. Even though the industrial and port activity faced harsh times during the second part of the 20th century and many jobs were lost, these political ideals persist, especially among those who were born and raised in the city and are influenced by the political strength of the local Peronism. Based on the ideas and legacy of Juan Domingo Perón, who was three times elected President of Argentina (1946, 1951, and 1973), Peronism continues to be the most influential political movement in the country. However, the lasting weight of this so-called "national-popular" movement in national politics does not imply any ideological continuity, having its leaders committed to policies ranging from the radical left to labourism, neoliberalism, and even the conservative right. Since the recovery of democratic institutions after a long period of military dictatorships in Argentina, 40 years ago, Ensenada's Peronist leaders have won every election regardless of the political alignment of the provincial and national administrations.

Mario Secco has been the mayor of Ensenada since 2003, as part of a broad Peronist and centre-left political alliance. Secco's administration has paid constant attention to social assistance, health services, and public space makeovers, supporting a public discourse that pictures Ensenada as re-entering an "age of economic autonomy and prosperity".[9]

Following national trends, the municipality created its own Citizen Security Secretary in 2009, which is in charge of supporting the Provincial Police, as well as sharing the expenses for training, equipping, and managing the local police. The Secretary's first task was the implementation of a video surveillance system, which made the most of a national fund aimed at promoting local investment in security technology. Since its creation in 2010, Ensenada's Municipality Operational Center (MOC) has experienced rapid growth and now has 200 cameras covering much of the city.

This local commitment to security is not necessarily linked with serious security issues. According to the National Crime Statistics System, Ensenada's crime rates emulate the provincial averages, recording lower figures than La Plata in robberies and other property attacks (1,000 annual reports per 100,000 inhabitants in 2014–2018, against almost 1,800 in La

Plata), but with higher figures for personal violence (rates above 1,000 victims of personal aggression per 100,000 inhabitants, twice as much as the provincial average). In any case, during my three years of ethnographic fieldwork, I found widespread agreement among MOC's officers and workers that "nothing happens in Ensenada". Whether presented as something to be proud of or as a boring feature of their daily work, they based this premise on a comparison with a perception of La Plata's relative disorder and threats to personal safety. Beyond the historical, political, and class cleavages, there are geographical reasons that sustain this comparison. Big industrial facilities mean there are only four roads through which to enter or leave the city, making most of the Ensenada district a space that is relatively isolated and easy to control. The main exceptions – some neighbourhoods next to La Plata that have a long avenue as their only border – are perceived as more dangerous and sometimes implicitly excluded from discussions of Ensenada as a whole. As many of the workers in the MOC's control room used to say, their city is "like a bubble" that still preserves some of its original village-like quality, even if it is located on the edge of a huge metropolitan area.

Exploring MOC's surveillance assemblage

If "nothing happens", what do they do at the Municipality Operational Center (MOC)? That was the initial question that guided the ethnography I conducted in Ensenada's MOC control room between 2017 and 2019 (Urtasun, 2021). My main fieldwork strategy was participant observation of the MOC's daily routines, complemented by an analysis of official documents and 20 interviews with camera operators, police officers, public servants, and other municipality staff. I present an account of the MOC's surveillance assemblage in four stages: first, I describe the "nonhuman" components of the system, giving special attention to their affordance and restrictive capacities. I then introduce "the watchers" and how they affect the functioning of CCTV. A consideration of the combination of human and nonhuman agency provides an answer to the question of what they do at the MOC, the routine, and what is being looked for. In the final part, I reflect on how personal knowledge and community bonds operate in relation to global trends in surveillance, rendering surveillance in Ensenada a personal "recognition experience".

"Nonhumans" as surveillance mediators

Control rooms are the perfect scenario to witness video surveillance in action. Ensenada's MOC concentrates the images from its cameras in a room inside the town hall, in front of the city's main square. The space is organised around eight workstations, each consisting of a computer, two screens displaying approximately 15 cameras, one swivel chair, and an assigned camera operator. They form a row separated by black panels "so [operators] don't get distracted by speaking with each other", as the Technical Director explained to me in an interview. In front of these, there are two desks. One is for the supervisor, whose work is to keep operators watching the cameras, register any relevant events that take place during the shift in a logbook, and answer emergency calls. The other is for a police officer stationed in the room, who is in charge of the link with the police forces. Six big screens hanging on the wall complete the scene, displaying images from the cameras in full size, so everybody can watch them simultaneously.

The control room is at the centre of a complex network that receives and processes lots of information. Apart from the police radio and phone calls, its main input is the constant flow of images from the cameras scattered all over the city, gathered through an optical fibreglass network, saved in massive storages, and watched live by the camera operators. Hence, once the cameras are set and the system is working, each workstation allows images and operators to meet so that the huge amount of data produced is interpreted and turned into meaningful situations and responses. Whatever these "electronic surveillants" produce – in operator's terms, "facts", situations captured by the cameras considered somehow worthy of being recorded and warned about – is the result of these two sets of agencies working together.

Video cameras are used by many people – politicians, camera sellers, and even social researchers – as a synecdoche for the whole surveillance assemblage. The MOC mostly uses 360-degree spinning "domes", capable of zooming up to 300 m. This capacity enables camera operators to get actively involved in controlling the camera, scanning the area, and looking for convenient shots. This also makes it possible to capture scenarios from devices located more than two blocks away. As such, it is difficult for pedestrians to spot cameras or be aware that they are being surveilled in specific instances. If nobody is watching a particular camera's feed – each workstation has many more cameras than any one person could simultaneously keep track of – it automatically enters "patrol mode", moving from one shot to another in a fixed sequence that goes through the most important locations – shops, banks, schools, bus stops, corners, and the like. One supervisor explained to me that this constant movement reduces the probability of "losing something big", even if no one is looking. Since images are stored for at least one month, there is always the opportunity to rewind recorded videos and find whatever went unnoticed.

Despite the apparent power of these cameras to extend the surveillant gaze, they also have some limitations. The scope of their reach implies that every time an operator chooses to focus on a particular spot, other places are left unwatched. Trees, signs, and buildings reduce visibility and expand the number of blind spots. The weather also affects visibility: rain mists up camera lenses, wind swings the devices, and bright sunlight dazzles them. Night-time produces dark, colourless images, and city lights create blurred yellow patches which glow on the screens. Cameras can also break down, either because of natural wear and tear or as a result of human attacks, especially in neighbourhoods considered "dangerous". The software itself can crash – and it frequently does – leaving some cameras frozen, out of order, or black.

The cameras cannot see everything, but they do produce a particular account of the city that features a characteristic "aesthetic of surveillance" (Kammerer, 2004). Surveillance camera images recall spies and police films in that they are soundless, shot from above, and show people who are usually unaware of the fact that they are being filmed. These features vest them with a powerful "reality effect" that makes it difficult to raise any doubt about what can be seen on the screen (Bruno, 2013). This logic is paradoxically reinforced by the poor image quality, since "the lack of clarity [that] should make their indeterminacy more apparent (…) also works, in a contradictory fashion, to lend them some measure of credibility" (Gates, 2013: 243). This sense of the cameras' "precision" is also articulated by an attitude of suspicion that enhances every detail that could suggest that something strange is going on. Surveillance aesthetics make anyone on the screens more likely to be a suspect.

Nonhumans play a very active role in shaping the local development of video surveillance systems. They enact powerful affordances that enhance human vision, but are also loaded with limitations, resistances, and interpretative frames that they impose on the scenes that fall within their line of vision. MOC's images bear the weight of reality and surveillance aesthetics: they are supposed to "tell the truth", but preferably a suspicious and incriminating one. Therefore, the whole system could be seen as a huge mediator between public places and the control room, feeding camera operators with a constant flow of images that renders a very particular account of what is happening in the city.

The human element behind the screens

The technological devices MOC workers have to deal with, as part of their daily work, are not unbiased, transparent, or failsafe; they are still powerful data sources. Workers are supposed to sit at their workstations and watch over the city, looking for possible risks and supporting police work if necessary. This "human element" is crucial since without it the system would be nothing but a blind register of senseless images. Who the camera operators are, how they experience their work, and what they actually do are, therefore, a central part of this assemblage.

The first thing to say is that monitoring is neither an attractive task nor is it well paid. As MOC's Technical Director explained, and many operators agreed, working there is an unprofitable job that has little future in terms of professionalisation or promotion. This surely impacts the workers' profile: most of the 40 camera operators were young, low-skilled workers, for whom this was their first "decent" job. As regards gender composition, most of the positions were held by women who struggled to find jobs in other areas of the local government which involve physical work supposedly more suited to men. Payment does not seem to be enough to motivate these exhausted and underpaid workers, so direct control is constantly required. Apart from the police and supervisor presence in the control room, the system itself can be used to expose each operator's performance and hold them accountable. Each camera movement is recorded and becomes proof of the professionalism of those who were in charge at the time. To some extent, cameras exert pressure on the humans that are supposed to control them, revealing the contradictory nature of a surveillance device in which nothing should go unnoticed, even if it lacks the necessary resources to achieve a real "live" coverage of all the images produced.

Most of my introductory visits to the MOC started with someone saying that "nothing happens in Ensenada". If we are looking for police chases or serious crimes, we will have to agree with them: it is quite rare to catch an offender in the act, even if we broaden our scope to mild incivilities and misdemeanours. Besides being the result of Ensenada's calm and lower crime rates, this is the likely outcome of the lack of information provided by the cameras. The displays are flooded with routine, meaningless images – simultaneous and unrelated scenes of people walking, light traffic, or empty streets, without any context or frame to interpret them. The constant flow of images exceeds the operators' capacity to watch them all, dissolving their gaze no matter how hard they try to stay focused. To cope with the data overload, they take advantage of other information sources like emergency calls and police radio, selecting where and what to watch. But even with this help, camera operators are often confronted with long periods during which nothing is interesting or clear enough to make any sense of.

A second thing to notice about camera operators is the particularly hard task they deal with. As many other CCTV studies show, boredom heavily determines the camera operator's work to the point of becoming the main feeling related to the surveillant experience (Smith, 2007). Work shifts are exhausting, stressful, and even depressing, especially when the "nothing ever happens here" assumption merges with images that represent "positive" ways of appropriating public space: people playing sports, drifting around, and enjoying a sunny day outdoors. Operators fulfil strenuous 12-hour shifts with 10-minute breaks per hour and then rest for 36 hours. This break between shifts is often not enough to ease their boredom and tiredness, but the shifts are made more bearable by a rich sociability created within each shift. Spending long hours with the same people allows operators to get to know each other very well. Rather than silent and engrossed stares at the screens, a heated conversation is the rule and usually involves the whole group, allowing some operators to spend long stretches of time without watching their cameras at all.

MOC's work environment is surprisingly relaxed and friendly. This is something that would not have caught my attention if it were not in sharp contrast with my previous research findings. Contrary to La Plata's windowed control room, which is in a commercial area under the gaze of hundreds of passers-by (Urtasun, 2016), the MOC's office remains hidden behind the walls of the town hall, on the second floor. Where La Plata's exposed CCTV control room portrays an image of transparency and accountability, it also puts its camera operators under the pressure of a near-constant gaze. By contrast, MOC's workers find their workplace very private and comfortable. Their relative privacy allows them to share the details of their lives with one another, such as political or musical preferences, gossip, and recipes, reinforcing their friendship and sense of belonging to the team. The black panels are clearly not enough to stop operators from chatting. Moreover, they often joke and use rude language to make fun of each other, showing a notorious disregard for authority.

The third significant feature of MOC's workforce is that, although they work side by side with the local police, they are civilian municipality employees who do not go through any special training, nor are required to have any previous work experience. The skills involved in monitoring the cameras are taught and learned through day-to-day practice, under the tutelage of the stationed police officers who are supposed to have the know-how related to detecting suspicious behaviours and potential offenders. The operators often demarcate this boundary between themselves and the police force through jokes and disclaimers, noting, for example, that monitoring does not tran,sform them into cops. To my surprise, most operators presented themselves as pro-government activists. They referred to themselves as "*municipales*" devoted to "Mario" (the mayor), and always "wearing green" (Ensenada's ruling party's distinctive colour), whenever there was any criticism of the city mayor's administration. For them, entering the MOC was an important part of a wider sense of belonging linking both work and political commitments. Almost every operator I interviewed claimed to have ended up there because they were "militants". They pictured their positions in the MOC as a reward for their political work and loyalty. Their political engagements with the centre-left Peronist alliance did, in turn, shape their worldview, ultimately affecting the way they exercise their role as camera watchers. Their general support for a human rights agenda and their own experiences participating in public demonstrations led, from time to time, to open conflicts with longstanding policing practices. This was particularly apparent in instances when they confronted the police officers in the control room with accusations of discriminatory or abusive police practice against youngsters from poor neighbourhoods.

What do surveillance workers look for?

The cameras are on, the operators are seated, police are radioing in, and the phone lines are working. Many things must be correctly assembled for the task of watching the city to be assumed. There is no simple definition of what this task consists of. If we are to believe public discourse and institutional frameworks on the subject, we might think of video surveillance as a mainly preventive device related to crime control and other security issues. However, the surveillance studies literature has long demonstrated that there is much more to be considered. Video surveillance systems are proven to be social sorting devices aimed at controlling deviant behaviour, excluding undesirable populations, and keeping profit-making processes running (Lyon, 2003). To do so, these systems draw on suspicion, an ungraspable but socially constructed practice built on a combination of surveillance aesthetics and the values, prejudices, and ideologies carried by camera operators. Most CCTV ethnographies show that "it was racist, sexist, fascist and classist ideas, beliefs and stereotypes, rather than behavioural forms, which largely determined where and at whom cameras were pointed", resulting in the criminalisation of young working-class males, minorities, and marginalised populations (Smith, 2012). However, there is also an undeniable "care" dimension to surveillance, related to harm prevention, risk management, and emergency response (Lyon, 1994).

My brief description of surveillance workers above may give the impression of a useless security device for a place like Ensenada, where "nothing happens", or of a large public investment dictated by electoral goals with no practical purpose, but these would be misguided conclusions to come to. As Howard Becker suggests, when we dwell on the sensation that "nothing happens", one "trick of the trade" is to suspend participants' perceptions and try to question that assumption (Becker, 2009). Talking about my previous research in La Plata, MOC workers claimed that the capital city's bigger size and population surely correlate with a larger and more advanced surveillance system. "They surely have more than a hundred camera operators," said the supervisor with respect, and the police officer added: "I once passed by their control room and covertly watched the screens: they had only four cameras per display". Although these descriptions most likely overplay the differences between the two control rooms, there is an element of truth in the comparison: in comparison to the scale of the big city, Ensenada's video surveillance system targets a small town where everybody seems to know each other. What these workers did not realise was the advantage this represented, as they were much more likely to recognise the people they were watching. This led to one of the most significant findings: community knowledge was one of Ensenada's surveillance workers' most important assets in tackling the contradiction between the superabundance of images and the lack of interpretative resources.

Community knowledge in Ensenada shapes how different types of situations are targeted as worthy surveillance objects. Ensenada's MOC responds to a broad range of surveillance rationalities, from "care" (traffic management, fires, health emergencies) to "crime control" (robberies, drug dealers, murderers, pursuits), including a large number of more common "public order" issues (drunkards, drug users, street fights, beggars, exhibitionism). Even if serious events are rare, less "important" issues constantly occur, triggering a systematic attempt to recognise those believed to be taking part. When a match is established, everyone shares the information they have in a collective effort to locate the people involved within the interpersonal networks and hierarchies they all share. Thus, whenever "nothing happens", community knowledge enables forms of recognition that support suspicion practices, detect unusual situations, and pose hypothetical risks or wrongdoings.

This "recognition experience" also applies to another range of targets for surveillance: those that may not be as relevant to care or security concerns but grab our attention because they are entertaining or funny. Camera operators use the system to play hide-and-seek games, trying to find people they know and then talk about them (What were they doing there? How were they dressed? Who were they with?). Sometimes public surveillance is used for private purposes, like filming their houses and cars or following friends and relatives down the street. Finally, some situations are interesting no matter the personal relation. That is the case when a camera catches people doing "weird", "private", or "embarrassing" things in public places. Although not as strong as that described by Cardoso (2010), operators also showed voyeuristic pleasure in looking at others.

Embedded CCTV: surveillance with a human face

> Stereotyping is not the only way of excluding people – far from it. Having more information on certain people should definitely not be equated with liking them more or taken to indicate some automatic reduction of hostility towards them.
>
> (Blokland, 2017: 101)

Community knowledge plays a vital role in the work of MOC's surveillance workers, but it certainly does not replace stereotypes as the main mechanism of social sorting. Most of the "facts" the operators establish are directly based on routine targeting of the "usual suspects", that is to say, young males from poor neighbourhoods hanging out on the street, gathered on a street corner, doing "nothing". Social stigmatisation and bureaucratic suspicion seem to work just like in bigger cities' CCTV: visual features like dress and body language are taken as cues that identify risky populations. MOC's camera operators would look for teenagers to zoom in on, searching for hints of drug or alcohol consumption, and would then follow them while they move around the city, trying to predict their future actions. Eventually, they would call the police if they thought that these youngsters were "planning to do something", no matter how poor the evidence at hand was. Inspired by surveillance aesthetics, most camera operators would also complete the image by engaging in speculative storytelling that located the scene in a bigger picture, posing hypotheses of who these people were and what they were capable of, or willing to do next. As other studies have shown, imaginary stories told by camera operators play a key role in justifying targeting practices (Smith, 2007).

The main difference between La Plata's impersonal gaze and Ensenada's closer look is that even if it is no longer a village, the city's scale results in a certain familiarity between the watchers and those being watched. The people in the camera's line of vision are almost always the same in Ensenada and the camera operators easily get to know them, either through their appearance on the screens or by sharing social relations in the world outside the control room. Thus, the work surveillance workers do is reinforced by their capacity to identify these suspects and locate them in their relevant groups and social hierarchies. The stories they build take advantage of this external knowledge that reflects a collage of police records, social media, news, anecdotes, and gossip. If the expansion of electronic surveillance devices poses a major threat to privacy, freedom, and civil rights, the situation in Ensenada also points toward the local embeddedness of surveillance in old traditional means of (informal) social control and boundary work.

Imaginaries and practical stances on surveillance futures

> The algorithms already exist, but we are missing the remaining data to make any use of them (...) As a country, we still have to further evolve and allow this information to be public for every state entity. If we share the information, it would be easy to set up a system like the one we are talking about. Cameras could use facial recognition to detect someone with an arrest warrant. It is not that complex, and we are not too far from it (...) How long will it take? I would say 15 or 20 years more. It is not a technical issue, the problem is the political work we need to undergo as a country.
>
> (MOC's former Technical Director, personal interview, 26/12/2018)

There was no FRS in Ensenada at the end of 2018 when I first asked MOC's Technical Director about the use of video analytics in the video surveillance system. My question stemmed from concerns in international surveillance studies, as well as from a curiosity informed by a Latourian approach to nonhuman agencies, so it was rather speculative ground for me. No one in the control room had ever heard of video analytics, apart from MOC's former Technical Director, whose main work was managing the network and setting up and maintaining the technological equipment. For him, the only computer expert in the Security Secretary, FRS surveillance, was something that was both imaginable and desirable for Ensenada, though not a real possibility in the near future. Rather than a result of any technological complexity, he thought the hindrances were political – distrust between national, provincial, and local governments, and a lack of social support for new surveillance measures, and privacy concerns. However, outside the MOC, most residents of Ensenada were most likely totally unaware of the mere existence of FRS when I asked MOC's former Technical Director about its possible implementation in the city.

Only six months later, the situation had completely changed. Accounts of CABA's implementation of a Russian software for FRS surveillance flooded the national media, and soon enough everyone in the control room knew how this system worked and what the criticisms and concerns about it were. Apparently, those political issues previously suggested by MOC's former Technical Director were not enough to prevent CABA's Mayor, part of the right-wing coalition that ruled the country between 2015 and 2019, from raising the stakes in security policies – or at least that was how the situation was perceived at the MOC. Whether the implementation of FRS was a smart move, and to what extent it was suitable for Ensenada, became a topic of debate among MOC's workers for a while, filling the long shifts in the control room.

I identified two different standpoints in these debates, each encapsulating possible resistance. On the one hand, MOC's Technical Directors spoke from their expertise. First, the founder of the MOC in 2010, and then his successor in early 2019, both studied computer science and previously worked for the same local internet provider. Their professional training allowed them to act as the only experts who could understand how hardware and software work, serving as spokesmen for the nonhuman elements in the surveillant assemblage. On the other hand, the police officers, supervisors, and camera operators that form the workforce of the system experienced this debate in a more impressionistic way. They might not really be capable of explaining how FRS functions, but they were eager to state their opinions based on a constant comparison with their own way of performing "traditional" surveillance.

Computer experts in command

> In my opinion, anything that allows you to use intelligence and leave human monitoring for more specific tasks … [is good] we are heading in that direction. (...) Because there is a moment in which you have so many cameras that you cannot afford more camera operators, so you need to use some sort of intelligence to cover it.
>
> (MOC's current Technical Director, personal interview, 25/10/2021)

The rapid expansion of electronic surveillance gives increased power to computer "experts" and their technological discourses inside the crime control field (Edmond and San Roque, 2013). The new algorithmic mediations relocate the legitimacy to act as a spokesperson on behalf of the entire surveillance assemblage from law enforcement officials and political authorities to programmers and network engineers. AI applied to video analysis also widens the growing power gap in surveillance footage interpretation. This is especially clear when those images turn into evidence for police and judiciary purposes, allowing the rise of a new array of supposed "experts" in video analysis whose capabilities and expertise are yet to be proven (Pérez Esquivel, 2021).

Although MOC's computer experts may not be very influential, as they mostly set up already coded systems, they still present themselves as legitimate translators and representatives of the power of algorithms. From their privileged perspective, they frame FRS debates within the wider picture of recent innovations. As MOC's former Technical Director stated in a personal interview, "here, nowadays, everything depends on algorithms", but no decision was currently being made based on them. He explained this contradiction by drawing a distinction between complex decision-making algorithms, like FRS, and other simpler agencies embedded in the basic functioning of the software, like image contrast and brightness correction. In fact, most surveillance software is coded to perform simple tasks that are supposed to be almost imperceptible, enhancing image quality without compromising the "reality effect". In this account, only more complex video analytics cross the line of decision-making, and only to assist traditional human-driven surveillance.

The main appeal of these complex forms of algorithmic surveillance is their promise to relieve pressure on the human elements of surveillance assemblages. My interviewees framed the use of "some intelligence" as a complement that could not replace surveillance workers. As discussed by scholars who point to the "assisted" rather than "automatic" nature of algorithms, FRSs still heavily rely on human settings and operation (Fussey, Davies, and Innes, 2020). MOC's sitting Technical Director agreed that despite being very effective in some aspects, there were many tasks in which "human beings are still superior to machines". He explained this with an example: "How can you know if that guy in the park is smoking tobacco or weed? We people could watch the screen and tell the difference" (Personal interview, 25/10/2021). The same applied to the evaluation of elaborate movement patterns (such as street fights), suspicious behaviour (marauding), and personal appearance ("he looks like a thief"). Video analytics can be especially effective when facing huge amounts of data, and they surely enrich the assemblage with new functionalities such as measuring the speed of cars, something no human operator could ever do, but suspicion and other interpretative skills remain at the core of surveillance, and this is something only humans can offer.

Expert discourse in Ensenada conveyed a much more moderate enthusiasm for the practical use of algorithms in surveillance. They recognised algorithms as a useful tool in particular settings but also expressed some scepticism. All things considered, according to MOC's Technical Director, the main drawback of FRS and other video analytic software was their high cost. The only use of video analytics that had been seriously considered by MOC authorities was plate recognition. This was regarded as extremely useful since plate recognition could save precious hours of manual searching every time there is a request for retrospective evidence on the circulation of a particular vehicle. No specific concern was raised in any case about possible system failures, police abuses, or threats to civil and human rights. In our interview, MOC's Technical Director argued that he did not understand why people might complain about the system: "Why is it a problem for the local government to have that information? Today, we have all already submitted all our personal data to the world, via our smartphones" (Personal interview, 25/10/2021). MOC's computer experts' perspective naturalises surveillance developments without any deeper critical thinking – they approach these devices as market commodities that have to prove themselves technically necessary before being incorporated into local surveillance assemblages.

In search of respect

> In China the cameras do everything, it is wonderful, they have all the data. Technology is meant to beat us, cameras will move by themselves and will find crime, and that's it.
>
> (Police officer. Field notes, 2/05/2019)

> It is useless, we can already recognise everyone. There is no need for costly software.
>
> (Camera operator. Field notes, 11/06/2019)

Surveillance workers embody valuable practical knowledge and personal bonds that play an important role in surveillance's daily functioning. They may be exposed to global changes in surveillance technologies and to the public discourses they trigger, but they also act as mediators for any technological innovation and have their say in the related controversies.

Police officers, supervisors, and camera operators mostly discovered FRS after CABA's pilot experience was discussed in local media. I was conducting my last weeks of fieldwork and seized the opportunity to ask for their opinions on the topic. It was the subject of a heated debate in which fascination, scepticism, and fear were expressed in equal measure. As the enthusiastic opinion held by the police officer quoted above suggests, my question sparked imagination across the control room. Camera operators added that FRS might be perfectly suited to enhance their performance in certain repetitive tasks, like retrospective searches in stored footage, a time-consuming practice that usually ended with some operators having their "eyelashes burnt" by long hours of scouring the footage. The technocratic dreams represented by China were, nonetheless, something that many of the individuals agreed was far from possible in the local context. Just like their technocratic bosses, surveillance workers balanced any positive evaluation with a lingering suspicion that these systems were likely to perform much more poorly than they were supposed to.

Critical stances were informed by media reports on false positives but also went into deeper considerations. Scholarly literature on FRS demonstrates that these systems tend to be much more efficient for verification purposes than in identification procedures, which is explained by the fact that the first setting is more controlled while the latter involves a higher number of uncontrolled variables (Melgaco and Hildebrandt, 2013: 30).

