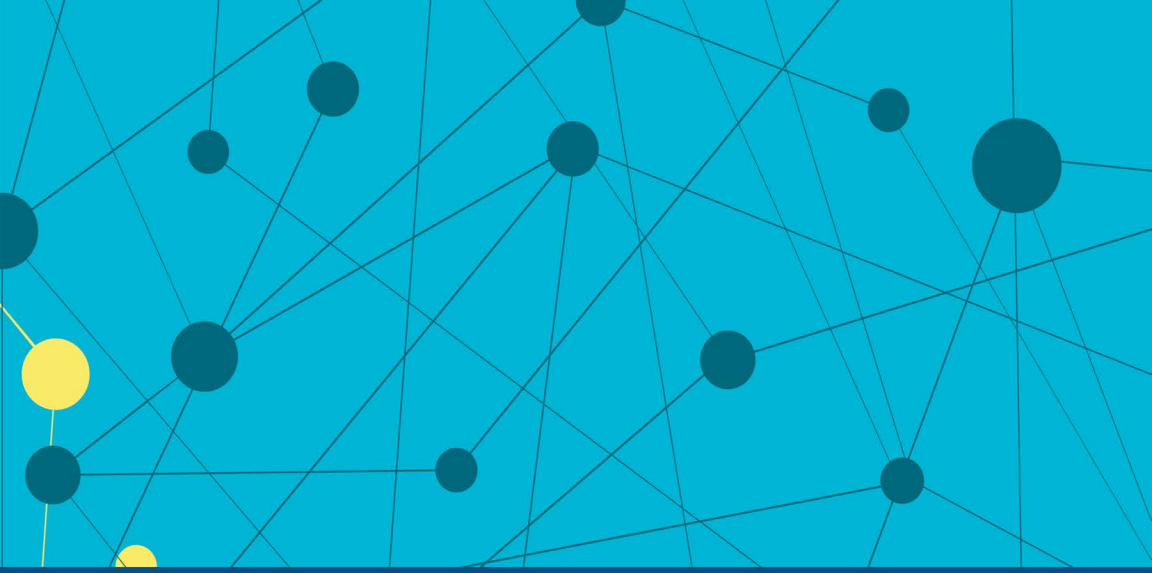


Routledge Research in the Law of Emerging Technologies

THE LAW OF GLOBAL DIGITALITY

Edited by
Matthias C. Kettemann, Alexander Peukert and
Indra Spiecker gen. Döhmann

The Law of Global Digitality

The Internet is not an unchartered territory. On the Internet, norms matter. They interact, regulate, are contested and legitimated by multiple actors. But are they diverse and unstructured, or are they part of a recognizable order? And if the latter, what does this order look like?

This collected volume explores these key questions while providing new perspectives on the role of law in times of digitality. The book compares six different areas of law that have been particularly exposed to global digitality, namely laws regulating consumer contracts, data protection, the media, financial markets, criminal activity and intellectual property law. By comparing how these very different areas of law have evolved with regard to cross-border online situations, the book considers whether cyberlaw is little more than "the law of the horse", or whether the law of global digitality is indeed special and, if so, what its characteristics across various areas of law are. The book brings together legal academics with expertise in how law has both reacted to and shaped cross-border, global Internet communication and their contributions consider whether it is possible to identify a particular mediality of law in the digital age.

Examining whether a global law of digitality has truly emerged, this book will appeal to academics, students and practitioners of law examining the future of the law of digitality as it intersects with traditional categories of law.

Matthias C. Kettemann, LL.M. (Harvard), is Professor of Innovation, Theory and Philosophy of Law at the Department for Theory and Future of Law at the University of Innsbruck, and heads research programs and groups on digital law and platform governance at the Leibniz Institute for Media Research | Hans-Bredow-Institut (Hamburg) and the Humboldt Institute for Internet and Society (Berlin).

Alexander Peukert is Professor of Civil and Commercial Law at the Faculty of Law at Goethe University Frankfurt am Main.

Indra Spiecker gen. Döhmann, LL.M. (Georgetown University) holds the chair of Public and Administrative Law, especially Information Law, Environmental Law and Legal Theory at the Goethe-University of Frankfurt/Main in Germany. She is also Director of the Research Institute on Data Protection, Managing Director of the Institute of European Health Politics and Social Law, both at Goethe University of Frankfurt/Main, and also Principal Investigator with the Competence Center on IT-Security (KASTEL) at the Karlsruhe Institute of Technology (KIT). Professor Spiecker publishes in the entire field of constitutional and administrative law with a special focus on information law as well as technology law.

Routledge Research in the Law of Emerging Technologies

Biometrics, Surveillance and the Law
Societies of Restricted Access, Discipline and Control
Sara M. Smyth

Artificial Intelligence, Healthcare, and the Law
Regulating Automation in Personal Care
Eduard Fosch-Villaronga

Health Data Privacy under the GDPR
Big Data Challenges and Regulatory Responses
Edited by Maria Tzanou

Regulating Artificial Intelligence
Binary Ethics and the Law
Dominika Ewa Harasimiuk and Tomasz Braun

Cryptocurrencies and Regulatory Challenge
Allan C. Hutchinson

Regulating Artificial Intelligence in Industry
Edited by Damian M. Bielicki

The Law of Global Digitality
Edited by Matthias C. Kettemann, Alexander Peukert and Indra Spiecker gen. Döhmann

Internet of Things and the Law
Legal Strategies for Consumer-Centric Smart Technologies
Guido Noto La Diega

The Law of Global Digitality

Edited by
Matthias C. Kettemann,
Alexander Peukert and
Indra Spiecker gen. Döhmann

Routledge
Taylor & Francis Group
LONDON AND NEW YORK

First published 2022
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

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
A catalog record has been requested for this book