Some police officers in the control room posed the same idea, stressing that surveillance situations are always dynamic, and people would not be likely to stop and stare at the camera for long enough for them to be identified. Even in the case that a match is finally made and the operator decides to ask the police for identity control over a person suspected to have an arrest warrant, police arrival at the scene would take more than seven minutes, rendering the effort "worthless". Available data about the system's early performance in CABA confirms this notion. Police officers only succeeded in intervening in 45% of the matches made by the FRS (Pérez Esquivel, 2021).

However, these general approaches were rapidly replaced by more situated accounts of whether these systems were suited to Ensenada. Everyone in MOC agreed that their city has "no place to hide", and that was the reason for rejecting onerous surveillance technologies. Based on their own experiences as part of the surveillance assemblage, they believed that they were already successfully handling the problem of passers-by's identification. They could simply recognise people, at least someone in the control room would, just because they knew them from their personal lives and community participation. Knowing who was who in town and how to locate every situation in the right interpretative frame were their two most valuable assets. The sort of personal data gathered in this way is incomparable to that of the private or public databases that could feed an FRS. Nonetheless, it is still a powerful source of information that MOC's surveillance workers carefully exploit. For them, the real problem is the failure of the police and judiciary to properly apprehend established criminals.

Camera operator: "it is nonsense, it won't change anything. Maybe if a kid is missing, it could be used to find him more quickly. But there are known thieves that the police overlook and cannot arrest".

> Supervisor: "That is right: you could arrest them and give them to the prosecutor, but later he will let them go. They should better invest that money in education; the country is not ready for this. If you know you have an arrest warrant, you could simply avoid that area and that's it. Let's say, Buenos Aires puts cameras in the city centre – you can simply stop going there, and you will be ok."
>
> (Conversation in the control room. Field notes, 2/05/2019)

FRSs are considered useless because recognition is not perceived as a problem that needs to be fixed in Ensenada. However, apart from contesting its usefulness, surveillance workers' comparison between algorithmic recognition and their practical skills also brought about a positive, moral appraisal of their own surveillance "with a human face". The question about whether algorithmic surveillance is more pervasive and dangerous than traditional surveillance did occupy the surveillance workers, though they most usually rejected any expectation of privacy in public spaces under the assumption that "nothing is wrong if you have nothing to hide". After all, the wide scope enabled by FRS was something that surveillance workers perceived as a risky leap in surveillance power. In line with Ferreyra's concerns over the misuse of surveillance capacities for political repression, some of those in the control room claimed that "they are going to take note of whatever you do, the demonstrations you go to", and thus no one will be "free of scrutiny". Surveillance workers defended their own ways of monitoring as less invasive, more accountable, and less threatening to their fellow citizens. Contrary to human-based surveillance, algorithms were seen as unable to evaluate individuals and situations with the need for proportionality in the surveillance power applied. It is important to remember that most supervisors and camera operators identify themselves as political militants.

> The thing is that they will use it for everything, to look for people with arrest warrants but also for everyone else, just like the register they created for people who go to demonstrations. It is going to be used in demonstrations, at football fans' gatherings … Let's say you participate in a demonstration in favour of legal abortion. Now they are going to know that you support it, even if you said nothing, even if you did not post it on Facebook (…) The system is automatic, it is not just a camera that shows you a photo and then someone has to look for a match in a previously selected face list. The dome identifies people while it spins. Who knows how many faces it can recognise per second!
>
> (MOC's Supervisor. Field notes, 2/05/2019)

The leap in surveillance power raised concerns about accountability and morality in the relationship between the watchers and those surveilled. Automatisation obscures the question of who is to be held responsible for the outcomes of the surveillance, as the blurry use of "they" in surveillance workers' speech makes clear. Uneasiness was also expressed with the detachment produced by the new technological mediation. Just as other "adiaphorization processes" analysed by Bauman and Lyon, FRSs reinforce the physical and social distance between watchers and those under watch (Bauman and Lyon, 2013). These new technological layers disguise the human relationships behind the surveillance assemblage, flattening the representation of the people surveilled in terms of target groups or behavioural patterns. Researchers have argued that automated surveillance creates a distance that "removes the possibility of negotiation, subtlety and discretion from one area of human interaction", limiting operators' discretionary powers to act either in a prejudiced or a sympathetic manner (Macnish, 2012: 164–165). Ensenada's COM operators perceive themselves as part of the local community they intend to protect, and thus they defend that discretion as a reassurance of the correct use of the system. The idea of losing control to some AI was framed as a weakening of the moral bonds that legitimise their work.

Obviously, this concern could also be understood in the context of a tangible threat to surveillance workers' control over their work processes. If the system could indeed be completely automated and no one would be needed behind the screens, that would be the end of their jobs, rendering surveillance workers useless and, arguably, unemployed. However, they did not seem to be really worried about that, partly because they felt confident that the local government's commitment to maintaining their jobs would continue. What is more, they also believed that human engagement in surveillance work was not likely to disappear, even if it could further evolve into a more hybrid technological form of assisted decision-making. Even if algorithms could effectively perform identification tasks, like in CABA's attempt to catch individuals with arrest warrants, they would definitely lack the required interpretative skills to assess surveillance situations and form coherent narratives useful for policing purposes. Contrary to the political authorities that promote innovation and the experts that raise their voices about possible bias, and harm to fundamental rights, those whose daily work it is to operate the video surveillance system were sceptical about the likelihood that these algorithmic dreams would come true. The assemblage they took part in was strong enough to impose its conditions on any newcomer, and they placed their trust in their capacity to mediate technological innovation so that they would retain crucial control over the processes.

The stability of the surveillance workers' distinction between algorithmic and human recognition is bound to be tested. It is their capacity to maintain their power to mediate between the diverse affordances that form the surveillance assemblage, while retaining significant margins to exert discretion and suspicion (Fussey, Davies, and Innes, 2020) that will decide the future of surveillance in Ensenada. As with the software currently in use, algorithms could be directed to control surveillance workers' attention and level up their performance. Conversely, the interpretative skills, social bonds, and practical knowledge they have, and that cannot be easily coded or automated, are perceived as the ultimate safeguard against their redundancy in favour of FRS.

Conclusions

Studying the impact of FRS surveillance in a small city in which this global trend has not (yet) arrived might seem paradoxical. However, my research on Ensenada's surveillance assemblage proves the relevance of surveillance workers in these networks of embedded agencies that mediate (foster, but also resist) the arrival of such global trends. While the Argentinian debates on the effectiveness and dangers of facial recognition technologies have faded away, MOC's workers engage in a much more pragmatic discussion on the effectiveness, automatisation, and morality of these systems which aim to influence the reorganisation of the surveillance assemblage and their role as mediators and their mutual bonds.

The research pointed to three findings that emerge as promising directions for further research. Firstly, it highlighted the importance of city scale in the functioning of surveillance assemblages. Surely, algorithms do add a new mediating layer to local surveillance, just as the cameras did to police and communal "eyes on the street" surveillance, in Argentina, one decade ago. However, small cities like Ensenada had another sort of facial recognition in place long before FRS started to gain any sort of purchase among city planners' and surveillance workers' imaginaries. For the moment, neither computer experts nor surveillance workers believe that Ensenada needs FRS, which they see as a costly solution for a problem that they already handle sufficiently well. But Ensenada's delay in adopting the latest surveillance fashion might also be related to a competition between these two methods of recognition, in which surveillance workers could be interested in preventing possible intruders' control over how the system functions. For how long the local government will resist global trends remains to be seen – in any case, we need to better understand the complexity of locally embedded human and nonhuman agencies before risking any further assumptions on how FRS could affect existing surveillance practices and how much resistance they could face.

The second reflection to be made points to how different these two recognition methods are concerning the internal power dynamics of surveillance assemblages. It is already well known that prejudices sneak into surveillance. The question is who has the power to decide which biases are embedded in the surveillant assemblage, whether these are coded into the software or enacted by human practices. Previous studies questioned whether human operators were ceding discretion to the computer judgement brought by this assisted surveillance, thus being relegated to an intermediary role (Fussey, Davies, and Innes, 2020). FRSs introduce external biases crystallised in their code that are not only gender and racially biased, but also created by foreign companies outside local governments' control. From the standpoint of MOC workers, the software can only be configured, but not changed, and how it works is likely to remain a black box even for computer experts. It also connects with criminal and biometric databases that are the property of the national state, thus widening the array of actors taking part in the governing of the surveillance gaze. Conversely, however, recognition based on MOC's workers' skills and social bonds keeps the arbitrariness of the system in local hands. These methods not only differ from one another in how accurate they are, but also in the sort of information they collect, the kind of intervention they enable, and the scale on which they operate. Altogether, this signals a second interesting line of research: who gets to say what is worth watching, international software companies and national security actors or local municipality workers? Also, relevant here is how the reconfiguration of discretion and suspicion affects the degree to which surveillance is rendered accountable.

In the wider global context, this also poses questions on international surveillance politics and how surveillance devices are part of centre–periphery power relations. Local surveillance assemblages are neither isolated nor resistant to change, and Ensenada's MOC has global forces knocking at its door. Argentina has practically no national production of surveillance technologies. Nowadays, Chinese companies dominate traditional CCTV in the country – according to MOC's Technical Director, Hikvision and Dahua make up 70% of the local market. The naturalisation of personal data being held by big tech corporations permeates the public discourses about FRS in Argentina, with criticism tending to focus on police or political abuses rather than on the private sector.

Finally, this case study relies on some useful methodological and analytical stances. Algorithms, especially when surveillance-related, stand out as fruitful research objects for a Latourian call to open the "black boxes". However, it is equally important to remember that algorithmic innovations in the crime control field are always mediated by previous elements in the surveillance assemblage and their respective agency. This is especially the case where human-driven, traditional CCTV continues to be enclosed in rather thick and multiple layers of opacity which require close investigation to be understood even before new technological elements are introduced. Machine learning and other artificial intelligence processes may add a crucial amount of ontological obscurity, but a significant portion of this has economic, political, and social roots. In-depth research of locally embedded surveillance applications is needed to infuse critical accounts with a broader empirical understanding of how local surveillance assemblages *actually* work. An ethnographic approach to surveillance workers, their practices, and imaginaries ensures fruitful research that unpacks the nuances of surveillance.

Notes

[1] *Vox*, "Amazon's facial analysis tech often mistakes dark-skinned women for men, study shows". Available online: https://www.vox.com/the-goods/2019/1/28/18201204/amazon-facial-recognition-dark-skinned-women-mit-study

[2] *Vox*, "Big tech companies back away from selling facial recognition to police. That's progress". Available online: https://www.vox.com/recode/2020/6/10/21287194/amazon-microsoft-ibm-facial-recognition-moratorium-police

[3] *Todo Noticias*, "De un DNI mal cargado a una cara parecida: las víctimas del sistema de reconocimiento facial en Buenos Aires". Available online: https://tn.com.ar/policiales/de-un-dni-mal-cargado-una-cara-parecida-las-victimas-del-sistema-de-reconocimiento-facial-en-buenos_980528/

[4] *La Nación*, "El debate detrás del uso de las cámaras de seguridad para identificar personas". Available online: https://www.lanacion.com.ar/tecnologia/el-debate-detras-del-uso-camaras-seguridad-nid2243734/

[5] See "The U.S. Fears Live Facial Recognition. In Buenos Aires, It's a Fact of Life". Available online: https://onezero.medium.com/the-u-s-fears-live-facial-recognition-in-buenos-aires-its-a-fact-of-life-52019eff454d

[6] Via Libre Foundation, Centro de Estudios Legales y Sociales (CELS), Civil Liberties Association, Amnesty International, and other national and international organisations assigned a letter calling for a drawback in FRS implementation. Available online: https://www.cels.org.ar/web/2020/10/la-legislatura-portena-debe-rechazar

-el-uso-de-la-tecnologia-de-reconocimiento-facial-para-la-vigilancia-del-espacio-publico/

7 Human Rights Watch released an opinion note and two public letters addressed to Argentina's President and Buenos Aires Mayor. Available online: https://www.hrw.org/news/2020/10/09/argentina-child-suspects-private-data-published-online.

8 The CABA dataset had previously been regularly updated on a publicly available website.

9 See, for example, the public discourse of Susana Gonzalez, former Security Secretary of Ensenada. Available online: http://laletrachica.com.ar/nota/2749/susana_gonzalez_elogio_la_independencia_economica_de_ensenada_en_el_aniversario_de_su_autonomia/

References

Abreu, L. and Gómez Berrera, J.C. (2016) 'Mirada maquínica y vigilancia digital: reflexiones a partir del caso del nuevo DNI argentino', *Questión. Revista especializada en Periodismo y Comunicación*, 1(49), 1–15. Available at: http://sedici.unlp.edu.ar/handle/10915/52372

Bauman, S. and Lyon, D. (2013) *Vigilancia Líquida*. Barcelona: Paidós.

Becker, H. (2009) *Trucos del oficio: cómo conducir su investigación en Ciencias Sociales*. Buenos Aires: Siglo Veintiuno.

Blokland, T. (2017) *Community as Urban Practice*. Cambridge: Polity Press.

Bruno, F. (2013) *Maquinas de ver, modos de ser. Vigilancia, tecnología y subjetividad*. Porto Alegre: Sulina.

Cannataci, J. (2019) 'Statement to the Media by the United Nations Special Rapporteur on the Right to Privacy, on the Conclusion of His Official Visit to Argentina'. Available at: https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=24639&LangID=E.

Cardoso, B. (2010) *Todos os Olhos. Videovigilâncias, videovoyeurismos e (re) produção imagética na tecnologia digital*. PhD Dissertation for Cultural Anthropology by Río de Janeiro Federal University.

Cardoso, B. (2011) 'Vigilantes eletrônicos no Rio de Janeiro: agenciamentos sociotécnicos e pesquisa em tecnologia', *Configurações*, 8, 98–108. Available at: https://journals.openedition.org/configuracoes/820

Cejas, E.B. and González, C.C. (2015) 'Estado de la normativa sobre video vigilancia en Argentina y su relación con la protección de datos personales', *Simposio Argentino de Informática y Derecho*. Available at: http://sedici.unlp.edu.ar/handle/10915/55549

Edmond, G. and San Roque, M. (2013) 'Justicia's Gaze: Surveillance, Evidence and the Criminal Trial', *Surveillance & Society*, 11(3), 252–271. Available at: https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/justicia

Ferreyra, E. (2020) 'Facial Recognition in Latin America: Towards a Human Rights-based Legal Framework to Protect Public Spaces from Mass Surveillance', *Global Campus of Human Rights Policy Briefs*. Available at: https://repository.gchumanrights.org/handle/20.500.11825/1624

Fussey, P., Davies, B. and Innes, M. (2020) '"Assisted" Facial Recognition and the Reinvention of Suspicion and Discretion in Digital Policing', *British Journal of Criminology*, 61, 325–244.

Gad, C. and Lauritsen, P. (2009) 'Situated Surveillance: An Ethnographic Study of Fisheries Inspection in Denmark', *Surveillance and Society,* 7(1), 49–57.

Galvani, M., Ríos, A. and Cañaveral, L. (2015) *Seguridad, policía y gobiernos locales: e Programa Integral de Protección Ciudadana*. Buenos Aires: Clacso.

Gates, K. (2013) 'The Cultural Labor of Surveillance: Video Forensics, Computational Objectivity, and the Production of Visual Evidence', *Social Semiotics*, 23(2), 242–260.

Graham, S. (1999) 'The Eyes Have It: CCTV as the "Fifth Utility"', *Environment and Planning B: Planning and Design*, 26(5), 639–642.

Gray, M. (2003) 'Urban Surveillance and Panopticism: Will We Recognize the Facial Recognition Society?', *Surveillance & Society,* 1(3), 314–330.

Green, N. y Zurawski, N. (2015) 'Surveillance and Ethnography: Researching Surveillance as Everyday Life', *Surveillance & Society,* 13(1), 27–43.

Haggerty, K.D. and Ericson, R.V. (2000) 'The Surveillant Assemblage', *British Journal of Sociology*, 51(4), 605–622.

INCLO (2021) *In Focus. Facial Recognition Tech Stories and Rights Harms from Around the World*. International Network of Civil Liberties Organization. Available at: https://www.inclo.net/pdf/in-focus-facial-recognition-tech-stories.pdf

Introna, L. and Wood, D. (2004) 'Picturing Algorithmic Surveillance: The Politics of Facial Recognition Systems', *Surveillance & Society*, 2(2/3), 177–198.

Kammerer, D. (2004) 'Video Surveillance in Hollywood Movies', *Surveillance & Society,* 1(2/3), 464–473.

Kessler, G. (2009)*El sentimiento de inseguridad. Sociología del temor al delito*. Buenos Aires: Siglo XXI Editores.

Latour, B. (2008 [2005])*Reensamblar lo social. Una introducción a la teoría del actor-red*. Buenos Aires: Manantial.

Lyon, D. (1994) *The Electronic Eye. The Rise of Surveillance Society*. Minneapolis: University of Minnesota Press.

Lyon, D. (ed.) (2003) *Surveillance as Social Sorting. Privacy, Risk, and Digital Discrimination*. New York: Routledge.

Macnish, K. (2012) 'Unblinking Eyes: The Ethics of Automating Surveillance', *Ethics Inf Technol,* 14, 151–167.

Melgaco, L., Verfaillie, K. and Hildebrandt, M. (2013) '*CCTV and Smart CCTV Effectiveness: A Meta-level Analysis', SIAM-Security Impact Assessment Measures*. Brussels: Vrije Universiteit Brussel. Available at: https://www.researchgate.net/publication/274077700_CCTV_and_Smart_CCTV_effectiveness_a_meta-level_analysis

O'Neill, C. (2016) *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. New York: Crown.

Pegoraro, J. (2001) 'Inseguridad y violencia en el marco del control social', *Espacio Abierto*, 10(3), 349–372.

Pérez Esquivel, A. (2021) 'Desafíos de la videovigilancia automatizada', *Derecho y Ciencias Sociales*, Noviembre 2020 – Abril 2021. Nº 24. Instituto de Cultura Jurídica y Maestría en Sociología Jurídica. Facultad de Ciencias Jurídicas y Sociales. Universidad Nacional de La Plata. Argentina, 100–122. Available at: https://revistas.unlp.edu.ar/dcs/article/view/11830/10758

Richardson, R. (2021) *Facial Recognition in the Public Sector: The Policy Landscape*. German Marshall Fund of the United States. Available at: https://www.gmfus.org/sites/default/files/Richardson%20-%20Facial%20recognition.pdf

Santi Pereyra, S.E. (2018) 'Biometrics and Social Surveillance in South America: Argentina as a Regional Laboratory for Migratory Control',*Revista Mexicana de Ciencias Políticas y Sociales,* 232, 247–326. Available at: http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0185-19182018000100247

Smith, G. (2007) 'Exploring Relations between Watchers and Watched in Control(led) Systems: Strategies and Tactics', *Surveillance and Society*, Part 2, 4(4), 280–313.

Smith, G. (2012) 'Surveillance Work(ers)', in K. Bell, K. Haggerty and D. Lyon (eds.) *Routledge Handbook of Surveillance Studies*. New York: Routledge – Taylor and Francis Group, 107–116.

Souza, M. and Zanatta, R. (2021) 'The Problem of Automated Facial Recognition Technologies in Brazil: Social Countermovements and the New Frontiers of Fundamental Rights', *Latin American Human Rights Studies*, 1. Available at: https://www.revistas.ufg.br/lahrs/article/view/69423

Sozzo, M. (2009) 'Gobierno local y prevención del delito en la Argentina', *Urvio, Revista Latinoamericana de Seguridad Ciudadana*, 6, 58–73.

Sozzo, M. (comp.) (2016) *Postneoliberalismo y penalidad en América del Sur*. Buenos Aires: CLACSO.

UNODC, Global Study on Homicide 2019 (Vienna, 2019). Available at: https://www.unodc.org/documents/data-and-analysis/gsh/Booklet2.pdf

Ursino, S.V. (2015) 'Ensenada de Barragán: hacia la conformación de un imaginario urbano industrial', *Estudios del hábitat,* 13(1), 112–126.

Urtasun, M. (2016) *Vigilancia detrás de cámara.Acercamiento etnográfico a un sistema de videovigilancia*. Dissertation for a Sociology Degree by La Plata National University. Available at: http://www.memoria.fahce.unlp.edu.ar/tesis/te.1245/te.1245.pdf

Urtasun, M. (2021) *Tramas de actores y objetos detrás de cámara. Una etnografía de los vigilantes electrónicos del Municipio de Ensenada*. Dissertation for a Social Sciences PhD by La Plata National University. Available at: http://sedici.unlp.edu.ar/handle/10915/120593

Part 2

Shaping epistemology

Problematising knowledge production in law enforcement

5 Algorithmic chains of translation

Predictive policing and the need for team-based ethnography

Simon Egbert and Maximilian Heimstädt

Introduction

Around the world, police departments use crime prediction software to predict and prevent future offences. Predictive policing is just one of the many ways in which security authorities – and law enforcement agencies in particular – strive to make the future manageable by generating future-related knowledge via socio-technical means. When engaging in predictive policing, police departments do not merely generate anticipatory insights about the future, but actively shape what is to come by intervening in the present. In this chapter, we analyse predictive policing as a socio-technical process of producing and shaping crime-related futures. More precisely, we analyse predictive policing as a "chain of translation" (Latour, 1999: 70). In doing so, we trace the production of crime predictions from algorithmic programming and data input to their execution by police officers: a process that involves many epistemic translations – at different locations but often close in time. We describe predictive policing as an incremental process consisting of different stages, focusing specifically on the German place-based crime prediction software PRECOBS. Approaching this process as a "chain of translation", we show a wide (epistemic) gap that emerges between the beginning of the predictive process and its end. This gap is filled by humans and non-humans alike, in the course of a more or less seamless process, starting at the crime analysis departments of the corresponding police headquarters, and ending on the streets of predicted risk areas. Understanding predictive policing as a chain of translation enables us to analyse it as a productive socio-technical process that proceeds in contingent and, at times, non-linear ways.

This chapter draws on a research project about the implementation and use of crime prediction software that we carried out in Germany and Switzerland between 2017 and 2018. We collected qualitative data from 11 police departments, 4 of them located in Switzerland and 7 in Germany. At the time of data collection, all the departments were either already using predictive policing tools on a regular basis, running field experiments to determine whether to use and/or how to best implement such tools, or developing their own tools. In total, we conducted 62 semi-structured interviews with police officers. These officers worked in a variety of roles, including back-office work,

DOI: 10.4324/9781003412908-8

managerial work, and patrol work on the street. In addition, we conducted focused ethnographic research with officers to better understand the practical ways in which predictive policing plays out in everyday police work. We were particularly interested in how crime analysts generated and checked crime predictions. Overall, we produced 40 field protocols. Additionally, we drew on a total of 378 documents (e.g., presentation slides, manuals, guidelines) related to the implementation of predictive policing in Germany and Switzerland to complement our ethnography.

Our argument unfolds as follows: first, we characterise predictive policing as a socio-technical process and, ultimately, as a "chain of translation". In the next section, we use the German place-based crime prediction software PRECOBS and its application as an empirical example of such a chain of translation in which we isolate four main stages: crime data, algorithmic analysis, visualisation and dissemination, and patrolling. We close by reflecting on the need for team-based ethnography of predictive systems in policing and beyond.

Predictive policing as a chain of translation

Predictive policing is understood here as the application of algorithmic analysis technologies, which are intended to produce statements about (near-)future crime (cf. Perry *et al.*, 2013: 1f.; Egbert and Leese, 2021: 19). By stressing the analytic work done by algorithms, this understanding of predictive policing highlights the new type of algorithmic agency being introduced to policing through crime prediction software, since older forms of computer software – like text processing or case management software – do not intervene so independently in the knowledge work of police officers. The given understanding of predictive policing implies that we are not dealing with forecasts that convey a long-term view of the (criminal) future, as is the case with crime trends (e.g., Hanslmaier *et al.*, 2015), but with *operational* predictions that can be more or less directly translated into police measures. While crime trends may affect long-term structural changes in police work (such as the overall availability of resources), operational predictions immediately affect how police work is done within existing resource constraints. It is therefore precisely the *acceleration in knowledge generation* achieved through the new technologies of algorithmic data analysis that makes predictive policing possible as a new strategy for police forces (see also Egbert and Leese, 2021: 69–93). Finally, our framing of predictive policing here implies that predictive policing does not only consist of a technical component – the algorithmic creation of crime forecasts – but that the implementation of these forecasts in police measures must always be considered as well, since a perfect crime prediction will not have any preventive effect if the police are not able to act on this prediction in a suitable manner (e.g., because of lacking resources or oversized prediction areas) (Egbert and Leese, 2021: 3f). Predictive policing is, therefore, to be understood as a multi-dimensional, socio-technical process, in the context of which it is not only important to create forecasts that are as accurate as possible, but at least equally significant how these forecasts are brought to the streets. Observing this chain of translation in full can be achieved, as we argue at the end of this chapter, through a multi-sited, team-based ethnography of predictive policing.

It is this socio-technical as well as iterative-processual character of predictive policing that we aim to highlight in this chapter. More precisely, we propose to understand this process as a "chain of translation". The concept was developed by Bruno Latour (1999: 24ff) in the course of his anthropological study of a soil scientific field expedition in Boa Vista, Brazil, during which he observed the research practice of pedologists, geographers, and botanists, who sought to study whether the savanna was advancing into the forest or the forest was progressing into the savanna. After his ethnographic study of Roger Guillemin's scientific laboratory at the Salk Institute for Biological Studies (Latour and Woolgar, 1979), Latour again paid close attention to day-to-day scientific practices and how scientific facts come about. In doing so, he followed the scientists from Paris to the Amazon rainforest in Brazil, observing the "journey" of the scientific findings from the Brazilian forest to the Parisian laboratory and from there into a journal article. Latour describes this journey as a chain of translation (1999: 27), referring to "the work through which actors modify, displace, and translate their various and contradictory interests" (Latour, 1999: 311). This "chain of transformation" (Latour, 1999: 70) is understood as a cascading, socio-technical process, in the course of which scientific reference is constantly being modified. It is, in the words of Glaser, Pollock, and D'Adderio (2021: 17), "never a simple and clean process."

Drawing on this approach, we argue that the discursive and political circumstances of the introduction and development of crime prediction software are an essential part of predictive policing. This also makes apparent that predictive policing should be recognised first and foremost as a nation-specific phenomenon – depending on the political climate but also on the legal conditions that prevail in each case. With reference to Germany, the introduction of crime prediction software by the PRECOBS manufacturer IfmPt (Institut für musterbasierte Prognoseforschung [Institute for Pattern-Based Prediction Research]) seemed to be market-ready at just the right time: For years, the number of domestic burglaries had steadily increased, leading to an intensifying discussion on the role of police and responsible politicians in the media, turning burglaries into a tangible political problem (Egbert, 2018). In this context, the implementation of predictive policing offered the police the opportunity to indicate an awareness of the burglary problem and to associate themselves with "modernity" and "innovation" as they promised to tackle it (Egbert, 2018, 2022). In this sense, the focus of predictive policing in Germany (and also Switzerland) on domestic burglaries is closely related to political processes around the rising case numbers in this category of offence. However, this type of offence is also quite well suited to predictive policing from an analytical and technical perspective, since professional serial burglars, who are the main focus of crime prediction software (see below), show quite robust spatio-temporal patterns, which lend themselves to predictive policing (Kaufmann, Egbert, and Leese, 2019). In addition, because such a pattern can be analysed without the need to gather a lot of data and, more importantly, without the necessity to analyse person-related data, it is also a rewarding approach from a legal standpoint (cf. Singelnstein and Busch, 2020; Sommerer, 2020).

In the following section, we focus on the generation of the predictions, their dissemination within police organisations, and their implementation on the streets.

The translations of predictive policing

Understanding predictive policing as a chain of translation has two important implications: first, predictive policing is a process consisting of different stages enacted at different locations and at different times. Second, predictive policing does not end with the technical production of predictions, but also *includes* the ways in which the crime predictions are passed along and modified within police departments in order to be implemented on the streets. In this process, many epistemic modifications take place, in the course of which the information carried by the prediction constantly changes. In the following, we describe the different stages of a predictive policing process, as depicted in Figure 5.1: crime data, algorithmic analysis, visualisation and dissemination of patrols, and patrolling in predicted risk areas.

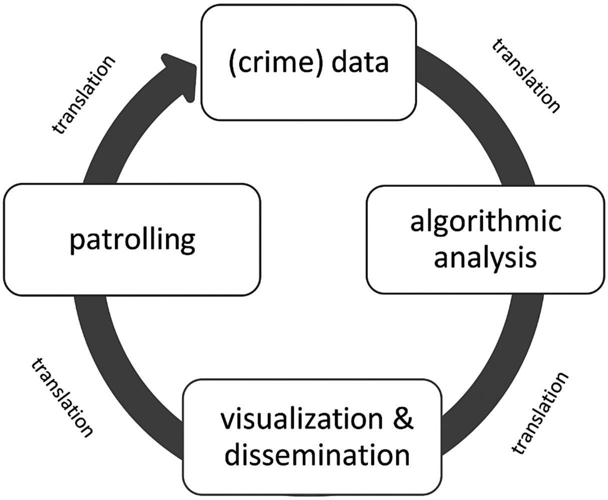


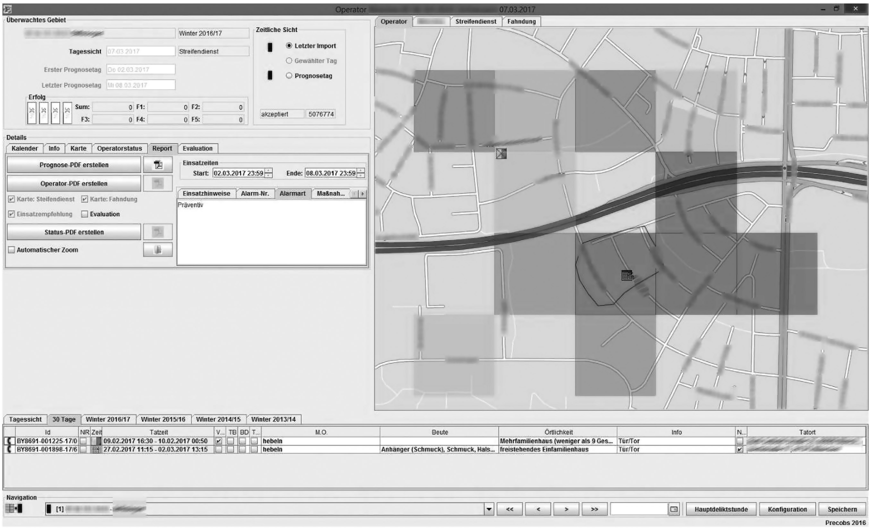
Figure 5.1 Predictive policing as a chain of translation (Egbert and Leese, 2021: 4).

Crime data

To follow the crime prediction, our journey starts before a prediction exists. One of the main epistemic components of crime predictions is the police's crime data. The police mobilise external data as well as their own data in order to generate predictions. For example, the police of North Rhine-Westphalia bought data – inter alia, concerning the socio-economic composition of residential neighbourhoods – from the geo-marketing agency Nexiga[1] for their prediction system SKALA (System zur Kriminalitätsauswertung und Lageantizipation [System for Crime Evaluation and Situation Anticipation]) (LKA NRW, 2018: 24). However, the most important source of information for the production of crime predictions in Germany is the crime data gathered by the police themselves (this is also true for Switzerland). Notably, no arrest data are used, which is important when it comes to the question of bias and feedback loop (see below), as arrest data reflect the biased control and detention practices of police officers (Lum and Isaac 2016; Egbert and Mann, 2021).

In Germany, this data refers principally to the times and places of residential burglaries, which is the main offence predicted in Germany. In most cases, no other police data are used for prediction (Egbert and Krasmann, 2019). This is directly related to the dominant theory used for predictive pattern recognition in Germany, the near-repeat theory (see below). This theory requires only a few data points, usually only concerning the type of offence that is of interest, in this case, domestic burglary. For example, this applies to the crime prediction software PRECOBS (Pre Crime Observation System), which is the only commercial crime prediction software in German-speaking countries and the model for most non-commercial crime prediction software used by police in these countries (Egbert and Leese, 2021: 7). As depicted at the bottom of Figure 5.2, which shows the PRECOBS" "operator view", the software only uses the times and locations of past burglaries, the modus operandi (how the offender gets into the residence), and information about the goods that were stolen.

However, if the underlying data are not reliable, the algorithmically generated results will not be, either. This is known in computer science as "garbage in, garbage out" and poses a huge challenge for police departments using crime prediction software, as the crime data gathered by the police is inherently biased – due to racial profiling, to name only the most obvious problem (Richardson, Schultz, and Crawford, 2019; Egbert and Mann, 2021). Nevertheless, for current predictive policing applications in Germany, bias is less of a problem because domestic burglaries are reported by victims and their reporting behaviour does not correlate with offenders' ethnic background – as it is generally not known to them. Reporting behaviour in general, however, is correlated to the socio-demographic status of the victims, with individuals from marginalised groups being less likely to report crimes to the police. This is partially because low-income households do not have relevant insurance



Operator [redacted] 07.03.2017

Überwachtes Gebiet

[redacted] | Winter 2016/17

Tagessicht: 07.03.2017 | Streifendienst

Erster Prognosetag: Do 02.03.2017

Letzter Prognosetag: Mi 08.03.2017

Erfolg

Sum: 0 F1: 0 F2: 0

F3: 0 F4: 0 F5: 0

Zeitliche Sicht

● Letzter Import

○ Gewählter Tag

○ Prognosetag

akzeptiert | 5076774

Details

Kalender | Info | Karte | Operatorstatus | Report | Evaluation

Prognose-PDF erstellen

Operator-PDF erstellen

☑ Karte: Steifendienst ☑ Karte: Fahndung

☑ Einsatzempfehlung □ Evaluation

Status-PDF erstellen

□ Automatischer Zoom

Einsatzzeiten

Start: 02.03.2017 23:59 Ende: 08.03.2017 23:59

Einsatzhinweise | Alarm-Nr. | Alarmart | Maßnah...

Präventiv

Operator | [redacted] | Streifendienst | Fahndung

Tagessicht | 30 Tage | Winter 2016/17 | Winter 2015/16 | Winter 2014/15 | Winter 2013/14

Id	NR	Zeit	Tatzeit	V...	TB	BD	T...	M.O.	Beute	Örtlichkeit	Info	N...	Tatort
BY8691-001225-17/0	□		09.02.2017 16:30 - 10.02.2017 00:50	☑	□	□	□	hebeln		Mehrfamilienhaus (weniger als 9 Ges...	Tür/Tor	□	[redacted]
BY8691-001898-17/6	□		27.02.2017 11:15 - 02.03.2017 13:15	□	□	□	□	hebeln	Anhänger (Schmuck), Schmuck, Hals...	freistehendes Einfamilienhaus	Tür/Tor	☑	[redacted]

Navigation

[1] [redacted]

Figure 5.2 PRECOBS "operator view". The map on the right is given to patrol officers. Light to dark shades of gray refer to tiles coloured blue, green, yellow, or red depending on predicted levels of risk. The table at the bottom contains the data PRECOBS analyses to estimate whether a newly registered domestic burglary was executed by a professional burglar based on place and time of offence as well as modus operandi (”M.O.”) and haul (”Beute”). Source: Screenshot by authors.

(e.g., KKV NRW, 2006). The relative completeness of data on burglaries is a consequence of insurance companies making compensation for damages conditional on providing a police report. Only when police activities directly shape the number of reported offences does racial profiling have an immediate impact on the predictions (Egbert and Mann, 2021).

Our ethnographic research of predictive policing practices shows that data quality as well as data input speed poses a challenge for police departments. The case processing systems of German police departments do not align well with the needs of crime prediction tools, which call for reliable and frequently updated data. As we will see in the next section, the near-repeat prediction pattern is an ephemeral one, demanding fast prediction work and quick patrol reaction. However, this poses a particular challenge, as the data input of police reports is less reliable the more recent it is, since some information is not available when the data are initially entered, or they are simply entered incorrectly (Egbert and Leese, 2021: 69–93). In fact, the police in Hamburg cancelled the pilot project of crime prediction software because they found that generally, their police officers were not sufficiently aware of the need for proper and fast data input, making it impossible to implement crime prediction software in a functioning manner (Hauber, Jarchow, and Rabitz-Suhr, 2019: 317ff.).

The important role of different data sources, their quality, and accessibility suggests that an ethnography of predictive policing should attend to the wider organisational processes through which input data gets assembled. These processes do not start with the software itself, but earlier, with the data entry. Our research thus points to the importance of attending to police practices *creating* the data entries that ultimately form the basis on which the crime prediction software functions. We will return to this further below and first consider the functioning of the software itself.

Algorithmic analysis

Like in the case of (crime) data, the algorithmic part of crime prediction is also relevant before a crime prediction even exists. Besides the (crime) data, the underlying prediction pattern that is "baked into" the algorithm is the second major epistemic component of predictive policing – without a pattern, there is no prediction (Kaufmann, Egbert, and Leese, 2019). To be manageable, the pattern must have a spatio-temporal context, which can be integrated into the police's day-to-day practices (see below).

As already noted, in Germany, the near-repeat prediction pattern is by far the most dominant theory informing the pattern recognition algorithms of crime prediction software (Egbert and Krasmann, 2019: 27ff.). Its main hypothesis comes from the assumption that previous victimisation is a good predictor for renewed victimisation. It follows the model of a professional serial burglar as "homo oeconomicus", acting as an "optimal forager" (Sidebottom and Wortley, 2016: 168). Rationally calculating the potential risks and earnings of a raid, professional burglars are assumed to strike again shortly after a successful burglary and in its vicinity. These follow-up offences, called near-repeats, are the target variable of most of the crime prediction software used in Germany, including PRECOBS. Ultimately, it is their aim to predict the follow-up offences for a defined spatio-temporal context (e.g., a radius of 500 m and a time span of seven days).

To accomplish this, PRECOBS uses so-called trigger and anti-trigger criteria for assessing the level of professionalism of a newly reported domestic burglary (Schweer, 2015; Balogh, 2016). In fact, the work of PRECOBS comes down to assessing whether the burglary in question was carried out by a professional or not. The near-repeat theory provides that a heightened risk can only be assumed when a professional offender was at work. More specifically, PRECOBS and similar crime prediction software are tasked with identifying burglaries that were carried out by non-professionals because non-professionals are assumed not to return according to near-repeat theory. Hence, sending patrols to the corresponding areas would be useless, or, perhaps more importantly, would be seen from an organisational viewpoint as a waste of resources.

PRECOBS uses so-called trigger and anti-trigger criteria, which indicate professional (trigger criteria) and non-professional (anti-trigger criteria) offender behaviour. As depicted at the bottom of Figure 5.2, the modus operandi ("M.O.") is assessed in order to determine (non-)professional proceedings. The possible ways of gaining unauthorised access to a flat or a house are categorised as professional and non-professional methods for this purpose. For example, drilling a window or a door to be able to open it without a key is assumed to be an expert skill, pointing to a professional offender. In contrast to this, if the police report states that a window or door was smashed with a stone, this is considered non-professional conduct, as it is noisy, something a professional offender would try to avoid. Besides the modus operandi, the stolen goods ("Beute") are also categorised as indicators for (non-) professional offender behaviour. While small and costly goods are assumed to indicate professional offenders, goods which are difficult to transport and/ or are hard to resell point to relationship crimes such as the theft of personal belongings or stealing to take revenge and, hence, non-professional offenders (Schweer, 2015; Balogh, 2016).

Two things become clear when looking at the prediction process of PRECOBS and similar crime prediction software. First, we note the relatively low technical sophistication, which is a long way from public and media images of artificial intelligence. Second, we find that crime prediction software in Germany is loaded with socially mediated criminological theories (like rational-choice theory) and expert knowledge (e.g., definition of trigger/ anti-trigger), which signals the general contingency of the corresponding predictions. In our research project, we reacted to this finding by complementing our observations of the prediction process at police stations with interviews with the developers of such software – be it from external firms or in-house developers.

Visualisation and dissemination

On our journey following a crime prediction, we are still in the police headquarters, observing the crime prediction production at the desk of the software operator. Once the software has determined whether a newly reported domestic burglary was carried out by a professional offender or not, the operator needs to decide whether this is a "meaningful decision" and whether the prediction should be sent to the responsible police station. PRECOBS and similar crime prediction software in Germany follow a semi-automated prediction process (Egbert and Leese, 2021: 98f). One reason a prediction might be declined could be that the operator knows that a serial burglar has recently been taken into custody – information the software cannot have – making the operator doubt that a near-repeat follow-up burglary could take place (Egbert and Leese, 2021: 99). In the course of the manual assessment of the prediction's reliability, and against the backdrop of the ethnically-coded narratives in police departments in Germany and Switzerland (see below), it is not unlikely that stereotypical knowledge – be it referring to burglars or to areas – will also play a role in the decision taken in the headquarters. Although our empirical data do not directly confirm this conjecture, the ethnographic study of the Dutch crime prediction software CAS (Crime Anticipation System) by Waardenburg, Huysman, and Sergeeva (2021: 10) shows that in the informational enrichment of place-based crime predictions of domestic burglaries, stereotypical knowledge of the area in question – namely referring to drug consumers ("junkies") – is used.

When it comes to the dissemination of predictions from the operator to the local police forces, it is of paramount importance to consider their visual character. The map excerpt depicted on the right in Figure 5.2 is also the visual extract given to the local police officers. The main idea is that police officers use the colour-coded map to decide where to patrol more intensively (Schweer, 2015). Following existing work on scientific representations in Science and Technology Studies (e.g., Coopmans *et al.*, 2014; Latour, 1990), the epistemic intervention of visual knowledge tools, as well as the hard and extensive work invested in the creation of corresponding images, can be considered. Like scientists, the police need to produce tables, graphs, diagrams, illustrations, and images in order to make insights from algorithmic risk calculations tangible and intelligible, in order to establish credibility for the calculated risk scores and corresponding patrol activities, and, last but not least, share insights among different specialised divisions (Egbert and Leese, 2021: 116ff). Several transformations take place in the process of making anticipated crime visible on a map. This process includes the collection and processing of burglary data from the last five years to assess the burglary intensity in an area. Only those areas where burglaries have happened often are analysed by PRECOBS (so-called "near-repeat affine areas"). These areas are more closely assessed in terms of the concrete distribution of near-repeat burglaries in the past, which is then translated into the colour-coded tiles Figure 5.2. Making use of colour perceptions deeply rooted in our culture, the red tiles demonstrate high-risk areas, which allegedly require a particularly high level of attention.

In our ethnographic research, we paid particular attention to the translations that representations of risk undergo as they are being circulated among different police divisions with specific functions and needs. Our analysis showed that as a visual risk representation began to circulate through a police organisation, it was gradually simplified and stripped of contextual information until, when it came to street-level policing, it had been transformed in such a way that police officers perceived it as a self-evident indicator for the fact that crime will happen unless it is prevented.

Patrolling

On our journey following the crime prediction through the police department, we have now arrived at our destination: the streets of the predicted risk area. As previously indicated, predictive policing is not only about producing crime predictions. A crime prediction itself has no value for the police. Rather, to have any preventive value, the forecasts must be implemented. That is, police officers have to use the predictions on the streets; otherwise, they have no effect.

In general, there are two strategies for using the predictions generated by PRECOBS and similar crime prediction software: first, a repressive approach can be applied, in the course of which surveillance forces are sent into the predicted risk areas. Dressed in civilian clothes, they can monitor the risk area and catch the perpetrator(s) in the act of committing the crime. Second, uniformed patrol forces can be deployed to patrol the predicted risk areas and deter inclined offenders through their visible presence ("focused deterrence", Ferguson, 2017: 35ff.). Since predictive policing is mainly used for cost-saving – the aim is to "do more with less" (Beck and McCue, 2009) – the second type of intervention is implemented almost exclusively. The observation of (complete) risk areas is much too resource-intensive (Egbert and Leese, 2012: 194; Pett and Gluba, 2017).

Understanding predictive policing as a chain of translation makes it mandatory to analyse closely the (mostly) preventively orientated control practices of patrol officers in the predicted risk areas. In fact, it is an open question whether risk areas are patrolled more intensively at all. In some cases, the human resources to follow up on forecasts are simply not available. This was a problem for the Saxonian police in the course of their trial of PRECOBS, leading to the decision not to adopt this software for regular operation (Fengler, 2020). Another reason for local officers not to implement a prediction can be conflicting operations in the affected areas (about which the operators of the crime prediction software have no knowledge), for example, an observation mission, which would be disturbed by (increased) police presence.

Although we were not able to participate in patrol missions in the predicted risk areas, the numerous interviews we conducted showed quite clearly that the predictions change the way the police control the affected areas and the people who are present there. The police officers who are supposed to increase patrols in a predicted risk area usually only have information about the location and size of the area to be patrolled. Their only task is to show their presence there, to dissuade potential perpetrators from their plans, who – as the assumption goes – are not willing to take the risk of arrest or conviction (Pett and Gluba, 2017). However, these patrols are also regularly used to look for suspicious incidents and, if indicated, to check people and cars. In this respect, the question of who or what is considered suspicious becomes virulent. In a way, people who happen to be in the risk area at the time the police are patrolling there tend to become the object of "ecological contamination" (Smith, 1986: 316) – the spatial risk passes on to them (Egbert, 2020; Egbert and Mann, 2021). This is in fact an ecological fallacy, as the risk attached to the area does not allow for a connection to the risk level of the people present in this area. The problem gets worse when focusing on the group of people the police regularly target in the risk areas. Police officers in the risk areas mostly look for cars and people coming from Eastern Europe (Egbert and Mann, 2021: 34; Egbert and Leese, 2021: 194) because of narratives that the expansion of the European Union to the East is a major reason for the increase in burglaries in Central Europe (see e.g., Winter, 2015) – racial profiling par excellence.

Team-based ethnography of crime prediction software

In proposing to understand predictive policing as a chain of translation, we have highlighted our understanding of predictive policing as a socio-technical and processual practice. Predictive policing consists not only of technical practices around precise and reliable predictions but also of the predictions' dissemination in police departments and their implementation by patrol officers. Understanding predictive policing as a chain of translation enables us to focus specifically on the epistemic transformations inherent in this algorithmically mediated practice and highlight its locally dispersed character. As we have shown, an analysis of predictive policing as a chain of translation is missing important parts if it does not account for the actual practices of patrol officers in the streets, implementing the predictions and making predictive policing potentially effective in the first place. Among other things, analysing control practices in risk areas shows that an understanding of predictive policing from a purely technical perspective does not capture the whole translation picture – especially when it comes to the question of discrimination and bias. In the context of place-based predictions that we have described, no personal data is used for creating the predictions. Proponents of place-based predictions therefore often claim that this form of prediction cannot be discriminatory in itself. However, our look into the concrete implementation practices makes clear that people can nevertheless (unjustifiably) become the focus of the police in the context of predictive policing.

When examining the data generated by the patrol of predicted risk areas, the chain of translation of predictive policing becomes a circle. This implies that the control practices in the risk areas have an effect on how crime numbers develop, which in turn changes the data to be processed by the predictive algorithms. From the police's point of view, that is not necessarily a bad thing because changing the data by reducing the number of domestic burglaries in the predicted areas is a key aim of predictive policing. However, this proactive policing character of predictive policing has the potential to generate self-fulfilling prophecies, more specifically a self-escalating feedback loop (O'Neil, 2016: 87; Egbert and Mann, 2021: 35f). By sending police officers into risk areas, who then – by stopping people and reporting crimes there, etc. – generate more data about this very area, predictive policing increases the possibility of future predictions in the same area. This problem does not (yet) exist in Germany, as the crime prediction software only uses data coming from the police investigation reports filed at the initiative of burglary victims.

And the likelihood of reporting a domestic burglary to the police does not correlate positively with the presence of police patrols – as the regulations of the insurance companies are influential here (see above). Therefore, as the intensified patrols do not generate a higher probability of more burglaries being reported in these areas, the probability of future predictions in affected areas will not be increased by current crime predictions. Ethnography, we argue, is especially well suited to a thorough analysis of the full chain of translation constituting the practice of predictive policing. This is even more true when approaching predictive policing as a team: a real-time, multi-sited ethnography of predictive policing allows for following a specific forecast "live" as it travels through the various stations.

We would frame this approach as a *team-based ethnography of algorithmic systems*.

For several years now, there has been a lively discussion on the role of the internet and digital technologies in ethnographic research. Initially, the focus of the debate was more on the role of the internet and its possibilities of communicating and (virtually) interacting, referred to as "virtual ethnography" (Hine, 2000), "webnography" (Strübing, 2006; translation by the authors), or "netnography" (Kozinets, 2010), but recently digital ethnographic approaches have become more prominent (e.g., Pink *et al.*, 2016). These approaches have broadened the scope of ethnographic research by not exclusively focusing on the internet, but on digital practices in general, especially smartphone use. However, what is missing in most of these accounts is a focus on the algorithmic work behind it, including the developers' interests and values written into the algorithms, as well as the effects of algorithmic affordances on users. This approach – which, following Seaver (2017) and Christin (2020) – could be called the "ethnography of algorithmic systems", is interested, on the one hand, in the work that goes into the creation and maintenance of algorithms; on the other hand, it interrogates the social consequences of algorithms on their surroundings. Seaver (2017: 1), for example, writes about tactics of an "ethnography of algorithmic systems" by focusing on algorithms as "heterogeneous and diffuse sociotechnical systems" and thus understanding them not as rigid, fixed formulas, but, following Mol's (2002) praxiography, as "part of broad patterns of meaning and practice that can be engaged with empirically" (see also Glaser, Pollock, and D'Adderio, 2021). Algorithms are not to be understood merely as cultural components, therefore, but as culture itself, which is produced situationally through culturally conditioned practices (Seaver, 2017: 4f). Against this background, following Seaver, ethnography offers itself aptly as a methodological approach because "(e)thnography is also good for seeing algorithms *as*, rather than *in* culture – for apprehending the everyday practices that constitute them and keep them working and changing" (2017: 6; emphasis in original). Additionally, Kitchin (2017: 24–26), in his overview of (critical) algorithm research, focuses on a total of six methodological approaches, two of which are explicitly ethnographically orientated: participant observation of programming teams to reconstruct the story behind the creation of an algorithm, and the study of people's practices with algorithmic systems and their effects, e.g., on organisations and how they perform and (re)structure their endeavours. Likewise, Christin (2020) highlights the suitability of ethnographic approaches for the study of algorithms given the black box character of most algorithmic systems in contemporary society – for example, due to their proprietary nature or their complex architecture (see also Pasquale, 2015; Burrell, 2016). In her words: "(E)thnographic approaches shed light on the complex intermingling of social, cultural, and technological aspects of computational systems in our daily lives. They provide rich and fine-grained data on how algorithms are built and used" (Christin, 2020: 903). In addition, she proposes making use of the sociology of enrolments, especially by following Callon (1986), thus understanding algorithms as embedded in complex and dynamic networks of human and non-human actants (Christin, 2020: 904f). Combining both approaches, Christin (2020: 906) proposes reducing the problem of algorithmic opacity by "decentering the analysis" of algorithms. That is, to focus not on the algorithmic system alone but to study the corresponding collective of human and non-human actants as a whole (see also Glaser, Pollock, and D'Adderio, 2021). In a similar vein, Lange, Lenglet, and Seyfert (2019: 606f), with reference to high-frequency trading algorithms, propose reacting to the character of algorithms as "quasi-objects" – following Serres' (1982) – since they are not collectable in a material sense, to make use of multi-sited ethnographic approaches, so enabling "different modes of interpretation of algorithms".

Building on these ethnographic accounts of algorithms, a team-based ethnography – near real-time and multi-sited – of algorithmic systems seems to be well-suited to observing the different stages of predictive policing's chain of translation. Such an ethnography of predictive policing would need to be a multi-sited ethnography (Marcus, 1995), as the crime predictions travel. And it would need to be a team-based ethnography (e.g., Jarzabkowski, Bednarek, and Cabantous, 2015), since predictions travel in (near) real time, making it impossible for a single researcher to follow a particular crime prediction from its generation in the department onto the streets, where it is implemented by patrol officers. For the implementation of predictive policing discussed in this chapter, this would mean that one ethnographer shadows the operator of the crime prediction software, closely observing the generation and assessment of the prediction. Another ethnographer attends the decision-making of local police authorities concerning the (non-)application of predictions. Yet another ethnographer attends the patrol situation in the risk area, enabling them to observe the arrival of the prediction at its final destination. This also allows for close attention to the possible feedback loop associated with crime predictions. That is the question of how police presence in the predicted risk area generates new data, which flow back into the department and affect future predictive work. This necessitates close observation of what data are entered into the police databanks, for example, by the patrol officers, and how these data are then further used for new crime predictions. In this context, the benefit of a team-based ethnography of predictive policing emerges, by allowing not only the analysis of a predictive policing chain at different locations but also the analysis of a predictive policing chain in (near) real time, as multiple ethnographers study the process in parallel.