ISBN: 978-1-032-07369-9 (hbk)
ISBN: 978-1-032-25550-7 (pbk)
ISBN: 978-1-003-28388-1 (ebk)

DOI: 10.4324/9781003283881

Typeset in ITC Galliard
by Apex CoVantage, LLC

Contents

Contributors

Christopher G. Bradley, Wyatt, Tarrant & Combs Associate Professor of Law, University of Kentucky, J David Rosenberg College of Law

Roland Broemel, Professor of Public Law, Economic and Currency Law, Financial Markets Regulation and Legal Theory, Faculty of Law, Goethe University Frankfurt am Main

Beatrice Brunhöber, Professor of Criminal Law, Criminal Procedure Law, Philosophy of Law and Comparative Law, Faculty of Law, Goethe University Frankfurt am Main

Indra Spiecker gen. Döhmann, Professor of Public Law, Information Law, Environmental Law and Legal Theory, Goethe University Frankfurt am Main

Stephan Dreyer, Senior Researcher in Media Law and Media Governance, Leibniz Institute for Media Research | Hans-Bredow-Institut

Ellen P. Goodman, Professor, Rutgers University Law School

Matthias C. Kettemann, Professor of Innovation, Theory and Philosophy of Law, Head of the Department for Theory and Future of Law, University of Innsbruck; Research Program Head, Leibniz Institute for Media Research | Hans-Bredow-Institut, Hamburg

Ronald J. Krotoszynski, John S. Stone Chair, Director of Faculty Research and Professor of Law at the University of Alabama School of Law

Felix Maultzsch, Professor of Civil Law, Civil Procedure Law, Private International Law and Comparative Law, Faculty of Law, Goethe University Frankfurt am Main

Alexander Peukert, Professor of Civil and Commercial Law, Faculty of Law, Goethe University Frankfurt am Main

Thomas Riis, Professor, PhD, LLD at the University of Copenhagen, Centre for Information and Innovation Law (CIIR)

Jens Schovsbo, Professor, PhD, LLD at the University of Copenhagen, Centre for Information and Innovation Law (CIIR)

Wolfgang Schulz, Director of the Leibniz Institute for Media Research | Hans-Bredow-Institut and Professor of Media Law and Public Law at the University of Hamburg

Theresa Josephine Seipp, Junior Researcher, Leibniz Institute for Media Research | Hans-Bredow-Institut

Introduction

The Law of Global Digitality

Alexander Peukert and Matthias C. Kettemann

1 Context, Subject Matter and Aim of This Book

According to German sociologist Niklas Luhmann, it took some 200 years until the disruptive potential of the printing press started to influence all segments of society, eventually leading to a fundamental change in the structure of Western European societies from a feudal-hierarchical to a modern, functionally differentiated society.[1] If this observation is correct, and global digital communication via the internet has a disruptive potential similar to that of the printing press,[2] then we are in a relatively early stage of the socio-economic transformations triggered by this new communication technology. The control of U.S. public authorities regarding the infrastructural backbone of the internet did not officially end until 30 April 1995.[3] The mid-1990s also mark the beginning of the widespread public use of the World Wide Web in the U.S.[4] In 1994, AOL linked to the internet for the first time, Yahoo! was established and Amazon began operations as an online bookstore.[5] Prior to the mid-1990s, the internet had also not had a significant impact on the law. Even in the U.S., internet-related legal disputes remained rare until 1995.[6] This is even more true for Germany, where an article was published in the most widely read legal journal in late 1995, titled: "The Internet for Lawyers—An Introduction".[7]

1 Niklas Luhmann, *Die Wissenschaft der Gesellschaft* (1st edn, 1990) Suhrkamp, 600; see also Mireille Hildebrandt, *Smart Technologies and the End(s) of Law* (2015) Edward Elgar, 159ff (distinct characteristics of modern law were triggered by the printing press).

2 Cf Manuel Castells, *The Rise of the Network Society: The Information Age: Economy, Society and Culture* (1996) Wiley-Blackwell; Kevin Werbach, 'The Song Remains the Same: What Cyberlaw Might Teach the Next Internet Economy' (2017) 69 Fla L Rev 887, 916–17 ("predictions that the internet and electronic commerce would have dramatic economic and social effects, eventually becoming pervasive in much of the world, proved accurate").

3 Janet Abbate, *Inventing the Internet* (1999) MIT Press, 196, 199.

4 James Boyle, 'Is the Internet Over?! (Again?)' (2019) 18 Duke L & Tech Rev 32, 36.

5 Michael L Rustad and Diane D'Angelo, 'The Path of Internet Law: An Annotated Guide to Legal Landmarks' (2011) 10 Duke L & Tech Rev 3, 9.

6 Ibid 10.

7 Thomas Hoeren, 'Das Internet für Juristen—eine Einführung' (1995) 48 Neue Juristische Wochenschrift 3295.

DOI: 10.4324/9781003283881-1

At that point in time, U.S. scholars started to debate whether what was then called "cyberspace" required new, special legal approaches or whether existing legal principles and rules could and should apply at least *mutatis mutandis*. Was "cyberlaw", in other words, a return of the law of the horse?[8] Or do "we see something when we think about the regulation of cyberspace that other areas would not show us"?[9]

Initially, cyber-exceptionalists dominated the debate.[10] In view of the heterarchical, acentric structure[11] of the original internet and its global reach,[12] they argued that governments could not and should not control cross-border electronic communication;[13] that a new "network governance paradigm" is needed that "must recognize all dimensions of network regulatory power";[14] that at least one non-governmental internet standard setting procedure "meets Habermas's notoriously demanding procedural conditions for a discourse capable of legitimating its outcomes";[15] and that generally an autonomous, self-regulatory "*lex informatica*", "*lex electronica*" or "twenty-first-century Law Merchant" beyond the State appears to be the adequate form of regulation.[16] Textbooks on "Cyberlaw"

8 Frank H Easterbrook, 'Cyberspace and the Law of the Horse' [1996] U Chi Legal F 207, 212; Joseph H Sommer, 'Against Cyberlaw' (2000) 15 Berkeley Tech LJ 1145.