While we focus here on the concrete implementation of crime predictions in police departments, the chain of translation constituting predictive policing can also be defined more broadly, as we have already indicated above, for example, by integrating the political and discursive contexts of such algorithms, including their role in the programming of the software. In fact, with reference to the extensive scientific work behind image-processing algorithms, Jaton (2021) illustrates the importance of starting an (ethnographic) analysis by studying the programming of the algorithms themselves – well before they are implemented on a daily basis "in the wild". However, in many cases, algorithmic chains of translation will likely contain too many sites, actors, and/or actants to be analysable in their entirety, making it necessary to focus on particular segments of the chain.

Finally, the advantages of such an approach should be contrasted with some of its disadvantages. Gaining field access is a challenging part of ethnographic research. This holds particularly true for settings like the police, where "formal secrecy" (Costas and Grey, 2014: 1424) plays an important role. In a multi-sited ethnography, researchers need to negotiate access at more than one site. A clear disadvantage is that negotiating field access for multiple sites of formal secrecy can take a very long time and bears a substantial risk of failure. Failure can occur even after having gained access, for example, when researchers get caught up in micro-political struggles between involved organisations. For example, we learnt from our previous research that oftentimes predictive policing systems are maintained by a state-level police department. This state-level department creates predictions and delivers them to municipal-level police departments. State-level departments are interested in whether municipal-level departments use the predictions or not. However, they often refrain from establishing formal evaluation procedures. We see the risk that state-level organisations try to enrol ethnographers as informants on the activities of municipal departments. In turn, municipal departments might become sceptical of the researchers, suspecting them to be informants for the state-organisation. Even in a situation of formal access, getting caught up in such a dynamic might hamper the success of the ethnographic endeavour.

Conclusion

Drawing on ethnographic fieldwork in Germany and Switzerland, we analysed predictive policing as a chain of translation (Latour, 1999). In doing so, we followed the implementation of crime prediction software within a police department to the destinations targeted by the software, highlighting both the processual and socio-technical character of this approach. In the course of our research, we placed special emphasis on the epistemic transformations, which involve examples such as the visualisation of a crime prediction for the sake of its convenient manageability by patrol officers. Based on our account of predictive policing, we ultimately proposed that the ethnographic study of predictive policing as a socially embedded chain of translation calls for a team-based approach following the multi-sited and (near-)real-time journey of crime predictions.

Note

[1] https://www.nexiga.com/ (last accessed: 16.11.2021).

References

Balogh, D.A. (2016) 'Near Repeat-Prediction mit PRECOBS bei der Stadtpolizei Zürich', *Kriminalistik,* 70, 335–341.

Beck, C. and McCue (2009) 'Predictive Policing: What Can We Learn from Wal-Mart and Amazon about Fighting Crime in a Recession?', *Police Chief,* 76(11). Available at: http://acmcst373ethics.weebly.com/uploads/2/9/6/2/29626713/police-chief-magazine.pdf (Accessed: 17 November 2021).

Burrell, J. (2016) 'How the Machine "Thinks": Understanding Opacity in Machine Learning Algorithms', *Big Data & Society,* 3(1), 1–12.

Busch, J. and Singelnstein, T. (2020) 'Rechtliche Grenzen für Predictive Policing', in F. Bode and K. Seidensticker (Hrsg.) *Predictive Policing. Eine Bestandsaufnahme für den deutschsprachigen Raum*. Frankfurt am Main: Verlag für Polizeiwissenschaft, 161–271.

Callon, M. (1986) 'Some Elements of the Sociology of Translation: Domestication of the Scallops and the Fishermen of St. Brieuc Bay', in J. Law (ed.) *Power, Action, and Belief: A New Sociology of Knowledge?* Abingdon: Routledge, 196–223.

Christin, A. (2020) 'The Ethnographer and the Algorithm: Beyond the Black Box', *Theory and Society,* 49(5–6), 897–918.

Coopmans, C., Vertesi J., Lynch, M. and Woolgar S. (eds.) (2014) *Representation in Scientific Practice Revisited*. Cambridge: MIT Press.

Costas, J. and Grey, C. (2014) 'Bringing Secrecy Into the Open: Towards a Theorization of the Social Processes of Organizational Secrecy', *Organization Studies,* 35(10), 1423–1447.

Egbert, S. (2018) 'On Security Discourses and Techno-Fixes – The Political Framing and Implementation of Predictive Policing in Germany', *European Journal for Security Research,* 3(2), 95–114.

Egbert, S. (2020) 'Predictive Policing als Treiber Rechtlicher Innovation?', *Zeitschrift für Rechtssoziologie,* 40(1–2), 26–51.

Egbert, S. (2022) 'Predictive Policing als multimodales Dispositiv', in S. Bosančić and K. Reiner (Hrsg.) *Diskurse, Dispositive und Subjektivitäten. Anwendungsfelder und Anschlussmöglichkeiten in der wissenssoziologischen Diskursforschung*. Wiesbaden: Springer VS, 273–290.

Egbert, S. and Krasmann, S. (2019) *Predictive Policing. Eine ethnographische Studie neuer Technologien zur Vorhersage von Straftaten und ihre Folgen für die polizeiliche Praxis*. Project Report. Hamburg: Universität Hamburg (Accessed: 30 April 2019).

Egbert, S. and Leese, M. (2021) *Criminal Futures. Predictive Policing and Everyday Police Work*. London/New York: Routledge.

Egbert, S. and Mann, M. (2021) 'Discrimination in Predictive Policing. The Myth of Objectivity and the Need for STS-Analysis', in V. Badalič and A. Završnik (eds.) *Automating Crime Prevention, Surveillance, and Military Operations*. Cham: Springer, 25–46.

Fengler, M. (2020)*Predictive Policing in der sächsischen Polizei – Evaluation des Tests einer Prognosesoftware zur Bekämpfung des Wohnungseinbruchdiebstahls im Raum Leipzig*. Master Thesis. Münster: German Police Academy.

Ferguson, A.G. (2017) *The Rise of Big Data Policing. Surveillance, Race, and the Future of Law Enforcement*. New York: New York University Press.

Glaser, V.L., Pollock, N. and D'Adderio, L. (2021) 'The Biography of an Algorithm: Performing algorithmic technologies in organizations', *Organization Theory,* 2(2), 1–27.

Hanslmaier, M., Kemme, S., Stoll, K. and Baier, D. (2015) 'Forecasting Crime in Germany in Times of Demographic Change', *European Journal of Criminal Policy and Research,* 21(4), 591–610.

Hauber, J., Jarchow, E. and Rabitz-Suhr, S. (2019) *Prädiktionspotenzial schwere Einbruchskriminalität – Ergebnisse einer wissenschaftlichen Befassung mit Predictive Policing*. Hamburg: LKA Hamburg.

Hine, C. (2000) *Virtual Ethnography*. London/Thousand Oaks, New Delhi: SAGE.

Jarzabkowski, P., Bednarek, R. and Cabantous, L. (2015) 'Conducting Global Team-based Ethnography: Methodological Challenges and Practical Methods', *Human Relations,* 68(1), 3–33.

Jaton, F. (2021) *The Constitution of Algorithms. Ground-Truthing, Programming, Formulating*. Cambridge: MIT Press.

Kaufmann, M., Egbert, S. and Leese, M. (2019) 'Predictive Policing and the Politics of Patterns', *The British Journal of Criminology,* 59(3), 674–692.

Kitchin, R. (2017) 'Thinking Critically about and Researching Algorithms', *Information, Communication & Society,* 20(1), 14–29.

KKV NRW (Kriminalistisch-Kriminologische Forschungsstelle Nordrhein-Westfalen) (2006) 'Das Anzeigeverhalten von Kriminalitätsopfern. Einflussfaktoren pro und contra Strafanzeige', Analyse Nr. 2/2006. Available at: https://polizei.nrw/sites/default/files/2016-11/Anzeigeverhalten.pdf (Accessed: 18 October 2022).

Kozinets, R.V. (2010) *Netnography. Doing Ethnographic Research on the Internet*. Los Angeles: SAGE.

Lange, A.C., Lenglet, M. and Seyfert, R. (2019) 'On Studying Algorithms Ethnographically: Making Sense of Objects of Ignorance', *Organization,* 26(4), 598–617.

Latour, B. (1990) 'Drawing Things Together', in M. Lynch and S. Woolgar (eds.) *Representation in Scientific Practice*. Cambridge/London: MIT Press, 19–68.

Latour, B. (1999) 'Circulating Reference. Sampling the Soil in the Amazon Forest', in B. Latour (ed.) *Pandora's Hope. Essays on the Reality of Science Studies*. Cambridge/London: Harvard University Press, 24–79.

Latour, B. and Woolgar, S. (1979) *Laboratory Life.The Social Construction of Scientific Facts*. Beverly Hills: SAGE.

LKA NRW (Landeskriminalamt Nordrhein-Westfalen [Land Office of Criminal Investigation North Rhine-Westphalia]) (2018) *Projekt SKALA. Abschlussbericht*. Düsseldorf: LKANRW. Available at: https://polizei.nrw/sites/default/files/2019-01/180821_Abschlussbericht_SKALA_0.PDF (Accessed: 16 February 2022).

Lum, K. and Isaac, W. (2016) 'To Predict and Serve?', *Significance,* 13(5), 14–19.

Marcus, G.E. (1995) 'Ethnography in/of the World System: The Emergence of Multi-Sited Ethnography', *Annual Review of Anthropology,* 24, 95–117.

Mol, A. (2002) *The Body Multiple.Ontology in Medical Practice*. Durham: Duke University Press.

O'Neil, C. (2016) *Weapons of Math Destruction. How Big Data Increases Inequality and Threatens Democracy*. London: Penguin Books.

Pasquale, F. (2015) *The Black Box Society.The Secret Algorithms that Control Money and Information*. Cambridge/London: Harvard University Press.

Perry, W.L. *et al.* (2013) *Predictive Policing. The Role of Crime Forecasting in Law Enforcement Operations*. Santa Monica: RAND.

Pett, A. and Gluba, A. (2017) 'Das Potenzial von Polizeipräsenz für Maßnahmen im Sinne des Predictive Policing', *Die Polizei,* 108(11), 323–330.

Pink, S., Horst, H.A., Postill, J., Hjorth, L., Lewis, T. and Tacchi, J. (2016) *Digital Ethnography. Principles and Practice*. Los Angeles: SAGE.

Richardson, R., Schultz, J. and Crawford, K. (2019) 'Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice', *New York University Law Review,* 94, 192–233.

Schweer, T. (2015) 'Vor dem Täter am Tatort' – Musterbasierte Tatortvorhersagen am Beispiel des Wohnungseinbruchs', *Die Kriminalpolizei,* 32, 13–16.

Seaver, N. (2017) 'Algorithms as Culture: Some Tactics for the Ethnography of Algorithmic Systems', *Big Data & Society,* 4(2), 1–12.

Serres, M. (1982) *The Parasite*. Baltimore: Johns Hopkins University Press.

Sidebottom, A. and Wortley, R. (2016) 'Environmental Criminology', in A.R. Piquero (ed.) *The Handbook of Criminological Theory*. Chichester: John Wiley & Sons, 156–181.

Smith, D.A. (1986) 'The Neighborhood Context of Police Behavior', in A.J. Reiss, Jr. and M. Tonry (eds.) *Communities and Crime*. Chicago/London: University of Chicago Press, 313–342.

Sommerer, L. (2020) *Personenbezogenes Predictive Policing.Kriminalwissenschaftli che Untersuchung über die Automatisierung der Kriminalprognose*. Baden-Baden: Nomos.

Strübing, J. (2006) 'Webnografie? Zu den methodischen Voraussetzungen einer ethnografischen Erforschung des Internets', in W. Rammert and C. Schubert (Hrsg.) *Technografie. Zur Mikrosoziologie der Technik*. Frankfurt am Main: Campus, 249–274.

Waardenburg, L., Huysman, M. and Sergeeva, A.V. (2021) 'In the Land of the Blind, the One-Eyed Man Is King: Knowledge Brokerage in the Age of Learning Algorithms', *Organization Science,* 33(1), 59–82.

Winter, M. (2015) 'Osteuropäische Einbrecherbanden auf Beutezug durch die Republik', *Kriminalistik, 69*, 572–575.

6 Mapping and the construction of criminal spaces in Delhi

Shivangi Narayan

Introduction

Existing research in Western policing contexts addresses how racialised minorities suffer from discriminatory data practices. This literature has demonstrated that the use of GIS maps in policing confirms existing social biases, especially of racialised areas being criminal (Jefferson, 2018). Maps often provide a veneer of objectivity to such conclusions (Eubanks, 2018; Benjamin, 2019). They have been conceptualised as a tool of state surveillance that reflects the cultural context of their creation (Turnbull, 1996; Scott, 1999; Ervin, 2009; Hull, 2016). This chapter extends this literature by focusing on map-making in the context of Indian policing, and shows how assumptions about caste, religion, and gender come to be represented in crime maps and feed into the continued targeting of marginalised populations by the police.[1]

This follows insights from social constructivists who contrast the assumed objectivity of technological systems, especially in the form of algorithms, with the influence of social aspects in the making and functioning of these systems (Knorr-Cetina, 2009; Berger and Luckmann, 1991). An example of this is Seaver's (2017) insistence on approaching algorithms as culturally diffused sociotechnical systems that are shaped extensively by social norms and ideas. Similarly, Bowker and Star's (1999) work on the categories underlying data collection demonstrates the political nature of categorisation rendering social groups visible or invisible. Borrowing from Latour and Woolgar's (1979) conception of maps as "inscriptive devices", I analyse the making of crime maps in Delhi and show how the end product legitimises policing processes that reinforce the control and surveillance of marginalised populations.[2]

Relying on ethnographic data collected over a period of two years (2017–2019), I present the bureaucratic, social, and technological entanglements in the production of crime maps. My research focused on hotspot mapping, as it is being used by Delhi Police to map "criminal" hotspots. My research was located in the Central Police Control Room (CPCR) of the Delhi Police Head Quarters.[3] I spent my time observing the working of four departments where the majority of the work was done for crime mapping. These included the (1) Digital Mapping Division (DMD), (2) the Dial 100 call centre, (3) Command, Control, Communication, Computing, and Intelligence (C4i), and (4) the

DOI: 10.4324/9781003412908-9

Dispatch floor and its command room. Along with supervision, the Dispatch floor is responsible for maintaining crime databases and producing a daily crime report called the Green Diary. Crime mapping in Delhi Police is done both manually and automatically. The Digital Mapping Division (henceforth the DMD) is where the mapping is done manually whilst the Crime Mapping Analytics and Prediction System (CMAPS) is responsible for automated mapping.

This chapter is divided into four sections. In the first section, I explain how ideas of certain spaces as criminal, especially those inhabited by the marginalised, play a central role in policing in Delhi. I explore how the prevalent assumption that poverty is the cause of crime influences how crime data is collected, disseminated, and analysed (Das and Chattopadhyay, 2015). Despite the existence of studies that problematise the common conflation between the poor and crime, this problematic relation endures and influences the way crime mapping is done in Delhi (De Courson and Nettle, 2021).The next section delves into some of the details that influence the production of crime maps, including how officers contend with mapping crime despite the lack of a complete address database for the city. In the third section, I attend to mapping as a digital process and consider how it is not just the input data but the entire gamut of plotting, mapping infrastructure, and the politics of mapping that work together to produce a crime map. It highlights the tensions that exist between narratives of modern technology imitating products used in the US or Europe, the manual labour that goes into working around the inadequacies of the underlying infrastructure, and an ongoing reliance on paper. The final section expands on the importance of approaching mapping as a socio-technical process, rather than a neutral technological endeavour. It explains how although histories of marginalisation and disparities in wealth and service provision are not visible on the maps, the solution is not adding more (socio-economic) data to the process of mapping. Instead, it is important to examine the meanings police associate with space and crime and problematise the association of being marginalised with being criminals. The increasing automation and opacity of mapping processes will make it more and more difficult to do this kind of intellectual and political work.

Policing the margins in New Delhi

Policing in Delhi is heavily influenced by social stereotypes about crime and the perception of certain bodies as criminal, such as those of poor persons, slum dwellers, immigrants, Dalits, or those belonging to minority religions. This is rooted in the Indian caste system where historically those living at the fringes of society were associated with deviance and non-normative lifestyles. Such fringe elements were almost always members of the lower castes or nomadic tribes. Their criminality was enshrined in sections 109–110 of the Indian Criminal Procedure Code (CrPC) where they could be put under police surveillance on the pretext of being “dangerous” and would be asked to produce "surety" (in the form of money) to prove an honest livelihood (Singha, 2015). Failure to produce this surety would result in a jail term of anywhere from six months to three years. Three such arrests or even requests for surety could make one an "habitual offender". This law was often used to arrest members of nomadic tribes and lower castes in efforts to assuage the "respectable" class's panic about rising crime or in order to use them as free labour for government projects (such as the construction of roads).[4] Still today, the criminalisation of the poor is often part of the rationale given by authorities for the clearing of irregular areas such as slums. As Gerthner (2015) shows, almost all the applications for slum removals submitted in the municipal offices in Delhi claim a safety threat to citizens living near the slum. These informal spaces are seen to break the "aesthetic" and "functional" order of the city, rendering urban spaces unsafe for other residents of the city. As others have noted, by demolishing these spaces and criminalising, arresting, torturing, or even killing their residents, the Indian state can perform security as a spectacle and assuage the fears of those in power (Khanikar, 2018; Singha, 1998, 2015; Nandi, 2016, 2019; Nigam, 1990).

These dynamics were reflected in my interactions with the police in New Delhi who see disadvantaged youth from marginalised communities as habitual offenders (Narayan, 2021). I visited a police station in the Northeast region in Delhi, an area known for its high crime rates. A police officer – an old man – sat at the "welcome desk" – told me that the area is prone to crime because children learn from their parents and others around them. Crime is what they see here, he said. According to him, children in the area lack social role models and education. This was also a prevalent opinion amongst other officers at the station. Officers in the Delhi Police HQ, including the DMD officials, routinely spoke about migrants, especially from neighbouring Bangladesh, and slum dwellers as the reason for high crime numbers in the city. The usual refrain was that people in those areas could not be trusted. Marginalised residents are policed for small infractions such as venturing out after work hours in elite areas of the city (Jamil, 2014) indicating that their labour is welcome but not them (Khanikar, 2018; Singha, 1998, 2015; Nandi, 2016, 2019; Nigam, 1990).

Statements made by high-level officials in the police also reflect this perception.[5] Reflecting on Delhi's 2019 crime statistics, the then commissioner of police stated that immigrants and youth's frustration are what lead to crime in the city. He said that the youth who live in underprivileged neighbourhoods next to affluent neighbourhoods had ambitions to get rich quickly because of what they would see in the rich neighbourhoods. According to the commissioner, "The socio-economic disparities between the rich and the poor are giving rise to criminals". In another news report,[6] the commissioner of police stated,

> There are identified clusters in all 14 districts (of Delhi) where some youths are known to indulge in criminal and anti-social behaviour.

> Division and beat staff of all these colonies should be assigned to identify antisocial youths, who have high-end motorbikes, but do not have a proper mode of income. After identifying them, staff will have to monitor their activities and nab them.

A possible explanation for these commonly held perceptions could be attributed to the lack of diversity in Delhi's police force. According to the *Status of Policing in India* report prepared by a group of Indian NGOs,[7] Delhi's police ranks 11th in terms of diversity among the 22 states that were surveyed for the report. A majority of Delhi Police's workforce belong to the neighbouring state of Haryana and often to a landowning dominant caste. A number of them join the Delhi Police because of the job's presumed "respectability" of being a government officer and its promise to give them a high social status amongst family and village kin. This is reflected in a young constable's statement who had joined the police to enhance his status: "It will improve my marriage prospects back home," he said. These dominant caste police officers attribute natural criminality to lower caste communities, those belonging to minority religions and other marginalised groups because of age-old beliefs regarding caste status and criminal inclinations of people (Narayan, 2021). These beliefs have resulted in a history of discrimination and abuse of the said population.

However, with the police being the only arm of government that is accessible to the poor and the marginalised in the city, the relationship between them and the police is complicated: Many calls at the Dial 100 call centre do originate from areas traditionally considered "unsafe" or "crime prone" areas of Delhi. These are areas in which lower caste communities, immigrants, and especially Dalits and Adivasis often reside. But the high numbers of calls should not be taken as proof of high crime in these areas. Rather, it is indicative of the police's emergency response system as the only part of the state that the residents of slums or shanty colonies can easily access. This is because the Dial 100 system is designed to respond to *any* call-in-distress. Therefore, residents from these colonies summon the police in any situation where they experience distress, even when they know that the police may not always take their side. This also often contributes to high volumes of calls from these areas.

At the same time, officers are dismissive of residents' concerns. Officers in the DMD claim that the residents of slums or unauthorised residential areas call the emergency helpline because the calls are free of charge. One officer claimed that the daily call burden of anywhere between 5,000 to 20,000 calls would be halved if the calls became chargeable. There was a prevalent assumption that callers would exaggerate their problems to gain police attention because the police are only interested in pursuing urgent cases, given their high workload.[8] For example, an officer questioned a caller's claim that he had lost ₹ 5,000. He told me it was hard to believe that people from "those areas" would have so much cash with them.

Call-ins by women are another way in which crime statistics in poor areas are inflated. Khanikar (2018) highlights that the abusive relationship between the police and slum dwellers in Delhi is turned around when the latter use the police's ability for violence to their own advantage. She notes that a number of women in the slums use the police to help them in cases of domestic violence. They ask the police to keep their abusive husbands in the police station lock-up for a day or night in order to teach them a lesson. The women do not file official complaints against domestic violence (DV) but cut informal deals with their local police officers because they do not have the social support or economic means to pursue court cases against their husbands. Police know this, along with the fact that they also do not want to be involved in the circuitous judicial processes that would ensue if the women were to file DV cases. However, the police often make use of the women's disadvantageous position to strengthen their authority in these areas and later use this advantage for arbitrary arrests or detentions.

As the next section demonstrates, the final crime maps do not reveal any of the complexities of creating maps such as capturing call data and turning it into crime data, or the infrastructural realities through which human prejudices turn into the "objective" realities of the map.

Address database inadequacies and human judgement in crime mapping

Delhi Police set up the Digital Mapping Division (DMD) in 2005 to provide it with geographical information about crime. In 2007, it started mapping crime events related to car thefts in the hope that this technology could solve the problem. Though no one in the DMD knew if it was the mapping that reduced car theft or if the problem resolved itself, the presumed success of this venture led to more crimes being added to the list. Eventually, rape, robbery, snatching, and e*ve-teasing*[9] were added while car theft was removed. One DMD team member explained to me that the remit of the DMD was expanded through ad-hoc decisions made by senior officers and without clear guidelines. DMD became the centre for all mapping-related activities of the Delhi Police, mapping incidents of fire, crime against women, and the placement of streetlights in the city. The DMD is also in charge of updating the address database and training call takers in the Dial 100 emergency call centre. This section considers the role of human judgement in the DMD's attempts to map crime incidents without an address database.

The recording of the data included in the maps involves various steps. First, a person calls the Dial 100 call centre which is where initial details of the crime are recorded along with the caller's address and phone number. This information is passed on to a dispatch officer within the call centre who sends a police car to the address. The attending police officer will then collect additional information on the incident. This verified information is relayed back to dispatch where it is sorted by crime category. This category may not always be similar to the category the initial caller would have had in mind. There are no standard rules for classifying crimes and the classification depends on police officers' interpretations of the incident and wider beliefs about crime as discussed above and in Marda and Narayan (2020). Similar incidents could be categorised as "snatching" one day and "theft" the next.

The supervisory team of the dispatch floor in the call centre recorded four kinds of heinous crimes (rape, robbery, *eve teasing*, and snatching) in a list of verified crime events of the previous 24 hours. This list is known as the "Green Diary". The recorded crimes are then mapped manually in the DMD using the software ArcGIS (see Marda and Narayan, 2020). Every day at 9 am the DMD prepares and prints out 23 crime maps, one for each head of police, to help them brief their teams.

As mentioned before, this data is mapped manually in the DMD where an officer manually marks incidents in the Green Diary on a map of Delhi using the ArcGIS interface. This becomes complicated because Delhi lacks a complete address database. At the time of its first implementation in 2007, there were only about 500,000 addresses for a population of roughly around 30 million, which did not include slums or areas of "unplanned" housing. This is a reflection of the fact that Delhi's master plans for both the years 1962 and 2001 did not provide any spaces to accommodate its mobile population that mostly makes its home in shanty towns and slums (Khanikar, 2018). There was also no database of all the major construction from the year 2000 such as metros, major roads, and flyovers. For the latter, officers in the DMD had to undertake extensive surveys of Delhi between 2005 and 2007 to prepare a base map of Delhi for crime plotting. A separate survey was done to mark police jurisdictional boundaries. Police station locations and jurisdictional boundaries remain the only complete location data held by the police. For this reason and with a turnaround time of about three minutes per call, call takers sometimes plot crime events at police stations rather than their actual locations, as this is the only information available to them.

The availability of a police station database as a drop-down menu (in the automated form where the call takers record call data) encourages this practice. However, the form has no provision for recording call locations separately from crime locations. The call takers are therefore trained to assume the location from where the caller is calling as the location of the crime. For example, call takers at the Dial 100 call centre recorded a hospital as the location of a crime, rather than the perpetrator's house, when a woman who was abused by her husband's family died at the hospital where she was being treated for her injuries. This mismatch occurred because the woman's father called the emergency number from the hospital and not from the husband's house.