9 Lawrence Lessig, 'The Law of the Horse: What Cyberlaw Might Teach' (1999) 113 Harv L Rev 501, 502.

10 Cf Lawrence Lessig, *Code and Other Laws of Cyberspace* (1999) Basic Books, 4–8.

11 Cf Robert A Heverly, 'Breaking the Internet: International Efforts to Play the Middle Against the Ends—A Way Forward' (2011) 42 Geo J Int'l L 1083, 1095–96; Joanna Kulesza and Roy Balleste, 'Signs and Portents in Cyberspace: The Rise of Jus Internet as a New Order in International Law' (2013) 23 Fordham Intell Prop Media & Ent LJ 1311.

12 This is still considered to be the case by, for example, Case C-507/17 *Google LLC v Commission nationale de l'informatique et des libertés (CNIL)* (CJEU, 24 September 2019), para 56 ("The internet is a global network without borders . . ."); *Warner Music UK Ltd & Ors v Tunein Inc* [2019] EWHC 2923 (Ch), [2020] ECDR 8, para 12 ("Users accessing the world wide web from the UK can gain access to websites all over the world. This is routine".).

13 John Perry Barlow, 'A Declaration of the Independence of Cyberspace' (1996) <www.eff.org/de/cyberspace-independence> accessed 30 June 2021; David R Johnson and David Post, 'Law and Borders—the Rise of Law in Cyberspace' (1996) 48 Stan L Rev 1367, 1390; David G Post, 'Against Against Cyberanarchy' (2002) 7 Berkeley Technol Law J 1365–83; see also Frederike Zufall, 'Shifting Role of the "Place": From Locus Delicti to Online Ubiquity in EU, Japanese and U.S. Conflict of Tort Laws' (2019) 83 RabelsZ 760, 780.

14 Joel R Reidenberg, 'Governing Networks and Rule-Making in Cyberspace' (1996) 45 Emory LJ 911, 926.

15 A Michael Froomkin, 'Habermas@discourse.net: Toward a Critical Theory of Cyberspace' (2003) 116 Harv L Rev 749, 752.

16 Cf Joel R Reidenberg, 'Lex Informatica: The Formulation of Information Policy Rules Through Technology' (1998) 76 Tex L Rev 553, 578; Gunther Teubner, 'Societal Constitutionalism: Alternatives to State-Centered Constitutional Theory' in Paul Schiff Berman (ed), *Law and Society Approaches to Cyberspace* (2007) 160–61; Leon E Trakman, 'From Medieval Law Merchant to E-Merchant Law' (2003) 53 U Toronto Law J 265; see also Marcelo Halpern and Ajay K Mehrotra, 'From International Treaties to Internet Norms: The Evolution of International Trademark Disputes in the Internet Age' (2000) 21 U Pa J Int'l Econ L 523, 561.

or "Internet Law" have brought the notion to legal education that there is indeed a separate legal field to be taught.[17]

Shortly after the burst of the dotcom bubble in 2001, it became however abundantly clear that at least the more aspirational visions of "cyberlaw" would not materialize.[18] Exceptionalists have been criticized in particular for their naïve technological determinism.[19] And indeed, if communication on the internet was ever anarchic and heterarchical, this structure has for quite some time been replaced by the hierarchies implemented by/through "very large online platforms" and other "gatekeepers".[20] Moreover, the State "never left the scene".[21] Only the State is said to have "the power, status and administrative capability to become the Kantian superego" of big tech.[22] Intellectual and other forms of property have not only been retained, but strengthened, and are enforced on the internet on the basis of merely adapted private international law rules.[23] Litigation involving electronic transactions is also said to be "virtually indistinguishable from that involving old-fashioned paper contracts".[24]

But even if one thinks that the "hoary" debates between cyber-exceptionalists and cyber-realists are, if at all, only of historical interest,[25] their core question, namely

17 Cf Raymond SR Ku, *Cyberspace Law* (5th edn, 2020) Wolters Kluwer; Michael L Rustad, *Global Internet Law in a Nutshell* (4th edn, 2019) West Academic Publishing; Volker Böhme-Neßler, *CyberLaw: Lehrbuch zum Recht des Internet* (2001) C.H.Beck; Thomas Hoeren, *Internetrecht* (3rd edn, 2018) De Gruyter; Louisa Specht-Riemenschneider, Severin Riemenschneider and Ruben Schneider, *Internetrecht* (2020) Springer.

18 Lawrence Lessig, *Code 2.0* (2006) ix; Rolf H Weber, *Internet Governance at the Point of No Return* (2021) EIZ Publishing, 1.

19 Meg Leta Jones, 'Does Technology Drive Law? The Dilemma of Technological Exceptionalism in Cyberlaw' [2018] U Ill JL Tech & Pol'y 249, 252–53.

20 Cf European Commission, 'Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act)' COM(2020) 825 final, art 25ff; European Commission, 'Proposal for a Regulation of the European Parliament and of the Council on Contestable and Fair Markets in the Digital Sector (Digital Markets Act)' COM(2020) 842 final, art 3ff.

21 Michael D Birnhack and Niva Elkin-Koren, 'The Invisible Handshake: The Reemergence of the State in the Digital Environment' (2003) 8 Va JL & Tech 6, 1–2.

22 Boyle (n 4) 49, confirming Jack L Goldsmith, 'Against Cyberanarchy' (1998) 65 U Chi L Rev 1199, 1200–01.

23 See the International Law Association's Guidelines on Intellectual Property and Private International Law ("Kyoto Guidelines") (2021) 12 JIPITEC 4–12, and the contributions by Riis/Schovsbo and Peukert, in Chapter 1.

24 Juliet M Moringiello and William L Reynolds, 'The New Territorialism in the Not-So-New Frontier of Cyberspace' (2014) 99 Cornell L Rev 1415, 1419–20.

25 Derek E Bambauer, 'Middlemen' (2012) 64 Fla L Rev F 64, 65; contra F Willem Grosheide, 'Being Unexceptionalist or Exceptionalist—That is the Question' (2012) 9 SCRIPTed 340 <http://script-ed.org/?p=690> accessed 30 June 2021:

> whether Cyberspace requires a system of rules which are quite distinct from the laws that regulate physical, geographically-defined territories, or whether it is necessary to develop for Cyberspace its own effective legal regulations [is] a question [that] has kept its momentum and as a consequence is still very topical today.

the interrelationship between digital technologies and the law, remains valid and topical to this very day. Digitalization is not finished but instead impacts ever more aspects of our daily lives. In February 2020, the European Commission observed that "digital communication, social media interaction, e-commerce, and digital enterprises are steadily transforming our world", requiring a regulatory answer "towards a digital transformation that works for the benefit of people through respecting our values".[26] The COVID-19 pandemic has further accelerated this transformation but also laid bare fundamental challenges in digitalization.[27]

The debate concerning a proper description and an adequate theory of internet-related "cyberlaw" or, more generally, digital law, is also far from over or settled. Reviewing three generations of internet law scholarship, Paul Schiff Berman concluded in 2007 that "*something* is changing".[28] Since then, several efforts have been undertaken to carve out precisely what is changing and what is special about digital law.[29] For example, Julie Cohen introduced the notions of "networked space" and "networked self" to describe and theorize respective developments.[30] Thomas Riis, one of the contributors to this collection, put forward a theory of "user-generated law" that emerges, evolutionary-like, from user practices and norms, which are later sanctioned or adopted by State actors.[31]

Last but not least, several authors have stressed the particular mediality of digital law.[32] In 2009, Vaios Karavas observed the emergence of a "techno-digital normativity", that is, the amalgamation of normative and digital expectations inside the digital medium.[33] According to Mireille Hildebrandt, law will indeed "have to respond to transformations in the dominant [information and communication infrastructure]" because it "depends on human language, and is

26 European Commission, 'Shaping Europe's Digital Future' COM(2020) 67 final, p 2.

27 Samer Faraj, Wadih Renno and Anand Bhardwaj, 'Unto the Breach: What the COVID-19 Pandemic Exposes about Digitalization' (2021) 31 Inf Organ 100337.

28 Paul Schiff Berman, 'Introduction' in Paul Schiff Berman (ed), *Law and Society Approaches to Cyberspace* (2007) Ashgate Publishing Ltd, xxiii; see also Andrea M Matwyshyn, 'The Law of the Zebra' (2013) 28 Berkeley Tech LJ 155, 155 ("At the dawn of internet law, scholars and judges debated whether a 'law of the horse'—a set of specific laws addressing technology problems—was ever needed. Time has demonstrated that in some cases, the answer is yes".).

29 For an overview see Rolf H Weber, *Internet Governance at the Point of No Return* (2021) EIZ Publishing, 17ff (distinguishing between first and second generation regulatory models).

30 Julie E Cohen, 'Cyberspace As/and Space' (2007) 107 Colum L Rev 210; Julie E Cohen, *Configuring the Networked Self* (2012).

31 Thomas Riis, 'User Generated Law: Re-constructing Intellectual Property Law in a Knowledge Society' in Thomas Riis (ed), *User Generated Law* (2016) Edward Elgar Publishing, 2–3.

32 See generally Thomas Vesting, *Legal Theory and the Media of Law* (2018) Edward Elgar Publishing; Volker Böhme-Neßler, *Unscharfes Recht: Überlegungen zur Relativierung des Rechts in der digitalisierten Welt* (2008) Duncker and Humblot Berlin, 617ff.

33 Vaios Karavas, 'The Force of Code: Law's Transformation Under Information-Technological Conditions' (2009) 10 German LJ 463, 478.

entirely dependent on communication to establish and consolidate its normative framework".[34] If we ignore this dependency and continue to regulate technologies as before, we might face, posits Hildebrandt, "the end of law as a reliable framework" in what she calls the "onlife world".[35] Our Frankfurt colleague Thomas Vesting also argues that traditional legal hierarchies no longer function under conditions of global digital communication and that it is necessary to rethink even our concepts of individual freedom and human rights.[36]

These developments in legal theory form the context of this collection. The hypotheses and basic concepts that guided the book's composition can be summarized as follows: To understand and adequately describe the ongoing digital transformation of law and society, it is firstly insufficient to only focus on technologies as such. For these technologies, for example the basic internet protocols, only exhibit effects on society if and insofar as they are actually implemented by various actors.[37] The term "digitality" is supposed to articulate this link between digital technologies (hardware, software, applications) and their practical use.[38] Secondly, most current laws and other normative orders[39] evolved prior to the advent of digitality. Their application to digital human behavior creates frictions up to the point that non-digital norms become dysfunctional or illegitimate. Digital transformation can, however, also not be reduced to a one-sided effect of digitality on the law. Instead, digitality is itself subject to numerous constraints (e.g. business model concerns and, not the least, applicable laws). In short, the digital affects us and vice versa.