The officer responsible for plotting the Green Diary data on an ArcGIS map of Delhi is Himesh.[10] He uses his own knowledge of the city, a result of 28 years as a beat constable, for plotting "crime" locations. He told me that if the address is just the name of a road, he plots it in the middle of the road.

The expectations are low as far as accurate mapping is concerned. Himesh said that he tries to map the positions as close as he could to the correct location. Addresses are easier to find if they mention landmarks. When in doubt about a crime location, Himesh would choose a nearby slum to plot a crime to rather than an upscale area (see Marda and Narayan, 2020).

In an attempt to improve the recording of addresses, police officers were given handheld digital devices to make communication easier. However, training along with the unavailability of charging ports rendered these devices nearly useless. The devices could have made sure that the correct location of a crime was relayed for plotting. The DMD's head said that officers' reluctance to use the devices was also to avoid their own surveillance as they would sometimes prefer not to attend the site of a crime and conduct the investigation on the phone instead. Officers explained to me in private that this was a result of the excessive workload assigned to them. It was impossible for them to attend to every call in person.

Like Himesh, many of those in the Mapping Division are officers who are on the verge of retirement or those stuck in bureaucratic processes such as a pending disciplinary enquiry making them ineligible for promotions or deputations. Thus, many of the current officers in the DMD are not very conversant with technology when they join and may take a long time to get used to working on a computer. Despite their crucial role in interpreting crime locations, as discussed in this section, there was a sense in the division that many senior officers did not consider it a priority in terms of funding or other resources, because the division was not involved in any mission-critical activities. Senior officers commented on how DMD officials were "bindu lagane wale" (those who merely put dots). Plotting crime events could not be equated to the more dangerous, and thus more "real" job of policing done in the field.

CMAPS: an automated crime mapping system

The Crime Mapping Analytics and Prediction System (CMAPS) was supposed to overcome the problems in manual mapping with automation. Work on CMAPS, developed by the Advanced Data Processing and Research Institute (ADRIN) wing of the Indian Space Research Organisation (ISRO) especially for Delhi Police, began in 2015. It was publicised with much fanfare in 2017 with news articles celebrating that the Delhi Police now had the capacity to predict crime before it happens.[11] It was supposed to replace manual mapping in the DMD, but currently both systems work simultaneously and CMAPS uses data produced by DMD as historical data for its own mapping. While DMD sourced its data solely from the emergency response system, CMAPS also includes first information report (FIR)[12] data from police stations in the city through the Crime and Criminal Network Tracking System (CCTNS)[13] that connects police stations to each other and to CMAPS. CMAPS plots 13 kinds of crime, including those plotted by the DMD. Even though internally

Delhi Police officials consider crime mapping or data analytics only secondary to "real" policing, more money is put into technology because of its public relations (PR) potential.[14] The negative public perception of Delhi as the country's crime capital is assuaged by regular updates on the technological innovation of the police force. These are communicated to the public through social media.

Login IDs and passwords for web access to CMAPS were provided to each Station Head Officer (SHO) and other senior officers who could use CMAPS to ascertain crime situations in Delhi anytime during the day. Despite this, officers seemed to prefer paper maps and hardly bothered to login to CMAPS. Officers search for stability in the changing world of policing where they feared that new technologies might render older officers obsolete. In contrast to a perception of digital devices as ephemeral, paper was seen as a technology of lasting relevance. When I asked a police officer why he was making a paper register when the information was automatically being stored on a digital server, he explained, "Ma'am *yeh to rahega hi, yeh (pointing to the computer) chahe aaye, chahe jaaye*" (Ma'am, the computer can come and go but the paper will always remain[15]). Meanwhile, the most common reason given for digitisation is the ease in storing and retrieving records as compared to paper.

This attachment to paper is symbolic of the fraught relation between the department and new technologies. While CMAPS was celebrated as a modern fix-all technology, the story of DMD's technological struggles is indicative of the kinds of frictions that can emerge from the arrival of new technological solutions. Although the DMD was set up in 2005, it was only in 2018 that the team acquired a printer that met the specifications for printing large-scale maps. Previously, the crime maps were saved on a regular pen drive and printed at a nearby shop, without much consideration for the privacy and security of the data that officers were dealing with. The head of the DMD guarded the new printer with his life – every print output was carefully logged so that official printer ink orders could be justified. Other departments could only use the printer after much begging and pleading. The purchase of the printer, even when CMAPS was deployed shows the continuities between a leap to a futuristic technology and the comfort of the known systems that help the police function every day.

The inadequacy of the address database, as mentioned earlier, was not the only reason that crime mapping was difficult. In DMD, the ArcGIS software that was used for mapping was not regularly renewed and there were no funds for high-functioning digital devices. The processors used in the computers used for running the mapping software were Intel Pentium P3 (being used in 2017–2019) and did not have the required processing power. When accessing the address database, I often saw DMD officials gently tapping the monitors waiting for them to come back on.

Steps taken to work around infrastructure gaps can create grave consequences in technologies such as predictive policing, as we have seen in the previous section on the way officers plot the crime according to their own interpretation of where the crime occurred and their knowledge of Delhi's geography. This can in turn impact the representation of certain areas as crime zones and, at the very least, the accuracy of the maps. As the same data became incorporated in CMAPS, the automated mapping system perpetuates existing errors and biases.

Infrastructure is relational (Star and Ruhleder, 1996) and a technology only becomes workable when these relations are maintained regularly. Merely buying a piece of technology does not guarantee that it works. Mapping is done in an ad-hoc way by Delhi Police partly because the very infrastructure that is assumed to be commonplace in the UK or US, such as a well-functioning address database, is simply not available in India. The costs of keeping this technology running often become prohibitive leading to decreased use and untimely closure of new projects. This trajectory is common to almost all imported, high-profile technological solutions in India. Even though CMAPS has been developed by an Indian organisation (ISRO), it replicates GIS-based crime mapping software developed in Western countries such as PredPol or CompStat. It thus provides little relief for the above-mentioned problems.

Upcoming markets in India and elsewhere are imagined as lucrative spaces for technological products developed in Europe or America. These technologies are sold at a mass scale to countries and often promote discriminatory data practices in the destination countries, such as the use of facial recognition in South Africa "re-entrenching racial apartheid".[16] While predictive policing is problematic even when it does work as intended, it being transplanted without looking into the social, cultural, or material aspects of the recipient countries can have additional problematic consequences on the marginalised populations.

Beyond the technical map

Numerous scholars have addressed maps and the meanings they convey. Wood describes how what is plotted on the map of North Carolina (US) is selected to present a suitable state for families (Wood, 2010). Deaths caused by traffic accidents and the city's air pollution are omitted from the map. Meanwhile, Leal shows how Latinx communities in Los Angeles (LA) have been using practices of "mapping from below" to register their presence in the city and stake a claim to its history (Leal, 2021). Leal describes mapping from below as a "self and collective cartographic endeavour" where communities define urban space on the map from their own vantage point. This is to counter the portrayal of the city as a gentrified, White-only space with only a few spaces for communities of colour, even when these Latinx communities have been part of the city's history from the beginning. What is omitted from a map matters. In the case discussed here, these are the decisions taken by officers in locating crimes on the map and attributing them to poor neighbourhoods. Even more so, the historic socio-structural processes of marginalisation and exclusion that are the main cause for crime in these neighbourhoods are missing.

The printed crime maps produced by DMD, as well as the digital map in CMAPS, show a uniform city. From colour palette, to map symbols, the city's different neighbourhoods look the same, but for the number of crimes in them. What is missing are the disparities such as the condition of municipal service delivery in poorer areas of Delhi. In reality, as shown in the "Cities of Delhi"[17]report, people experience marginalisation so severe as to amount to the condition of differential citizenship according to their place of residence. Deliveries of services like water, sanitation, waste removal, electricity, and transport are distributed according to space and legality. If maps genuinely displayed the conditions of the region they map, they would show these disparities and the histories of their making.

This is not a straightforward task as the software company's and police's discussion of including socio-economic variables demonstrates. During my fieldwork, a marketing executive told me that since poverty directly correlates with crime, Delhi Police needed to add socio-economic layers to CMAPS for efficient resource allocation and crime control, directly feeding into the bias that poverty begets crime. DMD officers agreed that such data intervention would greatly help in crime investigations in the city, in line with their own belief that poor areas are where crime takes place. DMD officials wanted to collect granular socio-economic data as well as profile data such as whether a person was a tenant or a homeowner, their occupation details, city of origin, and marital status, for every area in the city, but funds were not available. They were disappointed that few resources were directed towards surveying the "Bangladeshi immigrant colonies" that, according to them, are the "hotbed of crime" in Delhi.

One of the officers said that there should be a National Register of Citizens (NRC) [18] type of register in Delhi because immigrants contribute to high crime numbers. The NRC, currently underway in the Indian state of Assam, seeks to verify the documents of all residents and to identify so-called illegal Bangladeshi immigrants who have allegedly 'infiltrated' the state. Clearly including socio-economic data does not preclude police from blaming the marginalised for the crimes they experience. Rather, it would be used to target them more accurately. Like the hispanic neighbourhoods showing as White-only areas after gentrification in Leal's (2021) research discussed above, solely including socio-economic data does not reflect the history of these places and the lived experience of their residents. Instead, it reinforces existing ideas of criminality of these spaces being unsafe through increased surveillance and targeting of such areas.

Automation makes this worse. Even after spending two years at the Delhi Police HQ, I was not privy to the official documentation regarding the design and policy decisions of CMAPS. This is not just the case with CMAPS but with algorithmic systems across the world for reasons of proprietorship and to discourage people from "gaming" the algorithm. This opacity impedes criticism as the process of producing the map remains a "black box". In my research I have tried to circumvent this by looking closely at the organisation of the police and the people involved in collecting, processing, and plotting crime data. Considering crime mapping as a socio-technical system rather than merely a technical system gives a window to examine the resultant algorithmic systems even when the actual systems are not available to scrutiny (Marda and Narayan 2021).

Discussion and conclusion

Whether manual or automated, maps remain central to the distribution of resources in everyday policing. The refrain is that maps help police use their resources effectively by guiding them to spaces with a high probability of crime. Where in other places arrest data may play a role in this, in Delhi the crime maps are based solely on calls received on the emergency number 100 (now 112) (and are thus theoretically less biased). The maps created by the Digital Mapping Division (DMD) represent the previous day's crime data and direct the police to distribute their resources accordingly. By contrast, the automated system, CMAPS, was designed to work in real time. However, as my fieldwork suggests, so far, it is not used for daily or routine decisions by the police. On the face of it, these maps produce a daily picture of crime and do not discriminate based on caste, class, or gender. However, as this chapter has demonstrated, the geographical information systems that produce the crime maps work with data based on problematic assumptions about crime and criminality ingrained in Delhi Police crime recording practices. Maps render invisible the underlying social processes that characterise crime detection, reporting, and mapping.

Crime is a social construct and what is considered abnormal or non-normative behaviour changes with social context (Durkheim, 1933). Dominant groups can often more readily shape what is perceived as criminal. Criminalising certain actions can be used to control populations. For example, nomadic communities are controlled when their movement is criminalised. A focus on property crimes, rather than financial crimes or violence against women, indicates whose interests are being protected (Wallace, 2009). In Delhi, calls to the emergency helpline are mostly made by people living in poorer areas of the city. This is because the helpline is often the only way for them to access the state. These calls are then taken as proof that the inhabitants of particular areas are prone to be criminals. When unsure of the exact location of an incident because of the lack of an address database, plotters map crimes as having occurred in a nearby slum rather than in an affluent area. This manually recorded information then becomes input data for the automated mapping system (CMAPS). Though CMAPS uses First Information Report (FIR) data along with call data for its mapping, it does not make it less biased. FIR data is fraught with police discretion and assumptions about the criminality of certain groups within society (such as people from a particular class, caste, or gender). For example, most victims of rape and sexual crimes in India find it difficult to get an FIR registered. Maps thus perpetuate their makers' understanding of the locations of crime within the city which then provides a justification for the surveillance and control of areas such as slums and shanty colonies, traditionally considered hotbeds of crime. Maps do not provide information about crime in a region but, counterintuitively, are proof (Kindynis, 2014).

Crime mapping in Delhi does not provide explanations for why some areas contain more crime than others. The maps do not represent the realities of the geography they represent. There is no difference between an area which lacks basic municipal services and one that is more affluent. Without any reference to underlying social factors, the only response to such a map is to somehow *reduce* the crime numbers through surveillance and control of "crime prone" areas. Thus, crime maps not only encourage but justify the surveillance and control of marginalised areas of the city.

Notes

[1] See Das and Walton (2015) for a description of the life of people in urban slums and the politics to keep them that way. Taking the case of Muslims as a particular case of the urban marginalised poor, Jamil (2014) argues how the state makes sure that these bodies are restricted to the fringes.

[2] See Singha (1998, 2015), Khanikar (2018), and Narayan (2020, 2021) to understand policing in India and how it is extensively used to control and surveil marginalised populations.

[3] The Delhi Police HQ was running out of leased space from the Public Works Department in Central Delhi where I finished my fieldwork for this research. Since 2020, the Delhi Police HQ has shifted to its own new space in another part of Central Delhi. See here "Delhi Police has a new address" https://www.hindustantimes.com/cities/delhi-police-hq-has-new-address-jai-singh-road-in-central-delhi/story-ll7eNq24YhqKCalIMyt8YP.htmlhttps://www.hindustantimes.com/cities/delhi-police-hq-has-new-address-jai-singh-road-in-central-delhi/story-ll7eNq24YhqKCalIMyt8YP.html accessed 8 February 2022.

[4] Ibid.

[5] Delhi Police chief blames migrants, youth's frustrations for rising crime graph, https://www.hindustantimes.com/delhi-news/delhi-police-chief-blames-migrants-youth-s-frustrations-for-rising-crime-graph/story-jUOlAjinWl7i1Ae22tyYvL.html accessed Tuesday, 27 October 2020 11:59 PM

[6] To curb theft in the city, the Delhi Police chief asks to identify anti-social youth https://indianexpress.com/article/cities/delhi/to-curb-theft-in-city-identify-anti-social-youth-delhi-police-chief-5396450/https://indianexpress.com/article/cities/delhi/to-curb-theft-in-city-identify-anti-social-youth-delhi-police-chief-5396450/ accessed Wednesday, 28 October 2020 12:15 AM

[7] Status of Policing in India Report (SPIR) (2018) https://www.commoncause.in/pdf/SPIR2018.pdf accessed Saturday, 31 October 2020 8:03 AM

[8] Police work 14 hours a day and get few weekly offs accessed Friday, 15 April 2022 link: shorturl.at/etAP7

[9] A euphemism for any kind of public harassment of women, including catcalling and inappropriate physical contact, which cannot be legally defined as rape. It is a problematic word as it tries to downplay the abuse that women suffer in public

life in India. Its acceptance as a category of crime in the police indicates how public safety and mobility for women is not a priority issue for police as is made out to be.

[10] Names have been changed for anonymity.

[11] Preventing crime before it happens https://www.hindustantimes.com/delhi/delhi-police-is-using-precrime-data-analysis-to-send-its-men-to-likely-trouble-spots/story-hZcCRyWMVoNSsRhnBNgOHI.html accessed Friday, 15 April 2022

[12] First Information Reports are filed in police stations after a preliminary enquiry of a complaint to verify its authenticity. Once filed, a formal investigation is launched on the case, which culminates in a chargesheet and a trial. In Delhi (as also in all states of India), these FIRs are fed into the CCTNS system. In Delhi, CCTNS is connected to CMAPS for crime mapping.

[13] National Crime Records Bureau, Government of India, developed a crime and criminal tracking network system (CCTNS) to digitally record First Information Report (FIR) data and daily entries of police stations across India. CCTNS also connects the police stations with each other to streamline sharing of information amongst stations. https://ncrb.gov.in/en/crime-and-criminal-tracking-network-systems-cctns

[14] Delhi is in the news for all the wrong reasons when it comes to crime and is perceived to be the most unsafe city in India, especially for women read https://www.newslaundry.com/2020/01/27/why-is-delhi-indias-crime-capital and https://indianexpress.com/article/cities/delhi/delhi-is-most-unsafe-for-women-ncrb-data-confirms-7511261/ and https://www.news18.com/news/india/capital-crime-rape-tripled-kidnapping-of-women-doubled-in-delhi-in-last-10-years-says-police-data-4926263.html accessed Friday 15 April 2022. The furore against the police and the law and order situation in the city increased after a medical student was brutally raped after she was returning from the movies at 9 pm. See: https://www.hindustantimes.com/india-news/delhi-2012-gang-rape-case-what-happened-on-december-16/story-GboszJckGgslhWHpRcci4K.html accessed Friday, 15 April 2022.

She died soon after. Huge protests against the police saw the state reacting with water cannons and batons at the protestors, and the then Chief Minister of Delhi, Sheila Dixit, claimed helplessness as she did not have the police under her power. The police in Delhi are under the central government and do not answer to the state government. This event further cemented the perception that the law and order situation of the city is a problem of the inefficiency of the police and they are insulated from city work as they work for the central government.

[15] Matthew Hull (2016) has given a succinct description of the origins of a documentary system in governance in introduction (pp. 7) where he outlines the use of paper in Indian bureaucracy as a remnant of colonial rule. The British government used a paper trail as evidence of a job done instead of believing human accounts of the same.

[16] See Karen Hao's investigative series where she is looking at AI colonialism or how AI technologies are creating a new "digital world order" very similar to the imperial world order that subjugated countries especially in what is now known as the Global South https://www.technologyreview.com/2022/04/19/1049592/artificial-intelligence-colonialism/ accessed may17 2022. See also https://www.technologyreview.com/2022/04/19/1049996/south-africa-ai-surveillance-digital-apartheid/ where she talks about South Africa, its use of CCTV cameras and the surveillance and discrimination that follows.

[17] The cities of Delhi report http://citiesofdelhi.cprindia.org/wp-content/uploads/2015/12/Cities_of_Delhi-Overview.pdf accessed Wednesday, 28 October 2020, 4:18 PMhttp://citiesofdelhi.cprindia.org/wp-content/uploads/2015/12/Cities_of_Delhi-Overview.pdf

18 See 'What is NRC at https://www.business-standard.com/about/what-is-nrc accessed 15 April 2022

References

Benjamin, R. (2019) *Race After Technology: Abolitionist Tools for the New Jim Code*. Medford, MA: Polity Press.

Berger, P.L. and Luckmann, T. (1991) *The Social Construction of Reality*. London/ New York: Penguin Booked.

Bowker, G.C. and Star, S.L. (1999) *Sorting Things Out: Classification and Its Consequences*. Inside Technology. Cambridge, MA: MIT Press.

Das, V. and Walton, M. (2015) 'Political Leadership and the Urban Poor: Local Histories', *Current Anthropology,* 56(S11), S44–54.

De Courson, B. and Nettle, D. (2021) 'Why Do Inequality and Deprivation Produce High Crime and Low Trust?', *Scientific Reports,* 11(1), 1937. https://doi.org/10.1038/s41598-020-80897-8.

Durkheim, E. and Simpson, G. (1933) *Division of Labour in Society*. New York: Macmillan.

Ervin, M.A. (2009) 'Statistics, Maps, and Legibility: Negotiating Nationalism in Post-Revolutionary Mexico', *The Americas,* 66(2), 155–79.

Eubanks, V. (2018) *Automating Inequality: How Hight-Tech Tools Profile, Police, and Punish the Poor*. New York, NY: St. Martin's Press.

Ghertner, D.A. (2015) *Rule by Aesthetics: World-Class City Making in Delhi*. New York: Oxford University Press.

Hull, M.S. (2016) *Government of Paper: The Materiality of Bureaucracy in Urban Pakistan*. Los Angeles: University of California Press.

Jamil, G. (2014) 'The Capitalist Logic of Spatial Segregation', *Economic and Political Weekly,* 49(3), 7–8.

Jefferson, B.J. (2018) 'Predictable Policing: Predictive Crime Mapping and Geographies of Policing and Race', *Annals of the American Association of Geographers*, 108(1), 1–16.

Khanikar, S. (2018) *State, Violence and Legitimacy in India*. New Delhi: Oxford University Press.

Kindynis, T. (2014) 'Ripping up the Map: Criminology and Cartography Reconsidered', *The British Journal of Criminology,* 54(2), 222–243.

Knorr-Cetina, K.D. (2009) *The Manufacture of Knowledge: An Essay on the Constructivist and Contextual Nature of Science*. Pergamon International library, (ed.or 1981) https://nbn-resolving.org/urn:nbn:de:bsz:352-opus-83790.

Latour, B. and Woolgar, S. (1979) *Laboratory Life: The Social Construction of Scientific Facts*. Beverly Hills: Sage Publications. https://archive.org/details/laboratorylifeso0000lato.

Leal, J.N. (2021) 'Mapping the City from below: Approaches in Charting out Latinx Historical and Quotidian Presence in Metropolitan Los Angeles: 1990-2020', *European Journal of American Culture,* 40(1), 5–26. https://doi.org/10.1386/ejac_00035_1.

Marda, V. and Narayan, S. (2020) 'Data in New Delhi's Predictive Policing System', in *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency*. FAT* '20. New York, NY: Association for Computing Machinery, 317–324. https://doi.org/10.1145/3351095.3372865.

Marda, V. and Narayan, S. (2021) 'On the Importance of Ethnographic Methods in AI Research', *Nature Machine Intelligence,* 3(3), 187–189. https://doi.org/10.1038/s42256-021-00323–0.

Nandi, S. (2016) 'Respectable Anxiety, Plebeian Criminality: Politics of the Goondas Act (1923) of Colonial Calcutta', *Crime, Histoire & Sociétés / Crime, History & Societies,* 20(2), 77–99.

Nandi, S. (2019) 'Goondas of Calcutta: Crimes and Policing in Colonial India', in K. Jaishankar (ed.) *Routledge Handbook of South Asian Criminology*. New York: Routledge – Taylor and Francis Group, Ch.12

Narayan, S. (2020) 'Past, Present, and Past as Present in India's Predictive Policing', *XRDS: Crossroads, The ACM Magazine for Students,* 27(2), 36–41. https://doi.org/10.1145/3433144.

Narayan, S. (2021) 'Guilty Until Proven Guilty: Policing Caste Through Preventive Policing Registers in India', *Journal of Extreme Anthropology,* 5(1). https://doi.org/10.5617/jea.8797.

Nigam, S. (1990) 'Disciplining and Policing the "Criminals by Birth", Part 2: The Development of a Disciplinary System, 1871-1900', *The Indian Economic & Social History Review,* 27(3), 257–287. https://doi.org/10.1177/001946469002700302.

Scott, J.C. (1999) *Seeing like a State: How Certain Schemes to Improve the Human Condition Have Failed*, New Haven: Yale University Press.

Seaver, N. (2017) 'Algorithms as Culture: Some Tactics for the Ethnography of Algorithmic Systems', *Big Data & Society,* 4(2). https://doi.org/10.1177/2053951717738104.

Singha, R. (1998) *A Despotism of Law: Crime and Justice in Early Colonial India*. Oxford: Oxford University Press.

Singha, R. (2015) 'Punished by Surveillance: Policing 'Dangerousness' in Colonial India, 1872–1918', *Modern Asian Studies,* 49(2), 241–269. https://doi.org/10.1017/S0026749X13000462.

Star, S.L. and Ruhleder, K. (1996) 'Steps Toward an Ecology of Infrastructure: Design and Access for Large Information Spaces', *Information Systems Research,* 7(1), 111–134.

Turnbull, D. (1996) 'Cartography and Science in Early Modern Europe: Mapping the Construction of Knowledge Spaces', *Imago Mundi,* 48(1), 5–24. https://doi.org/10.1080/03085699608592830.

Wallace, A. (2009) 'Mapping City Crime and the New Aesthetic of Danger', *Journal of Visual Culture,* 8(1), 5–24. https://doi.org/10.1177/1470412908100900.

Wood, D. (2010) *Rethinking the Power of Maps*. New York: Guilford Publications.

7 Infrastructure shortcuts

The private cloud infrastructure of data-driven policing and its political consequences

Daniel Marciniak

Introduction

A shift occurred during the coronavirus pandemic of 2020: many police forces in the United Kingdom moved their databases online to allow their officers to work from home during the consecutive lockdowns that were imposed. A company representative at a security exhibition in 2021 was cheerful about the future business opportunities this would open. She recounted an extraordinary shift over 18 months during which police went from being very nervous about every little bit of data in the cloud to allowing for the heart of their IT infrastructure – the records management system – to be accessible from anywhere. In fact, the two companies that have cornered 60–70% of the market with competition-limiting practices (Ofcom, 2023), Amazon Web Services (AWS) and Microsoft Azure, are expressly marketing their products to police forces worldwide (Kwet, 2020; AWS, 2023; Microsoft, 2023). What on the surface looks like a boring, mundane change that, at most, cybersecurity experts would be concerned about, may have far-reaching consequences for how police create knowledge and, based on this knowledge, how we will be policed in the future.

Stored on cloud services, police data becomes open to third-party add-on software that seeks to generate insights from this data, routinely analysing it and visualising the results. Amazon and Microsoft offer (two separate and incommensurable) "ecosystems" of second-tier companies that provide these add-ons which run on the same servers and can thus be easily "plugged into" the data. For example, Saadian's Prisoner Intelligence Notification Systems runs on AWS servers and is used by police forces across the UK to track releases from prison (AWS, 2023). Similarly, Microsoft's partners include a full range of big names in policing technology like Accenture, Axon, Genetec, Motorola, and NICE (Microsoft, 2023). A whole new market offers itself up to policing.

Drawing on Srnicek (2016) and Langley and Leyshon's (2017) concept of *platform capitalism*, some authors have referred to this change as the *platformization* of policing, describing a cloud-based infrastructure that integrates data streams from disparate sources, internal and external to policing, allowing new forms of analysis and prediction that are intended to shape

DOI: 10.4324/9781003412908-10

future police action (Egbert, 2019; Gates, 2019; Linder, 2019; Wilson, 2019). Platform capitalism, as Wilson (2021: 51) puts it, is "integrating policing into the circuits of the digital economy through intensive datafication". This chapter develops this perspective by examining police's dependency on a private provision of cloud infrastructure as an *infrastructure shortcut*: a way for police to receive advanced data analysis without the need for developing and maintaining underlying infrastructure. Crucially, this also entails a lack of detailed understanding of the functioning and control over the design of this infrastructure.