On the basis of these assumptions, this book's purpose is to improve our understanding of the interplay between digitality on the one hand and law on the other, or, in Lessig's words before leaving the field, to provide a "richer sense of how these modalities . . . interact" in the course of the ongoing digital transformation.[40] The approach adopted herein to achieve this aim is in some respects relatively circumscribed, in other respects relatively broad.

It is circumscribed firstly in that this is a book written exclusively by lawyers studying the *law* of global digitality. The contributions reflect the technological and socio-economic aspects of digitality but they focus on the *legal* aspect of digitalization. A second limitation follows from the fact that the authors—in contrast to the first-generation cyberlaw literature of the late 20th century—do not take an *ex ante* perspective on possible future developments of digitality and digital law. Instead, we look back and reassess the evolution of the law after some

34 Hildebrandt (n 1) 175.
35 Hildebrandt (n 1) 218, 226; see also Teubner (n 16) 166 (code as "nightmare for principles of legality").
36 Thomas Vesting, *Legal Theory and the Media of Law* (2018) Edward Elgar Publishing, 556ff.
37 Bruno Latour, *Aramis, or the Love of Technology* (1996) Harvard University Press.
38 See Felix Stalder, *The Digital Condition* (2017) Polity.
39 On this topic see Rainer Forst and Klaus Günther (eds), *Normative Ordnungen* (2021) Suhrkamp Verlag.
40 Cf Lessig (n 18) 340.

25 years of digitalization. Thirdly, our approach is concrete in that we proceed inductively. We do not present a theory of the law of global digitality and then test it by considering certain examples but we look at certain legal areas and try to digest general characteristics of the law of global digitality from there.[41] Fourthly, all papers pay specific attention to cross-border, *global* aspects of digital transformation. Some contributions analyze genuinely global phenomena,[42] whereas other chapters provide comparative overviews on the legal evolution in the U.S. and the EU, thereby carving out varieties of global legal digitality.[43]

In two respects, however, this book adopts a deliberately broad approach. Firstly, the notion of "law" is understood in a very broad sense. Accordingly, the papers address international, supranational and national statutory black letter and case law, but also hybrid public/private governance instruments (e.g. codes of conduct), and purely private modes of regulating online communication and commerce, in particular via contracts and code. Secondly—and this, in our view, is the truly distinctive feature of the book—it assembles studies of six very different areas of law, namely intellectual property, data protection/privacy, consumer contracts, media law, financial market regulation and criminal law. By comparing how these very different areas of law have reacted to and at the same time shaped global digitality, we aim to identify structural regulatory patterns that occur across all fields. We notice that something is changing,[44] and we want to know precisely what and how. If a certain type of regulation, a substantive principle or another legal aspect could be observed in many or even all of these very diverse fields, it is plausible to assume that the recurring feature represents a specific characteristic of digital law and not just a variant of pre-digital law (aka "law of the horse"). Such a legal feature would be the "smoking gun" with which the early exceptionalists would eventually win their old battle with un-exceptionalists, if only in certain, exceptional respects. We will get back to this general research question in the concluding Chapter.

2 Chapter Overview

2.1 Intellectual Property Law

Property in general and intellectual property (IP) in particular are classical cyberlaw topics. In March 1994, John Perry Barlow, the great guru of cyberlaw exceptionalism, posited that the problem of "digitized property" seemed to be

41 See, in particular, the contribution by Riis/Schovsbo.

42 See the contributions by Peukert (global intellectual property governance on the internet), Broemel (digital currencies and their regulation) and Brunhöber (transnational cybercrime regulation).

43 See the chapters on data protection/privacy, consumer contract law, and media law and generally Eric Schmidt and Jared Cohen, *The New Digital Age* (2013) 126 (in ten years the relevant question will no longer be whether a society uses the internet, but which version it uses).

44 Berman (n 28).

"the root of nearly every legal, ethical, governmental, and social vexation to be found in the Virtual World" because "if our property can be infinitely reproduced and instantaneously distributed all over the planet without cost, without our knowledge, without its even leaving our possession, how can we protect it?"[45] Easterbrook's famous 1996 "Law of the Horse" article also concerned the topic "Property in Cyberspace", which Easterbrook tackled by resorting to orthodox property theory.[46] And ICANN's 1999 Uniform Domain-Name Dispute-Resolution Policy (UDRP) in the area of trademark law is considered the prime example of an autonomous, self-regulatory *lex electronica* beyond the state.[47] The long and complex relationship between global digitality and IP is assessed in the two IP contributions from different angles.

Based on the insight that the challenges of digitalization indeed first became acute in information law and in particular in copyright law, Thomas Riis and Jens Schovsbo argue that by studying the impact of digitalization within the field of copyright law, it is possible to deduce and identify methodological shifts of general significance. On the basis of detailed analyses of strategies adopted by the EU legislator and the CJEU during the last two decades to deal with the challenges of digitalization, they detect four general methodological shifts in the law of digitality, namely: (1) a shift from substantive law to procedural law; (2) a shift towards globalization; (3) a shift towards what they call a horizontally based law; and (4) a shift from state-enacted law to contract and code, implemented by private parties within certain "autonomy spaces".[48]

Alexander Peukert's contribution "Transnational Intellectual Property Governance on the Internet" directly connects to Riis's and Schovsbo's fourth methodological shift, from state law to private regulation. Peukert's article documents and classifies instances of transnational IP enforcement and licensing on the internet with a particular focus on the territorial reach of the respective regimes. He shows that the bulk of transnational enforcement measures is indeed adopted in the context of "voluntary" self-regulation by various intermediaries. Overall, he observes three layers of IP governance on the internet. Based on global licenses, Open Content is freely accessible everywhere. "Rogue" IP infringements are equally combatted on a worldwide scale. Territorial fragmentation persists, instead, in the markets for fee-based services and in hard cases of conflicts of IP laws/rights. All three universal norms (global accessibility, global illegality and global fragmentation) are supported by a quite solid, "rough" global consensus.[49]

45 John Perry Barlow, 'The Economy of Ideas' [1994] 2(3) Wired <http://groups.csail.mit.edu/mac/classes/6.805/articles/int-prop/barlow-economy-of-ideas.html> accessed 30 June 2021.

46 Frank H Easterbrook (n 8) 208; contra for example Michael A Carrier and Greg Lastowka, 'Against Cyberproperty' (2007) 22 Berkeley Tech LJ 1485, 1486.

47 Teubner (n 16); see also Lessig (n 18) 169ff.

48 See Thomas Riis (ed), *User Generated Law* (2016) Edward Elgar Publishing.

49 On the concept of "rough consensus and running code" see David G Post, *In Search of Jefferson's Moose* (2009) Oxford University Press, 136–37; Gralf-Peter Callies and Peer Zumbansen, *Rough Consensus and Running Code* (2010) Hart Publishing, 135–36.

2.2 Data Protection/Privacy

The second chapter is dedicated to another individual right deeply affected by global digitality, namely the right to the protection of personal data[50] or, in U.S. legal terminology, data privacy.[51] This legal area is of particular interest for the general research question of this volume because it emerged in the 1960s and 1970s as a separate field in Germany and other European countries in reaction to automated data processing and automated decision making, and thus early forms of computerization and digitalization.[52] Data protection/privacy is therefore a subject matter predestined for our study, which promises to reveal specific characteristics of digital law, both in its original form shaped in the 20th century and in its contemporary form, responding to ubiquitous computing, big data, cloud computing, high-speed volume processing and artificial intelligence. The two contributions on this topic further enrich the analysis by providing a comparison between EU and U.S. data protection/privacy approaches.

In her chapter, Indra Spiecker gen. Döhmann gives an overview of core regulatory goals and instruments of EU data protection law by comparing the starting point, the Data Protection Directive of 1995 (DPD),[53] with the present General Data Protection Regulation of 2018 (GDPR).[54] Spiecker gen. Döhmann identifies several characteristics of pre-internet data protection law, in particular its focus on automated decision-making processes and the imbalance of power inherent in them, and its preventive and horizontal character. From its inception, European data protection law furthermore followed the precautionary principle rather than setting up new *ex post* liability rules, and it applied irrespective of the type of personal information or area of life concerned directly to the processing of data at its origin. The GDPR, in turn, did not abandon these principles but adjusted and strengthened them in view of globalization and an increased "scale of the collection and sharing of personal data" on/via the internet.[55] Spiecker gen. Döhmann shows that the GDPR differs from the DPD in that it reformulates the precautionary principle as a gradual risk-based approach, introduces aspects of consumer protection, takes the private sector into focus and takes a global regulatory perspective on ubiquitous data processing.

Ronald J. Krotoszynski's analysis of U.S. data privacy law draws a very different picture. Krotoszynski posits that a global consensus concerning personal data

50 Cf Charter of Fundamental Rights of the European Union, 2012/C 326/02, art 8(1).

51 See Lessig (n 18) 200ff.

52 See Spiecker gen. Döhmann, in this volume.

53 Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281/31.

54 Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119L119/1.

55 GDPR (n 54), recital 6.

protection would be highly desirable in light of transnational data processing, but that it will be very difficult if not impossible to achieve such a consensus if it is to include the U.S. because the U.S. approach to privacy is starkly different from the rest of the world, both in its regulatory attitudes and substantive policies. Although the U.S. Supreme Court recognized a right to informational privacy even before the German Federal Constitutional Court's famous *Census* case,[56] current federal data privacy regulation still presents a patchwork. Furthermore, the qualification of the use of data—including gathering, storing and manipulating data—as a form of "speech" for purposes of applying the First Amendment seriously complicates any efforts to harmonize privacy regulations in the U.S. with those in the EU and elsewhere. This legal landscape is complemented, according to Krotoszynski, by a "general lack of concern about personal data protection within contemporary society in the U.S.". In his conclusions, Krotoszynski points out, however, that in spite of these legal and cultural differences, a transnational agreement including the U.S. might be achievable on the conflict-of-laws question of which sovereign, or sovereigns, may legitimately regulate personal data privacy.

2.3 Consumer Contract Law

Whereas the chapters on IP and data protection/privacy deal with the mutual interrelationships between global digitality on the one hand and individual (property) rights on the other, the third chapter addresses another cornerstone of private law, namely contracts, and, more specifically, business-to-consumer (B2C) contracts. Since the internet opened for businesses in the mid-1990s, consumer commerce has to a very large extent moved to the digital space. In 2020, 71% of EU consumers shopped online.[57] In the U.S., e-commerce shipments comprised 67.3% of all manufacturing shipments in 2018.[58] In their chapters, Christopher G. Bradley and Felix Maultzsch explore whether the digital revolution in consumer commerce has been accompanied by a revolution of consumer protection in the U.S. and the EU respectively.

Regarding the legal situation in the U.S., Bradley diagnoses a "ragged patchwork" of consumer protection laws, regulations and institutions. On the one hand, consumer contracts are subject to longstanding common-law principles as developed by courts. In their decisions, Bradley observes a tendency to

56 Cf *Whalen v Roe* 429 US 589 (1977) with German Federal Constitutional Court, Case 1 BvR 209/83, 15.12.1983, English abstract available at <www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/1983/12/rs19831215_1bvr020983.html> accessed 3 July 2021.

57 European Commission, 'Key Consumer Data 2020', <https://ec.europa.eu/info/policies/consumers/consumer-protection/key-consumer-data_de> accessed 3 July 2021.