Much research has followed Amoore's (2018) call to shift focus from the material question of where "the cloud" is to examining the new epistemologies of automatic pattern and anomaly detection that emerge from cloud computing and related fields of big data, machine learning, and artificial intelligence. Instead, this chapter seeks to illuminate the *interrelation* of materiality and epistemology by asking what the consequences are of who owns and maintains the cloud infrastructure. The tools running on data platforms often seek to structure workflows and ultimately to automate the epistemic work of interpreting the data routinely produced by police – answering questions of which areas police should patrol, which incidents to investigate first, which officers to put under closer supervision, and so on. With commercial solutions, there is no public discussion of the purposes and mechanics of data use because they are often proprietary and outside the purview of democratic decision-making. Moreover, by outsourcing this epistemic work to private companies, thus rendering it an invisible infrastructure, police may be risking not only a technical but also an epistemic lock-in by giving up on their ability to reflect on and revise the epistemic work central to their operation.

The analysis in this chapter centres on the example of place-based predictive policing and is based on semi-structured interviews with 18 members of police forces in analyst or planning positions representing 11 police forces in the United Kingdom and 3 in the United States, 12 employees from five predictive policing companies, and observations made at six security trade shows in the US, the UK, and Germany. Predictive policing refers to the use of data analysis detecting patterns in crime data that are used to identify targets for police intervention. This can be the use of risk scores for prioritising individuals likely to (re-)offend or forecasting the location of crime events. In this chapter, the focus shall be on the latter. It adds to the growing body of research that has extensively dealt with unmasking the "objectivity" of place-based predictive policing, analysing it as a socio-technical assemblage and revealing the risk of biased feedback loops, as well as studying police officers' attitudes towards this technology and its influence on their decision-making (Benbouzid, 2019; Kaufmann, Egbert, and Leese, 2019; Ratcliffe, Taylor and Fisher, 2019; Shapiro, 2019; Egbert and Leese, 2020; Marda and Narayan, 2020; Sandhu and Fussey, 2020; Brayne, 2021; Duarte, 2021; Lally, 2021; Tulumello and Iapaolo, 2021; Waardenburg, Huysman and

Sergeeva, 2022). While predictive policing may have already reached the end of its popularity with some police forces in the UK and the US ending its use and the EU considering an all-out ban, it has been one of the first machine learning-based technologies implemented widely in policing, and the linkages between infrastructure work and political decision-making presented in this chapter are indicative for future data-driven technologies in policing.

The idea for place-based predictive policing has its origins in hotspot mapping, which gained particular popularity with the advent of computerised systems for recording and mapping crime and the management of patrol through the COMPSTAT process, in which mid-level officers are held accountable for the crime statistics within their areas of responsibility (La Vigne and Groff, 2001; Wilson, 2020). Crime is addressed from a rational choice perspective which imagines the offender as more likely to commit crime in a familiar environment – a perspective that Jeffrey Brantingham, one of the main proponents of predictive policing and co-founder of the company PredPol, describes using the analogy of the offender as forager (Brantingham and Tita, 2008; Maguire, 2018). Without further knowledge about the offender, recorded crime patterns become a proxy for this behaviour and areas with higher crime concentration become the problem that needs to be addressed. While there are approaches such as risk terrain modelling which attempt to solve the "problem" by changing the built environment, for example, by changing the lighting conditions in a high-crime area, the primary "solution" to crime patterns in predictive policing is deterrence achieved through the allocation of police patrols (Benbouzid, 2015; Eck and Clarke, 2019).[1] With the problem and its solution thus identified, the predictive problem essentially becomes a management problem of how to produce timely forecasts, distribute them to officers, and ensure that predicted areas are patrolled (Benbouzid, 2019).

The predictive policing software that addresses this management problem exists in a variety of institutional arrangements between police and the private sector including (a) standalone software running on police servers, (b) customisable data analysis employing generalist tools like SPSS Modeller, SAS, or visual programming tools in Microsoft Azure, and (c) dedicated predictive policing tools that run on cloud servers (regularly owned by Amazon or Microsoft). The latter arrangement will be the focus of this chapter.

This chapter contributes an insistence on the minutiae of infrastructure work in laying out a nuanced critique of the platformisation of policing and (well-intentioned) design decisions in the automation of police functions. The chapter begins with a discussion of infrastructure work in terms of setting up and maintaining technical infrastructure as well as designing a process that engages all levels of the police organisation. Having set out the basis for why (some) police forces have opted for commercial products, the chapter then analyses the setting of priority crimes and the issue of feedback loops as examples of the detailed political decision-making that goes into the development of predictive policing. Finally, it critically discusses police agencies' dependence on private companies for their IT infrastructure.

Commercial infrastructure shortcut

As Star and Ruhleder (1996) have argued, infrastructure is fundamentally relational. While it is transparent to its users, it is the centre of activities for those who build and maintain it. The complexity and cost associated with this usually invisible infrastructure work form a central reason for police to outsource the production and maintenance of software and underlying hardware to private companies. The aim of this section is to provide insight into this complexity before the second part of this chapter explores how this outsourcing means that private companies gain considerable influence over political aspects of policing priorities.

Police data management systems have long been predicated on the logic of the archive; a record of information that is saved for an imagined future use (Derrida, 1995; Waterton, 2010). Police bureaucracies have been built around the archiving and retrieval of criminal records almost since their inception and, in the UK, challenges around territorial police forces recording crime data independently remain more than a century later (Thomas, 2007). These systems were designed to retrieve individual records one at a time. Thus, the underlying infrastructure is poorly adapted to the kinds of analysis required for predictive policing (or other forms of AI/machine learning for that matter). These require retrieving information from all files at the same time. Implementing predictive policing hence presents a major logistical challenge that further includes maintaining servers that are able to run the statistical models at regular intervals. These servers also need to allow for data entry and be able to display maps with predictions. This challenge can be difficult to meet for police forces, whether this is in getting the machines ready for the task or getting machines and humans to cooperate.

An example of this is a predictive policing implementation in West Yorkshire, UK, where technological "teething problems" with maps failing to update led to scepticism and minimal uptake (Hamlin, Ellinger, and Jones, 2019). Before it even gets this far, the technological requirements to regularly update complex statistical models can prove prohibitively expensive. This is why one of the interviewed analysts developing his own predictive models looked enviously towards the technology in the neighbouring police force:

> They were like a test force for the country. So they received quite a lot of investment from Microsoft and from IBM SPSS as well. And not just in terms of training and software but infrastructure: two 40 gigabyte servers to help process their information and stuff like that. So they can download their information every five minutes. We can do it [at] two in the morning.
>
> (UK Police Analyst)

It is this bridging of infrastructural problems by private companies that this chapter seeks to foreground.

Predictive policing is not a private sector innovation. Rather, it has emerged from the academic field of environmental criminology concerned with the spatial concentration of crime. One of the first implementations of the idea of focusing deterrence in specific places at specific times was an experimental study addressing near-repeat burglaries in Manchester (Wilson, 2020). As such, there are not many secrets around the way predictions are produced. One software developer even suggested that the company could make their prediction algorithms public without fearing for their market position as the main challenge would lie in providing the "plumbing" in the background (Software Developer). This section thus first describes the technical "plumbing" associated with maintaining and setting up the predictive policing infrastructure and then discusses the design of the underlying workflow that turns predictive policing from a research project into a product.

Infrastructure work

There are two main areas of infrastructure work that software companies do: maintaining and updating the code base and setting up infrastructure to take in data from new customers. This section describes the two in more detail and reflects on their role in privileging a centralised, commercial provision of the technical infrastructure required for predictive policing.

To begin with updates and maintenance: A software developer described the steps for a new feature update as the following: whenever there is a new feature that is added to the software, software developers first write the necessary code for a version of the software running on their local machines, the development environment. If everything seems to work, the changes move on to the release environment. This is an account with the cloud service provider that is not connected to any of the customers. Only once the updated software is running on these servers without issues, it is rolled out to operational servers, the staging environment. Testing the new features involves running a series of pre-programmed scripts that simulate a user to test comprehensively for errors (Software Developer). A similar approach is taken to check for security vulnerabilities: automated scripts ensure that different types of accounts (admins, analysts, data owners, data viewers) have access only according to set permissions (Software Developer).

There is thus a considerable amount of work that goes into ensuring that new features do not jeopardise the functioning and security of the system when they are rolled out. Quite opposite to the imagination of a fixed black box continuously transforming inputs into outputs, the software is subject to constant adaptation and change. As research on maintenance and repair has highlighted, it takes work to maintain the relations of socio-technical assemblages (Graham and Thrift, 2007; Denis and Pontille, 2019). Here, this applies both to the small adjustments of bug fixes as well as to larger readjustments of what the software's role is (see the shift from crime prediction to patrol management discussed in the next section).

Police analysts usually have the skills to develop predictive models but are not trained software developers able to maintain everything from data intake to user interface. Without a dedicated team of software developers, it is nearly impossible for a single police force to carry out the work described above and maintain its own computer code. Maintenance work can thus form one of the in-roads for private companies to provide predictive policing solutions. Being part of a cloud infrastructure that allows these continuous changes at a distance further supports the common subscription-based business model for predictive policing.

This is not to say that companies do not struggle with some of the same challenges as police forces – as well as challenges that are unique to them. This is particularly the case for the second type of infrastructure work which relates to the initial setup of links between different elements of the predictive policing assemblage. A central challenge that affects both companies and police is the integration of data from different databases. For instance, one interviewee described how he and his colleagues had to write multiple computer scripts that would regularly copy data from various legacy systems designed without interoperability in mind into a more general database (US Police Head of Analysis). Similarly, companies have to figure out how to retrieve data from a variety of systems. As a data scientist complained, "each department has different CAS [crime administration system] and RMS [record management system] systems" (Data Scientist 2).

A challenge unique to companies is to then apply their general predictive model to data that is subject to a large variety in recording practices. For example, some police departments record an incident with a single time and date referring to when it is recorded, and others record it as a period within which the incident is thought to have occurred (Product Manager and Data Scientist). Examples like this, and more generally the availability of different variables, result in the need for predictive models tailored to each police force. Only once this initial setup is completed, the models become cogs in the bigger machinery of data retrieval, processing, and display.

Apart from these technical challenges, companies face a unique challenge in institutional hurdles as outsiders to police departments. Some police forces would not have the resources to provide a dedicated contact person, or policies on data security would create hurdles for connecting the police's data into the companies' software (Product Manager and Data Scientist). With security guarantees by the big cloud providers (Microsoft and Amazon both offer services tailored to governments) and the recent move to cloud storage to allow working from home during the Covid pandemic, these concerns for data safety and technical issues around interoperability of data storage are becoming less and less of a hurdle.

Putting the challenges of the initial setup aside, hosting the predictive tools on servers in the cloud has the advantage for companies that they can reuse the same computer code for different customers, whereas police forces have to put things together from scratch. It is difficult to overstate the importance that cloud infrastructure plays in this. This is demonstrated by the case of one company that went from prediction software running on a desktop computer to a web-based interface, and most recently to a cloud-hosted solution. The Product Manager describes how crucial the move to a cloud-based service was for their business model:

> In the second phase of [the software], [its] version one. That was all built in a manner to be installed on a server at a police department's headquarters or in their IT … and so the price doesn't scale up and down very well because setting that up and getting it integrated and install is the same amount of work for a small police department as for a big department. So, when that was kind of ready, we had inelasticity of the price and then the economy wasn't doing well, so budgets were really tight and so we really didn't get a whole lot of traction on that.
>
> (Product Manager and Data Scientist)

With the software hosted in the cloud, smaller departments have access to an infrastructure that the company has built using government grants and investments from other customers when they would not have the budget to develop a predictive policing software themselves (Product Specialist 1). What predictive policing companies offer is the simplicity of boxes on a map accessible to all officers without needing to develop and maintain the infrastructure that automates prediction and delivery.

More generally, the increasing move to cloud services promises easier access to data for analysis rather than solely maintaining the chain of custody for the bureaucratic paper trails of policing. With the data already online, companies can attach their modes of analysis as add-ons. Companies take infrastructure problems that many police forces are ill-equipped to deal with, such as maintaining computer code and integrating data from proprietary databases, and they transform them into the forgotten, boring background of invisible infrastructure (Star, 1999).

Designing patrol management

Apart from the technical challenges described in the previous section, the development of predictive policing poses a design challenge: making the product enticing to a range of actors, or, to use Callon's (1984) phrase, *enrolling* them in the socio-technical assemblage of predictive policing (for a description of this assemblage see Egbert and Heimstädt in this volume). Companies have an institutional focus on making predictive policing work and can adjust their offerings through updates of software running in the cloud. In providing insight into some of the design processes, this section argues that companies employ these advantages to learn in an iterative process how to enrol various agents from police officers and police management to databases and prediction algorithms.

Predictive policing trials are emblematic of the different lessons that police and companies can take from them. In the UK, there have been multiple trials of predictive policing funded with innovation funding from the Home Office. These trials, as one interlocutor observed, often serve the career of the officer organising them but seldom lead to a stable application and remain at a prototype stage (UK Police Head of Intelligence Analysis). Other trials fail when the money runs out that was used to finance additional patrol time, or they never manage to have enough data to produce predictions. Designing a complete product is also a challenge for the software companies, as one interviewee described,

> The forecasting aspect was like we were building what was available in the academic literature, but it didn't kind of fuse things together enough to actually make it a very operationally useful product [...]. We had different features, like we had the [areas to focus on], we had the visualisation of past crimes, we had the near-repeat pattern zones. But it wasn't clear how that all came together to capture and secure workflow.
>
> (Product Manager and Data Scientist)

This highlights the importance of designing the whole workflow rather than just providing predictions. In contrast to police agencies, some companies have benefited from trial funding because it allowed them to refine their product in multiple stages. The outcome is a product that, as Benbouzid (2019) observes, not only provides a map of likely areas of crime but mainly enables the management of police patrols. Accordingly, PredPol has recently embraced patrol management in their rebrand to Geolitica as the product's main feature (PredPol, 2021). Managing patrols is no small feat: Manning (2008), for example, demonstrates the largely performative quality of crime mapping in the CompStat process, a precursor to predictive policing, and its failure in transforming existing patrol practices.

The police officers who are supposed to follow the computer's instructions on where to patrol are sceptics. As research by Sandhu and Fussey (2020) shows, officers question the superiority of the automated analysis over their own judgement and are concerned about biases in the data. Oftentimes, officers question the uniqueness of the insight provided by predictive policing. As one interviewee puts it, "No shit. We're going, 'Oh yeah, what a surprise'" (UK Detective Sergeant). Ratcliffe, Taylor, and Fisher (2019) encountered similar resistance in the Philadelphia predictive policing experiment. In a trial for West Yorkshire police, Hamlin, Ellinger and Jones (2019) found that it was difficult to convince officers of the software's effectiveness when the likelihood of encountering crime in a patrol zone was generally very low. As one of the sergeants they interviewed put it: "If you are wandering around and nothing's happening, it's hard for people to see that they are doing a good job" (Hamlin, Ellinger and Jones, 2019: 478).

To successfully insert themselves in the patrol management process, the companies studied in this chapter appeal to both the patrol officers on the street and their managers in the back office. Addressing the perceived attack on officers' professional judgement, one strategy is to move predicted areas around so that they are not just those that officers would expect from their own experience:

> We generally have to walk a fine line between telling them things that they agree with and surprising them a little bit. Because we want them to buy into the prediction and believe it and, and say that, 'oh yeah, I, I agree with what it's predicting', but we also want to change it up a little bit so that they, they don't sit there and say like, 'well, this thing isn't telling me anything new'. So, it's kind of the balancing you have to strike.
>
> (Product Manager 1)

Another approach is to reintroduce choice in the form of choosing between multiple predicted areas and choosing what to do in that area. A product manager describes how this is done to give officers a sense of agency,

> We don't give them one box to go to, to sit in all the time. We give them a few boxes and [...] we suggest tactics for them to try. And we rather than giving them one tactic, we've since developed the choice to decide what sort of tactic they want to try based on the situation or based on the timing or based on the type of crime. Whatever they think would be most effective. They can choose that. And I think some of that does drive some motivation or at least makes it less about like, "oh, I'm being told exactly what to do". And more about like, "oh, I have some agency in deciding what I can do".
>
> (Product Manager 1)

At the same time, predictive policing companies use GPS sensors from the devices that are used to display the maps to record officer movements and the time they spend in predicted areas (at times circumnavigating police unions' resistance to GPS trackers on police cars). They also provide a tool for officers to report what they do in a predicted area. All this information is then fed back to senior officers in the form of data visualisations "trying to provide agencies with better tools to manage their patrols" (Product Manager 2). This arrangement thus mobilises the authority of senior officers to supervise patrol officers and enables them to exercise control while simultaneously offering patrol officers a sense of professional independence. Evidently, there is more to predictive policing than boxes on a map. It is perhaps not surprising that the approach from some software engineers is this coupling of workplace surveillance and gamification (for examples outside policing see Whitson, 2013).

Some of the predictive policing providers, like PredPol/Geolitica and Hunchlab/Shotspotter Missions, also offer senior officers the ability to manually assign areas for patrol, moving further away from an "objective" crime reduction tool to a management tool. All these design decisions catering to the requirements of patrol management, rather than solely the production of predictions and their display on maps, depend on further infrastructure in the form of features in the software, some of which require major changes in user interfaces and database models (Software Developer).

The use of a cloud infrastructure and building on experiences in multiple trials with multiple police forces allow companies to build software in an iterative process that not only predicts crime but also creates a "workflow" aligned with the organisational requirements of supervising police patrol. Whether for predictive policing discussed here or more generally for (automated) data analysis and visualisation, the two elements of maintaining technical infrastructure and designing workflows tilt adoption and development towards commercial solutions in the form of plug-ins to data hosted on servers belonging to AWS, Microsoft, or another cloud provider. Not only does this create a problematic oligopoly of cloud ecosystems (Ofcom, 2023), it also comes with the danger of technological lock-in. As the conflict between NYPD and Palantir around moving police data to a different service provided by IBM shows (Iliadis and Acker, 2022), switching providers can come with difficult questions around how to transport not only the raw data but also the insights that have been created in the past.

Deciding priorities

Perhaps oligopolies of cloud providers with significant market power and technological lock-ins are only a nuisance. After all, police forces, as discussed above, are already used to being stuck with legacy systems that do not interoperate and with what Hayes (2012) terms the surveillance–industrial complex, which includes revolving doors between industry and state agencies – not exactly a "healthy" form of a competitive economy. So, what is the concern? Reflecting on the initial wave of computer adoption in US policing in the 1960s, Kent Colton (1979) warned already four decades ago that "the computer may also serve to reinforce the status quo, to lock in and substantiate our present approach, and to indirectly countermand other innovation" (Colton, 1979: 19). The concern is that just as patrol cars have cemented a form of patrol that hinders engagement with people on the streets, policing software may have lasting effects on the way we are policed. Products like predictive policing have a different character from other products police agencies purchase, like cars, guns, and even record management systems. Because they seek to automate knowledge production, they influence not only *how* the police act but also *why* they act.

This section discusses two ways in which the use and design of predictive policing contain normative decisions around what policing should be: it first discusses the (at times only implicit) weighting of police priorities, before then engaging with design responses to the common criticism that predictive policing reinforces existing institutional biases. In outlining the design choices of developers, the argument of this section is not to say that they make poor or dangerous decisions that worsen policing. Quite the opposite, developers are aware of the pitfalls of predictive policing and, with possibly limited success, seek to mitigate these. What this section does problematise is the fact that political decisions about the purpose of policing in terms of how it operates (patrol for deterrence) and what it prioritises (predictable types of crime) become fixed in products without ever being subject to wider political deliberation. Moreover, outlining the complexity of producing crime prediction highlights how the automation aspect of predictive policing outsources and partially replaces the roles of analysts and their intimate familiarity with crime patterns, removing core knowledge required to make strategic decisions. A police force that has automated its crime analysis risks losing the capability to rethink its approach to crime. In this, predictive policing is not much different from the larger trends of governments outsourcing expertise to consulting firms, as described by Mazzucato and Collington (2023).

Companies are involved in highly political decisions around what policing is today. This is particularly true in a context in which arguments from police abolitionists and the "defund the police" movement reverberate internationally (Vitale, 2017; Lum, Koper, and Wu, 2021). The question of how to allocate police resources to different tasks given a multitude of, at times contradictory, expectations from stakeholders like different parts of the community, local politicians, or oversight bodies is part of the day-to-day work in policing. Automating parts of this allocation then brings these tensions to the fore. This is reflected in an interview with a UK police officer in a planning function who was enticed by the idea of prioritising police work by harm as reflected in the Cambridge Harm Index, a simple measure reflecting the sentence length associated with a crime. During the interview, he quickly realised that other aspects such as community perception of crime, confidence in the police, and urgency of incidents would not be adequately reflected in the score. The "wicked problem" (Rittel and Webber, 1973) of policing does not have a singular problem description. There is a multiplicity of goals and therefore no single correct measure: "What is the goal? What are you trying to achieve? Everybody has a different view" (UK Detective Sergeant).

The core idea for predictive policing is that the purpose of police patrol, a central policing task, is to deter crime through police presence. Delivering the right "dosage" at the right time would maximise deterrence and prevent crime. Just as in the case of the Cambridge Harm Index above, this means prioritising some things over others: it assumes that the use of police time for patrol is an adequate measure to address crime and superior to other strategies. Moreover, the spatial location of patrols is optimised for deterrence rather than, for example, speed of response to emergency calls or fostering community relations. It is optimised for crime that is recorded by police, and it is optimised for crime that occurs in spatio-temporal clusters. When no explicit decision is made, volume and predictability of recorded crime determine priorities – the "politics of patterns", as Kaufmann,Egbert, and Leese (2019) term it, comes into play. However, it would be simplistic to say that the "objectivity" of patterns alone always trumps other concerns. Reflecting the balancing act of prioritisation sketched out above, some companies provide police forces with the option to rank crime types according to their own priorities and assign a likelihood that patrol would affect it (a strategy that surely helps to enrol police managers).

Explicitly or implicitly, decided by companies or police managers, with or without preconfigured values – predictive policing companies influence police priorities. Should this process be a discussion behind closed doors between companies and the police? How meaningful is ranking crime types without an understanding of the underlying data on the one hand and an overview of alternative modes of policing on the other? With technologies like predictive policing, the character of policing as a practice and its accountability to a democratic process are at stake. This is both an opportunity as it can trigger a discussion around priorities in police resource allocation, and a risk when this discussion does not happen because of black-boxed, proprietary software.

Another example of the politics embedded in predictive policing is the issue of feedback loops. The main criticism of predictive policing in academic and public discourse is that, since it is based on police records, it will only reinforce pre-existing patterns of police presence in overpoliced communities and, to make things worse, add a sheen of objectivity that could lead officers to be even more aggressive in their actions (see also Narayan in this volume). This argument can, for example, be found in O'Neill's (2016) popular book *Weapons of Math Destruction* and relates to a growing body of work concerned about discrimination facilitated and amplified by algorithms (Gandy, 1993; Eubanks, 2018; Noble, 2018; Benjamin, 2019). Perhaps the most convincing evidence for the possibility of feedback loops has been provided by Lum and Isaac (2016), who replicated PredPol's algorithm. Applied to drug crimes – typically detected by the police rather than reported by the public – they found a feedback loop further concentrating existing police activity. Predictive policing companies are, of course, aware of this criticism, and PredPol has sought to dispel it with a research paper published by its founders that claims patrol following its predictions would not lead to more biased arrests (Brantingham, 2018; Brantingham, Valasik, and Mohler, 2018).

Independent of whether the predictions affect officer behaviour, there are design decisions that interviewees highlight as mitigation for a feedback loop: First, they suggest the use of call-for-service data rather than crime records for types of crimes that are often recorded through officer-initiated contacts such as traffic stops.

> We like to have a focus on only dealing with, citizen-initiated calls [...]. So reports that ended up in the [record management] system that are citizen-initiated types of calls and work towards having less and less or no officer-initiated types of calls.
>
> (Data Scientist 2)

Without officer-initiated contacts in the data, the issue of a feedback loop is largely solved. It brings, however, a new challenge in that one incident may relate to multiple calls-for-service, and the difficulty lies in filtering these out. As the data scientist describes in the example of gunshots, the data retains some messiness as it has not been pre-filtered by the police bureaucracy.

> However, we have to deal with duplicates. A lot of times, especially with gunshots, you have to deal with error in these calls, wrong calls, you know, fake calls, [...]. [...] there's this sort of, the messiness of that data.
>
> (Data Scientist 2)

Second, following ideas from risk terrain modelling (Caplan and Kennedy, 2011), not all predictor variables need to be from police data; they can also be information about the night-time economy, lighting conditions, footfall, weather, and many more. The developers argued that including these provides further protection from biases in police data (Product Manager 2 and Data Scientist 2). As an added benefit, the Data Scientist at another company argued that it provides more long-term reliability to the models, making them less susceptible to changes in patrol strategies:

> [The] more the model uses things that are not being affected by the use of the model, I think the better, you know, accuracy will remain and the kind of validity of the actions.
>
> (Product Manager and Data Scientist)

Third, one company argued that implementing some randomisation around which of the predicted areas are shown to officers would further help in preventing over-policing. This is simultaneously intended to engage officers more and make following the predictions more interesting, as discussed above.