58 US Census Bureau, 'E-Stats 2018: Measuring the Electronic Economy', May 21 2020 <www.census.gov/library/publications/2020/econ/2018-e-stats.html> accessed 3 July 2021.

stimulate easy, mass commerce, whereas public policy or distributional concerns are referred to the legislative branch. On the other hand, numerous aspects of consumer transactions are subject to non-uniform State law of contract and of consumer protection. The overall picture of U.S. consumer law is thus highly complex and unstable. Bradly supports this finding in a summary of the "fiercest consumer law controversy in recent memory", the 2019 failure of the American Law Institute's proposed Restatement of the Law, Consumer Contracts, which he presents as a battle over standardization and baselines of consumer law. As regards the role of technology in consumer protection, Bradley argues for what he calls "tech realism": Market and technological approaches to new consumer protection problems of online commerce hold some promise, but their promise should not be overstated.

Maultzsch's depiction of paradigms of EU consumer law in the digital age reveals a very different legal landscape but surprisingly similar overall tendencies. In order to carve out whether and to what extent EU contract law is influenced by new patterns of digitality, Maultzsch deliberately focuses on the regulation of sales of "conventional" goods in contrast to contracts for the supply of digital content and digital services.[59] He argues that sales law in general is heavily influenced if not already dominated by a new paradigm of digital sales. Under this paradigm, the primary aim of contract law is no longer to protect the individual autonomy of the parties and to balance out their interests but more and more to protect and facilitate markets as such. In particular, classical ideas of freedom of contract and of protecting the weaker party are increasingly replaced by a statutory standardization of possible contractual contents with the aim to boost online markets and create "a kind of carefree consumption environment". This process is flanked on a procedural level by an enhancement of Alternative Dispute Resolution procedures and collective representative actions which favor fast and standardized "rough justice" solutions instead of an enforcement of individual rights *stricto sensu*.

2.4 Media Law

Chapter 4 is dedicated to a comparison of U.S. and EU perspectives of media law. Media law is of special importance to digitality because most content we interact with is "mediated". It is either reported on by traditional media outlets or in social media, or it is hosted, amplified, hidden, monetarized and recommended by platforms. We experience the world in a mediated way. And the "media" are becoming fewer: Today we use the internet, as Milton L. Mueller reminds us, "to place

59 Cf Directive (EU) 2019/770 of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services [2019] OJ L136/1 and Directive (EU) 2019/771 of 20 May 2019 on certain aspects concerning contracts for the sale of goods, amending Regulation (EU) 2017/2394 and Directive 2009/22/EC, and repealing Directive 1999/44/EC [2019] OJ L136/28.

telephone calls, watch live or recorded video, browse libraries and download or play music".[60] Different media—TV, books, radio, CDs, newspapers—were once regulated by different regimes. Their content is now being delivered, in a trend called *digital convergence*, through internet protocol (IP)-based services: through "the internet".[61] Regulating what can be said online therefore becomes central to the challenge of establishing a suitable media order. Clearly, freedom of expression by itself is a key enabling right, offline just as online. In one of its fundamental cases on the role of Art. 10 of the European Convention on Human Rights in online environments—the 2015 *Cengiz and Others* case—the Strasbourg judges confirmed that

> the Internet has now become one of the principal means by which individuals exercise their right to freedom to receive and impart information and ideas, providing as it does essential tools for participation in activities and discussions concerning political issues and issues of general interest.[62]

Ellen P. Goodman, in her contribution similarly puts free speech at the center of her study on U.S. approaches.[63] She shows how U.S. media law is adapting to digital platforms with a view to extraterritorial effects. Since the largest digital platforms are U.S. companies engaged in self-regulation and private ordering of media flows, those private activities have more extraterritorial effect than any public law effort. Goodman criticizes that the public law developments still are inchoate, with some states having adopted laws concerning political advertising and deceptive speech, and the Congress being in the process of renegotiating Sec. 230 of the Communications Decency Act, which provides platforms with immunity for online speech in most cases. Goodman shows how Sec. 230 has been contracted in the past, including through FOSTA/SESTA, and which developments in platform regulation seem likely.

In a contribution that is built on research conducted for the German EU presidency dedicated to reforming the EU's infrastructural order, Stephan Dreyer, Matthias C. Kettemann, Wolfgang Schulz and Theresa Josephine Seipp show how the media we use to communicate have changed in times of digitality. Media law, the authors say, has been strongly influenced by digitality, especially in light of the intricate interaction between media (as in newspapers) and media (as in communicative forms). The authors argue that we are currently observing a process of re-figuration in the field of democracy-relevant communication processes and actors. The authors then sketch the status quo of Europe's media order and offer glimpses into the future. The discussion on the status quo, the authors find,

60 Milton N Mueller, *Networks and States. The Global Politics of Internet Governance* (2010) The MIT Press, 9.

61 Cf ibid 10.

62 *Cengiz and Others v Turkey* App no 48226/10 and 14027/11 (ECtHR, 1 December 2015), para 49.

63 Cf Lessig (n 18) 233ff.

should not ignore the parallel normative processes related to the DSA/DMA, the Data Governance Act and the AI Act. Together, these four legislative packages can create an entirely new framework for regulating data, AI, users and businesses in the European single market. This, truly, would be not only a media order, but rather the foundation of a new European communication law of digitality.

2.5 Financial Regulation and Criminal Law

The fifth and final part concerns two areas of public law—financial regulation and criminal law—which have also been heavily impacted by global digitality but have not been in the focus of theorizing cyberlaw.