Notwithstanding these efforts: however advanced the modelling, however carefully selected the variables, area-based predictive policing remains always associated with patrol and all its problems. As Aaron Shapiro puts it,

> Ultimately, [predictive policing] is incapable of resolving two fundamentally incommensurate but concurrent functions of the police patrol. On one hand is a view of police patrols as distributing public safety as a common good [...]. On the other is the view from marginalized

> communities, who experience the patrol as an enactment of uneven geographies of legitimacy and authority, risk and danger, harm and abuse.
>
> *(Shapiro, 2019: 469)*

This fundamental contradiction seems to be behind some of the doubts and disillusionment of employees who were not quite sure if the software they were producing was contributing to the public good. This shines through in the statement of one of the Product Specialists:

> Although our product is great because we are moving people around and we're trying to like stop saturation and all of that, they're like, we're changing that up. It doesn't mean that a little kid might not get shot in the box, like, you know, at some point in time. So it's, it's hard.
>
> (Product Specialist 2)

A Product Specialist and a Software Developer expressed their hope that the tracking data gathered through their software could be used to identify factors such as the number and type of calls-for-service answered by an officer or their driving speed to predict and prevent mistakes and shooting incidents caused by high levels of pressure and emotional stress. Yet, these kinds of questions are not the main interest of the customer; "the focus tends to be on crime reduction" (Product Manager 2). Addressing the problems of police patrol is difficult and not a priority, as this Product Manager explained,

> The harm caused by police events […] is probably the less documented or it's not as easy to measure in some way. If we, you know, potentially if you look at survey data of the community in terms of what is your general perception of the police, how has that changed over time in some way? Or a number of looking at the counts of incidents where the police are, you can look at police shootings, you can look at like kind of violent interactions or sort of dangerous interactions with the police. […] We haven't done anything like that yet. It's just kinda been like, 'what's the most, what's the easiest, the lowest hanging fruit', essentially, like in terms of determining effectiveness. Well, we can look at, do we have a reduction in crime? Well, yes, we did. That's a good thing. That's kind of what the police departments are focused on.
>
> (Product Manager 1)

Thus, even when companies are well-intentioned and have ideas for improving policing, their customers, police departments, seem to show little interest in a product that provides more than the promise of crime reduction. The control that predictive policing companies have over police work is either opaquely produced through the way they select and weight variables in their statistical models or is closely aligned with the management goal of controlling patrol. Predictive policing reduces the multiplicity of goals associated with police patrol (deterrence, proximity to incidents for emergency response, building of community relations, and more) to the goal of deterring street crime through police presence and fixes this strategy in software design. Simultaneously, it automates the processing and interpretation of crime data and thereby poses a risk for police to lose some of their intimate knowledge of their data and an understanding of crime patterns – a knowledge lock-in in addition to the technology lock-in discussed earlier.

Discussion and conclusions

The literature on area-based predictive policing has extensively dealt with unpacking the black box, examining in detail its various elements, and highlighting the risks of bias and discrimination from amplifying existing problematic police practices (Egbert and Leese, 2020; Brayne, 2021). What this chapter contributes is a critical discussion of the role of private companies in this assemblage. Drawing on ideas from science and technology studies literature on infrastructure, innovation, maintenance, and repair (Star, 1999; Graham and Thrift, 2007; Denis and Pontille, 2019), it has highlighted the often invisible maintenance work and iterative change that underpins predictive policing. It has argued that the ability to provide this infrastructure work at a distance through cloud services can privilege private companies when police departments do not have the technical capabilities for this work. Companies can profit from economies of scale and build and maintain infrastructure developed with innovation funding from the state because providing their services through the cloud means they can deal with most of the infrastructure in one place. This also allows them to add extra features to their software that make predictive policing more amenable to patrol management processes that tie into the authority of senior officers by tracking officers' actions and whereabouts. While larger police forces might have the capacity to hire software developers to maintain a similar infrastructure, many police forces do not have the necessary resources.

The backstage, technical work is not just innocent "plumbing" but, as the second part of this chapter has demonstrated, means that private companies become entangled in the politics of policing. This is not to say that the interviewees were not genuinely concerned about the consequences of their software and tried to address common criticisms of predictive policing. But this chapter questions whether these deliberations should be had in opaque interactions between police and companies shielded by claims to intellectual property rights which has been widely criticised (Joh, 2016; Ferguson, 2017; Raso *et al.*, 2018). Political decisions on police priorities become fixed in the infrastructure of predictive policing: the imagined purpose of patrol is deterrence, crime that is predictable because of its spatio-temporal concentration becomes a priority, and so on. It replaces a multifaceted analysis of crime patterns that asks why crime happens with an automated conclusion informed by rational choice theory that it must be the lack of "capable guardians". One interviewee criticised the superficiality of this form of analysis:

> So, it's all very well, if you send a cop into that red square, red grid at that time and the evidence base shows a five percent reduction; that's not a root cause, dealing with a root cause, it's kind of like being a ready mixed plaster on top.
>
> (UK Police Business Intelligence Manager)

Fixing priorities in infrastructure limits the ability to shift priorities in accordance with the multiplicity of values that are negotiated in police resource allocation – driven, among other factors, by communities, local politics, the news cycle, and shifts in legislation. Moreover, automating the epistemic work of resource allocation means that police departments outsource a central epistemic function of analysing trends and patterns in crime. Without the institutional knowledge of regular engagement with crime numbers, alternative ways of interpreting crime patterns cannot develop.

This chapter is thus a call not to separate the political economy of "boring" infrastructure from the exciting shifts in knowledge production afforded by new technologies variously referred to as AI, machine learning, and big data. The question of who maintains infrastructure has consequences for who makes the political decisions about what this infrastructure does and will do, as highlighted in this chapter. Focusing on infrastructure should further open the door to questions around whether this technology is required considering the natural resources involved in keeping it running (Hogan, 2018; Crawford, 2021; Jue, 2021). Both the market for cloud infrastructure and the market for surveillance technologies are driven by the availability of capacities that are in search of customers. According to Jue (2021), the "data centre industrial complex" perpetuates itself by promoting increasing uses of data. Similarly, Hayes (2012) describes the "surveillance industrial complex" as a market in which lobbyists push the threats that their products, often developed with government funding, are supposed to address. Huang and Tsai (2022) demonstrate in the case of China how capitalist incentives can easily lead to "over-surveillance" with technological capacities exceeding expectations set out in state policy. There is thus a dual concern around, on the one hand, the technological solutionism, as Morozov (2013) calls it, of companies addressing our social problems instead of democratic politics, and, on the other hand, capitalist incentives driving some of this decision-making.

When companies provide the infrastructure for police management and, in some cases, the storage and processing of all data held by police, police agencies become dependent on these companies and are locked in technologically and epistemologically. Certainly, the New York police department's legal battle with Palantir over facilitating the transfer of results from past data analysis to their new provider, IBM, serves as a warning of the kinds of lock-in police forces can be faced with when committing to cloud-based products

(Hockett and Price, 2017). Moreover, while the cost for these systems is not always as egregiously high as news reports make it seem ($35,000–$50,000 for HunchLab and $200,000 for PredPol (Shapiro, 2019: 462), but $3.5 million for Palantir (Hockett and Price, 2017)), these costs are charged annually. Depending on the type of arrangement – analytical tools used by police but hosted in the cloud or analysis provided and automated by companies and hosted on cloud platforms – some share of this is paid to large cloud providers such as Amazon AWS and Microsoft Azure who have simultaneously cornered the market for storing government data online. So far, the commercial provision of cloud infrastructure has gone unquestioned, but as legislation is just catching up to the problem of bias in predictive policing, it is perhaps only a matter of time before we start discussing open-source government software and ways of limiting the environmental footprint of data analysis.

So, given the costs, the contribution to an oligopoly of cloud service providers (Ofcom, 2023), and the opacity of political decisions embedded in the software design, what are the alternatives? As one interviewee from a software company suggests, a product that supposedly has such a public benefit should perhaps not be provided by a private company:

> I have some natural scepticism about [...] companies who are trying to do public benefit and make money doing it. Actually, I feel like anything that has any sufficiently broad public benefit should be regulated as a public utility. And if predictive services have this huge public benefit, then predictive services should be like regulated as a public utility and possibly socialised.
>
> (Software Developer)

As stated in the introduction, predictive policing software is produced in a variety of institutional arrangements, not all of which involve private companies. Large police forces and nationwide efforts can have the technical resources to shoulder the required infrastructure work. An example of this is the development of the National Data Analytics Solution at West Midlands Police, funded with £5 million innovation funding from the Home Office. This project includes an ethics panel consisting of local stakeholders and subject matter experts that publishes regular reports on its work (Oswald, 2022). Public scrutiny is involved from the very beginning of the development process, and the software is developed in the direction of a public purpose rather than with the perspective of making a product that sells. Even if not necessarily a radical approach, this demonstrates the possibility of alternative institutional arrangements.

With public pushback, limited evidence of effectiveness, and the European Union planning an outright ban on predictive policing, this technology may already be on its way out. But the issues discussed in this chapter apply more widely to attempts at outsourcing knowledge production in policing. The technology market for police is awash with data visualisation dashboards, automatic resource optimisation, and software that enables investigators to identify leads in unstructured data. Microsoft and Amazon advertise their cloud services to police and the wider intelligence and defence sector as secure "eco-systems" in which companies can offer software solutions as plug-ins. Examples in policing are Accenture's Intelligent Public Safety Platform running on Amazon's AWS servers, and Motorola Command Central and Genetec Citigraf running on Microsoft's Azure servers. All of these products contain assumptions about how security services should operate and automate knowledge production, thereby closing off other ways of knowing.

There are fundamental questions about the role of policing that are raised by the need to distribute limited resources, and any attempt at automating these prioritisations shines a light on their complexity. Partial solutions like predictive policing have become viable ways of allocating resources mainly because they attempt to solve the problem of turning patrol allocation into a manageable process, what Sandhu and Fussey (2020) have termed the *uberization of policing*. But the time spent on patrol could be used differently. Particularly with voices from police abolitionists becoming louder, there is a need to rethink what police do, and this should not be decided behind the closed doors of private companies.

Note

[1] Note that this epistemology does not include addressing social factors like inequality (see also Narayan, this volume).

References

Amoore, L. (2018) 'Cloud Geographies: Computing, Data, Sovereignty', *Progress in Human Geography*, 42(1), 4–24.

AWS (2023) 'AWS for the UK Justice and Public Safety, Amazon Web Services, Inc'. Available at: https://aws.amazon.com/government-education/worldwide/uk/justice-and-public-safety/ (Accessed: 19 June 2023).

Benbouzid, B. (2015) 'From Situational Crime Prevention to Predictive Policing. Sociology of an Ignored Controversy', *Champ pénal/Penal field* [Preprint], (Vol. XII). https://doi.org/10.4000/champpenal.9066.

Benbouzid, B. (2019) 'To Predict and to Manage. Predictive Policing in the United States', *Big Data & Society*, 6(1), 1–13.

Benjamin, R. (2019) *Race After Technology: Abolitionist Tools for the New Jim Code*. Cambridge: Polity Press.

Brantingham, P.J. (2018) 'The Logic of Data Bias and Its Impact on Place-Based Predictive Policing', *Ohio State Journal of Criminal Law*, 15(2), 473–486.

Brantingham, P.J. and Tita, G. (2008) 'Offender Mobility and Crime Pattern Formation from First Principles', in L. Liu and J. Eck (eds) *Artificial Crime Analysis Systems: Using Computer Simulations and Geographic Information Systems*. Hershey PA: Information Science Reference, 193–208.

Brantingham, P.J., Valasik, M. and Mohler, G.O. (2018) 'Does Predictive Policing Lead to Biased Arrests? Results From a Randomized Controlled Trial', *Statistics and Public Policy*, 5(1), 1–6.

Brayne, S. (2021) *Predict and Surveil: Data, Discretion, and the Future of Policing*. New York, NY: Oxford University Press.

Callon, M. (1984) 'Some Elements of a Sociology of Translation: Domestication of the Scallops and the Fishermen of St Brieuc Bay', *The Sociological Review*, 32, 196–233.

Caplan, J.M. and Kennedy, L.W. (2011) *Risk Terrain Modeling Compendium*. Newark, NJ: Rutgers Center on Public Security.

Colton, K.W. (1979) 'The Impact and Use of Computer Technology by the Police', *Communications of the ACM*, 22(1), 10–20.

Crawford, K. (2021) *Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence*. New Haven: Yale University Press.

Denis, J. and Pontille, D. (2019) 'Why do Maintenance and Repair Matter?', in A. Blok, I. Farías, and C. Roberts (eds) *The Routledge Companion to Actor-Network Theory*. Abingdon; New York: Routledge, 283–293.

Derrida, J. (1995) 'Archive Fever: A Freudian Impression', *Diacritics*. Translated by E. Prenowitz, 25(2), 9.

Duarte, D.E. (2021) 'The Making of Crime Predictions: Sociotechnical Assemblages and the Controversies of Governing Future Crime', *Surveillance & Society*, 19(2), 199–215.

Eck, J.E. and Clarke, R.V. (2019) 'Situational Crime Prevention: Theory, Practice and Evidence', in M.D. Krohn et al. (eds) *Handbook on Crime and Deviance*. Cham: Springer International Publishing (Handbooks of Sociology and Social Research), 355–376.

Egbert, S. (2019) 'Predictive Policing and the Platformization of Police Work', *Surveillance & Society*, 17(1/2), 83–88.

Egbert, S. and Leese, M. (2020) *Criminal Futures: Predictive Policing and Everyday Police Work*. Abingdon; New York: Routledge.

Eubanks, V. (2018) *Automating Inequality*. New York, NY: St Martin's Press.

Ferguson, A.G. (2017) *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*. New York, NY: New York University Press.

Gandy, O.H. (1993) *The Panoptic Sort. A Political Economy of Personal Information*. Boulder, CO: Westview.

Gates, K. (2019) 'Policing as Digital Platform', *Surveillance & Society*, 17(1/2), 63–68.

Graham, S. and Thrift, N. (2007) 'Out of Order: Understanding Repair and Maintenance', *Theory, Culture & Society*, 24(3), 1–25.

Hamlin, R.G., Ellinger, A.D. and Jones, J. (eds) (2019) *Evidence-Based Initiatives for Organizational Change and Development:* IGI Global (Advances in Business Strategy and Competitive Advantage). Available at: https://doi.org/10.4018/978-1-5225-6155-2.

Hayes, B. (2012) 'The Surveillance-industrial Complex', in K. Ball, K. Haggerty, and D. Lyon (eds.) *Routledge Handbook of Surveillance Studies*. Hoboken: Taylor & Francis (Routledge International Handbooks), 167–175.

Hockett, E. and Price, M. (2017) 'Palantir Contract Dispute Exposes NYPD's Lack of Transparency', *Just Security*, 20 July. Available at: https://www.justsecurity.org/43397/palantir-contract-dispute-exposes-nypds-lack-transparency/ (Accessed: 24 November 2021).

Hogan, M. (2018) 'Big Data Ecologies. Landscapes of Political Action', *Ephemera. Theory & Politics in Organization*, 18(3), 631–657.

Huang, J. and Tsai, K.S. (2022) 'Securing Authoritarian Capitalism in the Digital Age: The Political Economy of Surveillance in China', *The China Journal*, 88, 2–28.

Iliadis, A. and Acker, A. (2022) 'The Seer and the Seen: Surveying Palantir's Surveillance Platform', *The Information Society*, 38(5), 334–363.

Joh, E.E. (2016) 'The New Surveillance Discretion: Automated Suspicion, Big Data, and Policing', *Harvard Law & Policy Review*, 10, 15–42.

Jue, M. (2021) 'The Data Centre Industrial Complex', in M. Jue and R. Ruiz (eds.) *Saturation: An Elemental Politics*. Durham: Duke University Press, 283–305.

Kaufmann, M., Egbert, S. and Leese, M. (2019) 'Predictive Policing and the Politics of Patterns', *The British Journal of Criminology*, 59(3), 674–692.

Kwet, M. (2020) 'The Microsoft Police State: Mass Surveillance, Facial Recognition, and the Azure Cloud, The Intercept'. Available at: https://theintercept.com/2020/07/14/microsoft-police-state-mass-surveillance-facial-recognition/ (Accessed: 19 June 2023).

La Vigne, N.G. and Groff, E.R. (2001) 'The Evolution of Crime Mapping in the United States. From the Descriptive to the Analytic', in A. Hirschfield and K. Bowers (eds.) *Mapping and Analysing Crime Data: Lessons from Research and Practice*. London: Taylor & Francis, 203–221.

Lally, N. (2021) '"It Makes Almost no Difference Which Algorithm You Use": On the Modularity of Predictive Policing', *Urban Geography*, 43(9), 1437–1455.

Langley, P. and Leyshon, A. (2017) 'Platform Capitalism: The Intermediation and Capitalization of Digital Economic Circulation', *Finance and Society*, 3(1), 11–31.

Linder, T. (2019) 'Surveillance Capitalism and Platform Policing: The Surveillant Assemblage-as-a-Service', *Surveillance & Society*, 17(1/2), 76–82.

Lum, C., Koper, C.S. and Wu, X. (2021) 'Can We Really Defund the Police? A Nine-Agency Study of Police Response to Calls for Service', *Police Quarterly*, 25(3), 255–280.

Lum, K. and Isaac, W. (2016) 'To Predict and Serve?', *Significance*, 13(5), 14–19.

Maguire, M. (2018) 'Policing Future Crimes', in M. Maguire, U. Rao, and N. Zurawski (eds.) *Bodies as Evidence: Security, Knowledge, and Power*. Durham: Duke University Press, 137–158.

Manning, P.K. (2008) *The Technology of Policing: Crime Mapping, Information Technology, and the Rationality of Crime Control*. New York: New York University Press (New perspectives in crime, deviance, and law series).

Marda, V. and Narayan, S. (2020) 'Data in New Delhi's Predictive Policing System', in *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency*. New York, NY: Association for Computing Machinery (FAT* '20), 317–324.

Mazzucato, M. and Collington, R. (2023) *The Big Con: How the Consulting Industry Weakens our Businesses, Infantilizes our Governments and Warps our Economies*. London: Allen Lane.

Microsoft (2023) 'Public Safety and Justice Solutions'. Available at: https://www.microsoft.com/en-gb/industry/government/public-safety-and-justice (Accessed: 19 June 2023).

Morozov, E. (2013) *To Save Everything, Click Here: The Folly of Technological Solutionism*. New York, NY: PublicAffairs.

Noble, S.U. (2018) *Algorithms of Oppression: How Search Engines Reinforce Racism*. New York: Combined Academic Publ.

Ofcom (2023) 'Ofcom Proposes to Refer UK Cloud Market for Investigation', *Ofcom*. Available at: https://www.ofcom.org.uk/news-centre/2023/ofcom-proposes-to-refer-uk-cloud-market-for-investigation (Accessed: 13 June 2023).

O'Neil, C. (2016) *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. London: Allen Lane.

Oswald, M. (2022) 'A Three-pillar Approach to Achieving Trustworthy and Accountable Use of AI and Emerging Technology in Policing in England and Wales: Lessons from the West Midlands Data Ethics Model', *European Journal of Law and Technology*, 13(1), 1–27.

PredPol (2021) 'Geolitica: A New Name, A New Focus', *Predictive Policing Blog*, 2 March. Available at: https://blog.predpol.com/geolitica-a-new-name-a-new-focus (Accessed: 18 May 2022).

Raso, F. *et al.* (2018) *Artificial Intelligence & Human Rights: Opportunities & Risks*. Berkman Klein Center for Internet & Society. Available at: http://nrs.harvard.edu/urn-3:HUL.InstRepos:38021439 (Accessed: 11 February 2020).

Ratcliffe, J.H., Taylor, R.B. and Fisher, R. (2019) 'Conflicts and Congruencies between Predictive Policing and the Patrol Officer's Craft', *Policing and Society*, 30(6), 639–655.

Rittel, H.W.J. and Webber, M.M. (1973) 'Dilemmas in a General Theory of Planning', *Policy Sciences*, 4, 155–169.

Sandhu, A. and Fussey, P. (2020) 'The "Uberization of Policing"? How Police Negotiate and Operationalise Predictive Policing Technology', *Policing and Society*, 31(1), 66–81.

Shapiro, A. (2019) 'Predictive Policing for Reform? Indeterminacy and Intervention in Big Data Policing', *Surveillance & Society*, 17(3/4), 456–472.

Srnicek, N. (2016) *Platform Capitalism*. Cambridge, UK; Malden, MA: Polity Press.

Star, S.L. (1999) 'The Ethnography of Infrastructure', *American Behavioral Scientist*, 43(3), 377–391.

Star, S.L. and Ruhleder, K. (1996) 'Steps Toward an Ecology of Infrastructure: Design and Access for Large Information Spaces', *Information Systems Research*, 7(1), 25.

Thomas, T. (2007) *Criminal Records*. London: Palgrave Macmillan UK.

Tulumello, S. and Iapaolo, F. (2021) 'Policing the Future, Disrupting Urban Policy Today. Predictive Policing, Smart City, and Urban Policy in Memphis (TN)', *Urban Geography*, 43(3), 448–469.

Vitale, A.S. (2017) *The End of Policing*. London: Verso Books.

Waardenburg, L., Huysman, M. and Sergeeva, A.V. (2022) 'In the Land of the Blind, the One-Eyed Man Is King: Knowledge Brokerage in the Age of Learning Algorithms', *Organization Science*, 33(1), 59–82.

Waterton, C. (2010) 'Experimenting with the Archive: STS-ers As Analysts and Co-constructors of Databases and Other Archival Forms', *Science, Technology, & Human Values*, 35(5), 645–676.

Whitson, J.R. (2013) 'Gaming the Quantified Self', *Surveillance & Society*, 11(1/2), 163–176.

Wilson, D. (2019) 'Platform Policing and the Real-Time Cop', *Surveillance & Society*, 17(1/2), 69–75.

Wilson, D. (2020) 'Predictive Policing Management: A Brief History of Patrol Automation', *New Formations: A Journal of Culture/Theory/Politics*, 98(1), 139–155.

Wilson, D. (2021) 'The New Platform Policing', in A. Završnik and V. Badalič (eds.) *Automating Crime Prevention, Surveillance, and Military Operations*. Cham: Springer International Publishing, 47–68.

8 Machine learning and artificial intelligence in counterterrorism

The "realities" of security practitioners and technologists

Mark Maguire and David A.Westbrook

Introduction

At approximately 09:24, on 28 February 1997, two armed robbers, Larry Phillips Jr. and Emil Matasareanu exited the North Hollywood branch of Bank of America, leaving terrified customers in their wake. They were confronted by waiting police, but they stood their ground and opened fire with assault rifles. Protected by homemade body armour, the two robbers behaved as if they were invulnerable. Officers ducked for cover behind squad cars only to see their vehicles disintegrate in a hail of bullets. Several officers made for a nearby gun store to plead for heavier weapons. Eventually, at 09:42, help arrived in the form of a rather casual-looking "SWAT" (from "Special Weapons And Tactics") team. The team was called up during a barbecue, and several members arrived in shorts and sneakers. But the SWAT specialists quickly turned the tide. Phillips, wounded, turned his gun on himself. Matasareanu fought on, despite taking several rounds to his body armour. Then a SWAT officer "skipped" bullets beneath a car, striking Matasareanu below his armour, and causing him to bleed to death.

The North Hollywood shooting lasted nearly 45 minutes and was recorded by circling news helicopters. The footage is spectacular, cinematic. It is regularly played on projector screens in counterterrorism training events to stimulate discussion of tactics. The audience is presented with a scene without context. The film is "the" reality on the table, albeit of a particular kind. The North Hollywood shooting speaks to security adepts as they train, learn, and so constitute the discipline of security. The constant replaying of footage of the event exemplifies the curation of an ideal-type reality within the expert domain of counterterrorism, and the closing of the mind to alternative possibilities. Security expertise, like all "disciplines" has an epistemology, which is inherently problematic, given the stakes. But it is not just film that shows, frames, and constrains the way we can think about a problem within a professional world. Today we must also worry about the growing intrusion of experimental technologies into this domain, which tend to add further layers of dangerous abstraction. It is therefore important to attend to the ways that security training and technology innovation are intersecting.

DOI: 10.4324/9781003412908-11

This chapter extends from our larger project on counterterrorism (see Maguire and Westbrook, 2020). We examined public behaviour during terror attacks in the UK, France, Ireland, and Kenya. Here, we will dwell on a specific French example, the foiled 2015 terrorist attack on the Thalys train from Amsterdam to Paris. Because of the paucity of cross-cultural research on emergency management, security bureaucracies welcomed our project, so participation in various meetings and joint training exercises was encouraged. We have already written about the roles of police and military special forces "operators" (see Westbrook and Maguire, 2019; Maguire and Westbrook, 2020, 2021). Such forces are glorified, emulated, and when it comes to equipment, no expense is spared. Indeed, having "the teams" adopt a new technology all but guarantees the commercial success of the product.[1] Though small in number, special forces have an outsized role in technological and material innovation in the security sector.

Elite teams train in secret, but their doors regularly swing open for arms and other technologies companies pushing the latest gadgetry. Training workshops and joint exercises often end with a formal opportunity to view the latest hardware and software. Retired members of elite police or military units are sometimes recruited by companies to sell products and services to their former employers. It is easy to observe the so-called corporate push, but some technologies are adopted while others are not. Solutions, after all, must address specific problems or better "problematizations", challenges that are acknowledged in expert communities of practice. As we shall show, counterterrorism, as bureaucratically organised violence, is converging with a broadly sympathetic style of reasoning coming from technologists. In this emergent space, complex social challenges are often simplified, and difficult moral problems are elided. We use unique data on the 2015 Thalys terror attack and introduce the concept of "boxology" to illuminate the conjuncture between two questionable versions of reality.

The discipline of security

> I simply tried to focus on my three-foot world. My job wasn't to complain; my job was to clear that compound under the orders we were given.
>
> — Navy SEAL Chief Matt Bissonnette

Members of elite military and police teams cultivate extraordinary martial prowess. Reputations – and this is a world in which reputations really do matter – are forged by displays of Olympian athleticism and preternatural mental resilience. But the small psychological literature on special force members also shows selection in favour of problem solvers and, especially, team workers (Stanton, 2011). Teams work together to solve problems using secrecy and surprise, cunning, and, of course, aggression. This is well known.

But there are also more subtle attributes, specific "styles of reason" (Hacking, 1992) that are as effective as any physical weapon.

Special forces, in our ethnographic experience, speak about narrowing their vision when confronted with chaos, imposing a small controllable "reality" onto the chaotic real world. There are a few public statements on this topic. For example, in *No Hero* (2014), quoted in the above epigraph, Navy SEAL Chief Matt Bissonnette, writing under the pen name Mark Owen, popularised the term "three-foot world". In contrast to the 30,000-foot view of strategists and politicians, the operator, he explains, must control chaos by implementing the three-foot world that she or he can affect. Similarly, we spoke to operators who described moments during violent action when they paused, "hit the reset button," and asserted control over their milieu, sorting friends and civilian "sheep" from the evildoers. One individual, an elite police officer involved in the fatal shooting of armed attackers, could recall only the persons and things of that he had been trained to see, a car with armed individuals, innocent civilians. Everything that lacked significance slipped from view. All that remained, at least in his memory, was a "scene" composed of facts, his act of violence, and the expected actions and reactions that followed.

When thinking of the trained actions and responses of elite military and police, one is tempted to reach for Michel Foucault's (1977) work on military "discipline," Marcel Mauss's earlier "Techniques du Corps," or recent ethnographic work on "skill". But Foucault moves gadfly-like across ostensibly different societal domains in order to illustrate general power-knowledge configurations. From Foucault, we learn that the military barracks resemble the school, hospital, and prison, but we learn little about the actual competencies developed in specific barracks. Mauss, for his part, conflates efficiency and effectiveness, a rather elementary misstep.[2] At first blush, "skill" seems to be a spongy term, but anthropologists have recently used the notion of "skilled vision" to illuminate the world of security professionals (Maguire, 2014) and other experts (Grasseni, 2007).

Skilled vision denotes the development of embodied and tacit competence, including acquired assumptions about the world, and biases and preferences, often supported by a formal body of knowledge, a "discipline". As one might suspect, it is hard for members of a community of practice to explain their skilled vision to uninitiated outsiders, to find the right words, and yet similarly competent individuals who have been through the apprenticeship simply "get it". But the realm of skilled vision, at least in counterterrorism, is not permitted to remain elusive, untranslatable. Anthropologists have certainly demonstrated that significant levels of opacity are common in skilled sociality, even in apprenticeships (e.g., Hanks, 2006), but in the example here opacity is punished by practice, and inscrutable fellows are not and cannot be included in elite teams. It is necessary for members of a team to "get it", but a common language with outsiders such as military planners, emergency professionals, and external agencies is also needed. Borrowing from Gregory Bateson (1972), Erving Goffman (1974) uses the simple term "frame" to articulate how groups stabilise the world to enable the deployment of embodied cognitive resources and in so doing transform the world, making it actionable even if fundamentally uncertain.

We are proposing that the discipline and skill of operators are available in and communicated through purposeful efforts to frame reality. The question becomes: what does such framing look like in practice?

Here we are speaking of elite soldiers who operate in milieus of constant, often frugal innovation, where style and efficiency yield to brutal effectiveness. And because of the high cost of innovation in their world – failure may involve capture, torture, and death, if one is lucky – the elite soldiers' frame, the "three-foot world", has acquired an air of profundity, insight, rather than communicating uncertainty. Indeed, Chief Bissonnette's term names and describes a combat team's emphasis on span of control over an operational field that is composed of facts. A fact here acquires meaning with reference to a known scenario, or it may be new information pressed into a narrow frame. In short, there is a narrowing of vision, such that reality becomes a milieu of knowable actions and reactions, a box.

Footage of the North Hollywood shooting is played in training sessions, while actual operations resemble the North Hollywood shooting. Of course, the creation of cognitive frames – both narrowing and enabling – through the interplay of training and experience is hardly new. Recall Roman historian Josephus said of the legions, "Their training is bloodless battle, their battles are bloody training". But we are not discussing strategy and tactics on the field of Mars here; rather, we are discussing the style of reason that underpins the deployment of kinetic force in a world populated by civilians.

Boxology

> Certain forms of knowledge and control require a narrowing of vision. The great advantage of such tunnel vision is that it brings into sharp focus certain limited aspects of an otherwise far more complex and unwieldy reality. This very simplification, in turn, makes the phenomenon at the centre of the field of vision more legible and hence more susceptible to careful measurement and calculation. Combined with similar observations, an overall, aggregate, synoptic view of a selective reality is achieved, making possible a high degree of schematic knowledge, control, and manipulation.
>
> James Scott, *Seeing like a State*

We carried out our research in Kenya, the UK, Ireland, and France, the latter example being explored in detail further below. Each jurisdiction had specific counterterror forces, the shadowy obverse side of modern bureaucratic order. In any one jurisdiction, a patrol police officer might be the first to respond to a major incident, but soon an alert travels to, say, Ireland's Emergency Response Unit (ERU) or to London Metropolitan Police's MO-19. A major incident alert would also go to military specialists such as the Irish Army Ranger Wing (ARW) or Britain's 22 Special Air Service (SAS). Such units sometimes train with each other and with other "friendly" forces (for a long time, for example, the ARW and SAS were interoperable, and British forces train Kenya's counterterror Recce Squad). In this small world, an "operator" is expected to deliver kinetic force in a flexible yet highly organised manner, an agile (bureaucratic?) service. French counterterrorism, perhaps unsurprisingly, elevates bureaucratic violence to a quasi-academic level, which merits discussion, and underscores the overall point we make here.

Should there be a major incident in Paris, municipal police will yield control to the Police Nationale's specialist unit, Recherche, Assistance, Intervention, and Dissuasion (RAID) or to their sister unit in the Gendarmerie, Groupe d'Intervention de la Gendarmerie Nationale (GIGN). In 2019, Mark, one of the authors, attended a closed counterterror workshop in the UK. RAID senior staff were guests of honour and presented details of their "methodology". They focused on an infamous incident in Dammartin-en-Goële three years earlier. The incident occurred in the wake of the Charlie Hebdo massacre by, among others, brothers Saïd and Chérif Kouachi. In the days after the massacre, the fugitive Kouachi brothers entered the offices of a signage company by impersonating police officers and proceeded to hold employees hostage at gunpoint. GIGN and RAID officers surrounded the building and established a series of concentric "boxes". In these boxes, persons and things are expected to conform to rigid, scenario-based proformas or be eliminated. The outermost box is the *cordon sanitaire*, protected by snipers. The next, smaller box is the operational milieu of joint forces. The innermost box is the jurisdiction of special forces. A plan is formed, and the plan is displayed as a diagram of and for reality.

The innermost box contains the terrorists and sometimes, unfortunately, their civilian victims. It is, essentially, a kill zone, and its occupants – including the hostages – are categorised as, to quote one senior RAID officer, the "already dead". Humans become facts, "the raw meat of history", to borrow from Albert Camus. This is worrying, not least for liberal democracy. Yet, in Europe, airports and other critical infrastructure sites have played scenarios through and contemplated shuttering off sections of buildings in the event of a major terror incident, effectively locking civilians into boxes with their attackers until armed assistance arrives to "resolve" the situation.

But there is more to worry about than secretive counterterror units operating in the shadows. We must also worry about the rise of AI and X Reality technology, and the intrusion of these technologies into counterterrorism – technologies for control in the search for an imprimatur.

X in a box

We are witnessing today the intrusion of X Reality systems into counterterrorism. X Reality is sometimes referred to as extended reality or simply as XR. The X here commonly denotes distinct but allied technologies: augmented, mixed, assisted, and fully virtual reality systems.

Each of these systems, to varying degrees, uses machine learning and other forms of artificial intelligence. Depending on the generosity of the listener, then, X Reality is either a useful umbrella term for a superset of technologies or an unreadable label for a chaotic collection of incompatible gadgetry.

Of course, some of these technologies have matured over long periods of time. Science fiction writer Stanley Weinbaum's 1935 essay *Pygmalion's Spectacles* fully anticipates virtual reality headsets. In 1961, the famous photographer Charles Wyckoff filed a patent for extended reality film to render nuclear explosions visible. Wyckoff later, allegedly, photographed the Loch Ness monster, a strange detour on the road to the first functioning virtual reality headset in 1991 (see Mann, 2001). Artificial intelligence also has a considerable pedigree. Its theoretical foundations were set by post-WWII Defence Advanced Research Projects Agency (DARPA)-funded projects, and it has been weaponised and used earlier, especially in artillery strikes and air force missions. (One could argue that the USSR's RYaN programme, which scanned US activity for "signs" of a possible nuclear strike, anticipates much of military AI's logic today).[3]

A sample of current AI military capability was available during the summer of 2021 in the US Northern Command's (NORTHCOM) Global Information Dominance Experiments which brought together AI-enabled tools from around the world, especially a cloud-based collaboration tool called Cosmos, a threat alert system called Lattice, and a data-rich "awareness tool" called Gaia. There is much handwringing about the role of Big Tech in air force AI projects, but Algorithmic Warfare is still immature, with the most generous commentators comparing NORTHCOM experiments to building the bicycle while riding it. Nonetheless, AI and X Reality are widely used in visualisation. After all, battlefields are hard to see, and there is an enormous advantage to adopting, essentially, a smart screen with data depth and action alerts. The goal is to replace Napoleon's *coup d'oeil,* the glance of the military genius, with the most relevant and up-to-date information, legible to lesser and more prevalent minds. There are numerous challenges here, not least understanding what's in the "black box" of modern artificial intelligence systems. Today, this challenge is framed as "the opacity problem", or "the problem of explainability" – how can one trust the answer given by the machine if one cannot understand where the answer came from (see also Maguire, 2018)? In military command, explainability is a sincere problem, because command must be exercised over dynamic situations, and multiple overlapping and uncertain three-foot worlds. The crisis commander in an anti-terror incident is also expected to use the latest technology and data, but, much like the military commander, he will eventually yield to the chaos of conflict, the fog of war, as Clausewitz had it, through which the dogs move.

The US Department of Defence AI Strategy (2019) imagines a future of warfare with artificial intelligence offering enhanced decision-making. But this is just one stream of techno-scientific development. The future of war will also include AI-enabled "symbiotic" man–machine systems, according to the Pentagon. These systems emerge from use, they require use, and thus, perhaps, resolve the "problem of explainability".

So, how are X Reality systems used in counterterrorism? The United Nations Office of Counterterrorism provides a clear statement on this:

> AR and VR technologies have the potential to become effective tools in the global fight against terrorism. AR/VR provides a cost-effective, rapid training solution used globally, and will one day be ubiquitous within training packages. … Moreover, these technologies can increase coordination in post terrorist attacks environments, enabling first responders to have a wholistic understanding of complex terrorist scenes. Such technology is already being tested in border security, emergency management, and criminal investigations.
>
> (UNOCT, 2021: 2)[4]

There is ample evidence that X Reality is making inroads in military command structures, using AI to aggregate and visualise patterns and signals; this is happening coterminous with an AI revolution in logical (cyber) and physical security. But, speaking specifically about the kinetic end of counterterrorism, our experience chimes with the view expressed by the United Nations Office of Counterterrorism: AI-enabled X Reality is intruding into anti-terror training, pre- and post-incident, nesting happily as yet more boxology.

Since 2017, we have attended multiple showcases, demonstrations, and training events where X Reality systems were put on display. During a quasi-academic event in Estonia in 2017, Mark was invited to test one "near-to-reality" system in a hotel. The system was a headset that promised visualisation of data and "terrorist" avatars. After several false starts, frank admissions of failure accompanied by fits of laughter from the commercial operator, the headset brought to life a ghost-like figure on the ground near a sofa. "Is he moving?" the commercial operator asked in response to Mark's description of the figure. "No? Well, you never know with these terrorists! (more laughter)". And, indeed, the most sophisticated bleeding-edge X Reality does have the power to amuse, but the systems are improving, rapidly.

During the same event, and again one year later, Mark met the founder and CEO of a major X Reality company, who was already selling into the counterterrorism and emergency management market. The product he offered was a sleek video-game-like training experience where multiple users could log on from anywhere in the world and play the role of emergency workers, police, or even anti-terror forces, on the ground or in command, and deal with a terror event or post-event response. For example, one could take on the role of a police officer in an airport who is confronted by a mass casualty event. AI, Mark was told, "scrapes" data from real scenarios and responds to users' actions and decisions to add "layers" of new micro-scenarios, and so the platform "evolves". During a demonstration, a scene unfolded in front of Mark on the platform's screen, and the CEO described how a police officer might make a decision based on what is visible, a drop-down menu of training advice, and new data introduced via "comms". But when asked about the civilian avatars in the visualisation, timing, speed, and several other basic matters, the CEO revealed that the "scenarios" used were in fact news reports read by his software engineers or videos found online. Engineers call this "under-specification". In plain terms, no actual participants in an actual terror incident were ever interviewed. Yet, to be clear, everything in the box felt real.

As explained earlier, this chapter extends from our larger project on counterterrorism (see Maguire and Westbrook, 2020). One of our goals has been to examine public behaviour during terror attacks in Kenya, the UK, Ireland, and, as elaborated in detail here, France. This work involved sitting down with members of the public to understand where they were on a fateful day, what they saw, and what they did. As it happens, we also drew boxes and cognitive maps to help us delimit the specific spaces and understand experiences. Here we indicate what actual terrorism looks like from the perspective of those involved, juxtaposed against the martial order of things and the technological rendering of reality.

Reality unboxed

At 17:45 on 21 August 2015, a young man named Ayoub El Khazzani exited the WC in Carriage 12 of the Thalys train from Amsterdam to Paris. El Khazzani was stripped to the waist and brandishing an assault rifle and a Luger pistol (he carried 900 rounds of ammunition in a backpack). His mission, as he saw it, was to murder as many people as possible, ideally overseas American servicemen and European bureaucrats. We interviewed almost everyone boxed in with the terrorist on Carriage 12 that day, El Khazzani's intended victims.

On seeing him emerge from the WC, a Thalys employee ran away and locked himself in a luggage compartment. But El Khazzani was challenged first by a Frenchman who remains anonymous and then by 51-year-old Mark Moogalian. He overpowered both men, gravely wounding Moogalian. Sixty-two-year-old Christopher Norman instantly recognised the severity of the threat. He had grown up in South Africa and spent time in Kenya. Guns sound the same the world over.

> My first thought was, 'Oh my God, it's happening to me'. … You know I remember the Tunisia thing, immediately before it, where people

> didn't get up and do anything and basically they were all shot down anyway. So, my thinking was you know what do I do, how do I react in relation to this? Is there anything I can do that will basically save our lives? At the same time being very, very scared. So, I was kind of trying to get myself ready to do something but I didn't know whether I was going to do anything or not and then.
>
> (Interview, 2019)

Ten metre further down the carriage, US servicemen Anthony Sadler, Alek Skarlatos, and Spencer Stone sat together. Here is Spencer Stone's account of what happened next:

> So, you know, I was initially woken up by the train employee running past me. … And then I looked at Alek and he was kind of looking towards the back of the train and then he kind of had, like, a shocked, you know, look on his face and then I looked at Anthony and he was just kind of like still looking up and kind of had the same look, like what the heck is going on? I took my headphones and I heard glass breaking, people screaming, and then I turned around and looked behind me and the first thing I see is a guy coming in to our train car bending down picking up the AK and he's trying to load a round in and, you know, I noticed he was kind of like … something was going on with this guy. … So I pretty much took it upon myself, because I just thought our time was running out, that I'd make a move, pretty much, and so I just took off in a full sprint down the aisle towards him and then, you know, I could hear him trying to work the gun again and even more like he actually ended up pulling the trigger on me but there was a bad timer on the bullet so it gave me more time to be able to make it to him, which is like probably the biggest miracle in the whole story.
>
> (Interview, 2019)

Alek Skarlatos takes up the narrative from here:

> Spencer tackled the guy. I caught up to him. We fought with him for a little bit. Then basically Spencer finally got him in a chokehold, and once he got him in a chokehold, the terrorist then pulled out a handgun to try to shoot him with it. I was standing right in front of him, so I pulled the hand gun from out of his hand before he could shoot anything and then put it to his head and told him to stop resisting. He didn't, so I pulled the trigger and the chamber was empty. So, then, I basically just threw it and then I picked up the AK that was on the ground, because I think Spencer was getting stabbed around this time, so I tried to shoot him with the AK but it was on safe so instead of messing with it anymore I just started to hit him in the head with the muzzle.
>
> (Interview, 2019)

Some commentators don't like to hear about "have-a-go heroes". Perhaps it plays to macho illiberal politics. But facts matter. In all of the terror attacks we studied, civilians attempted various interventions, from grappling with armed terrorists to organising medical care. Leviathan, in the form of highly trained counterterror operators, was invariably late to the scene. This is of great significance, then, because even in the box that was Carriage 12 of Thalys train 9364, behaviour was unexpected and full of lessons for public safety. The US servicemen rushed to prevent a terror attack and did so relying on military training, recreational martial arts, and early socialisation in the United States, where the threat of "active shooters" is present, expected even. The US servicemen subdued the terrorist, cleared the carriages in expert fashion, and saved the life of gravely wounded Mark Moogalian using their basic battlefield medical training. By the time counterterror police took charge, the situation was neatly tied up, literally.

Lessons learnt from Thalys included the need to better train frontline staff and the need to have advanced first aid kits onboard trains. But, unsurprisingly, corporations selling X Reality solutions to transport providers, like the global BMT Group, push for investment in "flexible simulation" platforms rather than investments in low cost but effective measures like better first aid kits.[5] And, to continue the juxtaposition, counterterror operators prefer to train to face heavily armed North Hollywood bank robbers rather than face the fact that actual terrorism is dysfunctional, messy, hard to train for, and the kind of thing that will be over before you arrive to save the day.

All of this gestures to a deep problem in the intrusion of X Reality into the boxology of counterterrorism. Our investigations of the Thalys train attack, the 2013 Westgate Mall attack in Nairobi, or the terror incident in London's Borough Market in 2017, and other incidents showed an extraordinary gulf between perceptions about public behaviour and the unboxed realities on the ground. Terrorists struck, the public reacted, from have-a-go-heroes to the selfless individuals who saved others, some froze, others panicked, and yet one could piece together all the stories into an account. One could tell truths about humans, and learn lessons about how to save lives. But counterterror bureaucracies wish to segment reality in order to rationalise expenditures and training, and ultimately the actual deployment of force. For-profit corporations wish to simulate a reality based on guesses that just happen to be addressed by their products, rather than use actual data with all its messy details, contradictions, and uncertainties. The danger in the intrusion of X Reality systems is that it will represent an incorrect version of reality to individuals whose job it is to use deadly force, and to the civilian world in which such force is exercised.

Conclusions

On one level, we have shown that there is a deep problem in contemporary counterterrorism: a limited and limiting style of reasoning that is potentially dangerous for democratic societies and which lends itself to technological gimmicks. But one cannot simply offer abstract criticism and nothing else in the face of a problem in the world of security. Firstly, because this is a deadly serious context, and, secondly, because today's "bleeding-edge" gimmick is tomorrow's cutting-edge, must-have kit.

Of course, critique is certainly possible and valuable: if one reduces counterterror violence to a series of boxes, one excludes the experiences of those who were there, including the terrorists who created the box. The likely effect of what we are calling boxology is to reduce time, space, and options. Moreover, in order to train, the box reproduces what is known, and therefore what is knowable, closing knowledge in with the expert. One could easily here make reference to Hannah Arendt's comments on bureaucratic "thoughtlessness" and "remoteness from reality" (Arendt, 1963). And yet, some sympathy is required here. What else can one do? Everyone complains about security measures until a white nationalist, Al Shabaab member, or some other unknown person demonstrates that there wasn't enough security. Lives are lost, people are blamed, and careers end. Counterterrorism must engage in reasonable actions with the aim of countering terrorism. X Reality promises something in a context where the most reasonable response is probably to do nothing at all. The question, then, is how to think about an intellectual response beyond critique, one that understands the demands of the day.

Today, scholars and activists are exposing the biases and errors encoded in security technology (e.g., Ferguson, 2017; Sandhu and Fussey, 2021), and some researchers are already looking to a future of interoperable, platform-based technologies that are imbricated with securitarian styles of reason (e.g., Leese and Egbert, 2020). This chapter is a call for more attention to how technologies nest in the security landscape alongside existing and sympathetic frames. When it comes to security, all too often we see only a "sketch of the façade", to borrow from Arthur Schopenhauer (1958: 128), but to understand the adoption of security technology – here AI, and X Reality technology – we must attend to the structures, meanings, and styles of reason behind the façade.

Notes

[1] In the United States, the image of the special forces operator is very powerful, and so the endorsement of a product by battle-hardened Teams is a coup for any equipment producer. There is a trickle-down effect within the military, with lower-tier units wishing to emulate their heroes. And there is a trickle-out effect too, as law enforcement becomes, in the USA and elsewhere, ever more reliant on Special Weapons and Tactics (SWAT) teams. In the USA, the FBI alone has over 1,200 SWAT officers, and 85% of all towns with populations between 25,000 and 50,000 persons have their own SWAT team (see Balko, 2013). The "public" special operator equipment market is enormous (the private market is enormous too: today people hunt deer dressed head-to-toe as special forces soldiers, and increasingly operator endorsement is a requisite for success in the Airsoft

equipment market). Moreover, because the so-called Pentagon Pipeline (the 1033 Program, curtailed by the Trump administration) has funnelled $16 billion worth of military equipment to law enforcement since 9-11, there is considerable churn in procurement. This is just the United States. Security is a global industry: from Kabul to Kiev, generic special forces equipment is widely available.

[2] On numerous occasions, Mauss conflates terms and offers a suggestive but ultimately specious analysis. For instance:

> The techniques of the body can be classified according to their efficiency, i.e. according to the results of training [*résultats de dressage*]. Training [*le dressage*], like the assembly [*le montage*] of a machine, is the search for, the acquisition of an efficiency. Here it is a human efficiency. These techniques are thus human norms of human training [*dressage humain*]. These procedures that we apply to animals men voluntarily apply to themselves and to their children. … As a result I could to a certain extent compare these techniques, them and their transmission, to training systems [*à des dressages*], and rank them in the order of their effectiveness.
>
> (Mauss, 1973: 77–78 [my emphasis])

In the specific example here of the application of kinetic force, a special forces team may be ranked in terms of efficiency by delivering maximum damage for relatively low cost to the military – think here of a small team of saboteurs delaying an advancing enemy. But extraordinary time, effort, and resources are often committed to special forces because effectiveness, though costly, is worth the expense in a realm that prizes results above all.

[3] During the Vietnam War, the US attempted to disrupt the real-and-imagined “Ho Chi Minh Trail” by littering borderland jungles with sensors that could communicate with overflying aircraft and to a data fusion centre for decision-making. Operation Igloo White turned out to be a sophisticated, expensive methodology for murdering trespassing wildlife with aerial bombardments. It was also open to spoofing. The war was lost, eventually, but the model survived to fight another day.

[4] The UNOCT also discusses empathy-building for deradicalisation.

[5] For examples of BMT products see: https://www.bmt.org/insights/vr-training-inspired-by-gaming/

References

Arendt, H. (1963) *Eichmann in Jerusalem: A Report on the Banality of Evil.* New York: Viking Press.

Balko, R. (2013) *The Rise of the Warrior Cop: The Militarization of America’s Police Forces.* New York: Public Affairs.

Bateson, G. (1972) *Steps to an Ecology of Mind.* San Francisco: Chandler.

Department of Defence (2019) Available at: https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/SUMMARY-OF-DOD-AI-STRATEGY.PDF

Ferguson, A.G. (2017) *The Rise of Big Data Policing*. New York: NYU Press.

Foucault, M. (1977) *Discipline and Punish: The Birth of the Prison,* trans. A. Sheridan. London: Allen Lane, Penguin.

Goffman, E. (1974) *Frame Analysis*. New York: Harper & Row.

Grasseni, C. (ed.) (2007) *Skilled Visions: Between Apprenticeship and Standards.* Oxford: Berghahn.

Hacking, I. (ed.) (1992) *Historical Ontology*. Cambridge, MA: Harvard University Press.

Hanks, W.F. (2006) 'Joint Commitment an Common Ground in a Ritual Event', in N. Enfield and S. Levinson (eds.) *Roots of Human Sociality*. Oxford: Berg, 299–328.

Leese, M. and Egbert, S. (2020) *Criminal Futures: Predictive Policing and Everyday Police Work*. London and New York: Routledge.

Maguire, M. (2014) 'Counterterrorism in European Airports', in M. Maguire, N. Zurawski and C. Frois (eds.) *The Anthropology of Security: Perspectives from the Front Line of Policing, Counterterrorism, and Border Control*. London/New York: Pluto Press, 118–138.

Maguire, M. (2018) 'Policing Future Crime', in M. Maguire, U. Rao and N. Zurawski (eds.) *Bodies as Evidence: Security, Knowledge, and Power*. Durham, NC and London: Duke University Press, 137–158.

Maguire, M. and Westbrook, D.A. (2020) *Getting Through Security: Counterterrorism, Bureaucracy, and a Sense of the Modern*. London/New York: Routledge.

Maguire, M. and Westbrook, D.A. (2021) 'Security By Design: Counterterrorism at the Airport', *Anthropology Now*, 12(3), 122–135.

Mann, S. (2001) *Intelligent Image Processing*. London: John Wiley & Sons.

Mauss, M. (1973), 'Techniques of the Body', trans. Ben Brewster, *Economy and Society,* 2(1), 70–88.

Owen, M. (2014) *No Hero: The Evolution of a Navy SEAL*. New York: Penguin.

Sandhu, A. and Fussey, P. (2021) 'The 'Uberization of Policing'? How Police Negotiate and Operationalise Predictive Policing Technology', *Policing and Society,* 31(1), 66–81.

Schopenhauer, A. (1958) *The World as Will and Representation*. Indian Hills: Falcon's Wing Press.

Scott, J. (1998) *Seeing Like a State: How Certain Schemes to Improve the human Condition Have Failed*. New Haven/London: Yale University Press.

Stanton, N.A. (2011) *Trust in Military Teams*. Wey Court East, England, Ashgate.

UNOCT – United Nations Office of Counterterrorism (2021) 'The Application of Augmented Reality and Virtual Reality Technologies in Countering Terrorism and Preventing Violent Extremism'. Available at: un.org/counterterrorism/sites/www.un.org.counterterrorism/files/20210708_statement_miedico_ar-vr_webinar.pdf.

Weinbaum, S.G. (1935) *Pygmalion's Spectacles*. New York: Simon & Schuster.

Westbrook, D.A. and Maguire, M. (2019) 'Those People [May Yet Be] A Kind of Solution: Late Imperial Thoughts on the Humanization of Officialdom', *Buffalo Law Review,* 67, 889–907.

Index

Note: Page locators in italics refer to figures; Locators followed by 'n' refer to notes.