In his chapter, "Regulating Virtual Currencies", Roland Broemel argues that Bitcoin and other digital/virtual currencies are both a specifically digital and a specifically global phenomenon. Regarding the technology, Broemel demonstrates that digital currencies are constituted and transferred by algorithm-based operations. Blockchain technology creates properties that conventional means of payment do not have. Digital currencies are also unique from an economic point of view in that they combine the characteristics of digital payment services (datafication) with those of digital platforms. As a result, digital currency "ecosystems" become a driver of complex, cross-market business models. The fact that digital currencies create units exclusively by code also eludes classification as national or international from the outset. They can no longer be assigned to a particular nation state and typically do not even have a particular local center. These characteristics raise unique regulatory issues, in particular in the areas of combating money laundering or terrorist financing, investor and consumer protection and the stability of financial markets. Broemel shows that some of these challenges have been addressed by applying existing laws (e.g. in the area of banking supervision and securities law), whereas others have led to the emergence of specific regimes for virtual currencies.

Beatrice Brunhöber's contribution to this collection concerns the interrelationship between global digitality and criminal law. In this area, "cybercrime" continues to be the technical term for the regulation of digital activity through criminal law. The relevant provisions are classified as either "cyber-enabled" offenses, where a computer system is used as an instrument (e.g. cyberfraud), or "cyber-dependent" offenses, when the crime targets information technology devices or infrastructures (e.g. computer hacking). Other definitions of cybercrime distinguish between access, use and content offenses. Brunhöber points out that these classifications do not attach to the protected legal interests, which in contrast structure traditional criminal law.[64] She further provides an overview of the two major approaches for dealing with cybercrime as a global phenomenon, namely legislation and policy measures. The former aims at harmonizing

64 See "Special Part" of the German Criminal Code, arts 80ff available at www.gesetze-im-internet.de/englisch_stgb/.

domestic substantive criminal law and establishing procedural rules for interstate cooperation for law enforcement. In the West and beyond, Brunhöber identifies the 2001 Council of Europe Convention on Cybercrime as the most important transnational legislation on this point. Cybercrime policy instead focuses on capacity building. This has been the primary approach pursued by the UN for some time. In her critique of cybercrime law, Brunhöber considers the Cybercrime Convention as "exemplary for the lack of democratic participation in crafting it", and argues that individual liberties are threatened by cybercrime prohibitions and the surveillance possibilities available to law enforcement authorities.

Part I

Intellectual Property

1 Towards a Legal Methodology of Digitalisation

The Example of Digital Copyright Law

Thomas Riis and Jens Schovsbo

1 Introduction

Digital technologies have shaped and continue to shape the world. Our economic, social, political and cultural life rely on how we regulate these technologies.[1] Digitalisation has also challenged our basic notions about law. In this contribution, we will examine how digital technology has influenced the construction of law and we will elaborate a framework for a *legal methodology of digitalisation*.

In this context "methodology" will be construed in a broad and pragmatic way referring to the procedures and practices used by international, regional and national regulators, courts and other decision-making bodies and private legal actors such as right holders and users of protected information in the adoption, application and governance of rules of information law.

Undoubtedly, digitalisation affects the entire field of law and challenges the fundamental norms, assumptions, practices, etc. within *inter alia* contract law, administrative law, health law, maritime law, construction law and competition law. However, for the purpose of the project of elaborating a legal methodology of digitalisation, we assume that the challenges of digitalisation first surfaced in information law and in particular in copyright law. Accordingly, most examples of how to cope legally with digitalisation are found within this legal field and it thus provides the most obvious cases of assessing the consequences of the legal choices. It is the proposition of this project that by studying the impact of digitalisation within the field of copyright law, it is possible to deduce and identify methodological shifts of general significance.

1.1 Characteristics of Copyright Law

Intellectual property rights (IPRs) grant exclusive rights in information such as original works or databases which represent a substantial investment, or inventions to stimulate creativity and innovation. IPRs enjoy protection like other

1 Arthur J Cockfield, 'Towards a Law and Technology Theory' (2003) 30 Man LJ 383.

DOI: 10.4324/9781003283881-3

types of property rights according to the Charter of Fundamental Rights of the European Union (CFREU), Art. 17(2). Legislation is based on a balancing of interests between creators of information and users, and even though exclusivity enables right holders to price products or processes which incorporate the protected element above marginal costs, the societal costs are expected to be offset by an increase in overall consumer welfare.

Rights in information are creatures of statutory law. As "islands of exclusivity in oceans of liberty", IPRs normally presuppose a basis in positive law (international conventions, regional (EU) rules and national acts). This is also the thrust of the CFREU[2] Art. 52(1): "Any limitation on the exercise of the rights and freedoms recognized by this Charter must be provided for by law" and "subject to the principle of proportionality".

Even though the international legal cooperation in the field of IPRs goes back to the Paris and Berne Conventions from the 1880s, the law has developed nationally or territorially. "Statutory basis" has traditionally translated inevitably into *national* laws. For the EU Member States, the harmonisation of IPRs through common rules has come a long way since the first Directive on the protection of computer programs was adopted in 1991. Today, more than 20 directives and regulations have been issued in the areas of copyright, trademarks, designs and patents. Add to this a significant number of decisions from the Court of Justice of the European Union (CJEU) based on those directives and regulations, and it becomes clear that the room for "national" rulemaking has been highly circumscribed when compared to the traditional starting point of free-standing national states.[3] Furthermore, important limits on the wriggling room for national courts and lawmakers also follow from the general principles developed by the CJEU, such as the principles of *effet utile* or proportionality. Still, even though EU harmonisation has changed the perspective from "national" and "international" to "regional", IPRs are still basically limited to the territory of individual states, enforcement remains mostly national and national laws provide the backdrop to the application of common solutions unless EU harmonisation has taken place.

2 Digitalisation *in Action*

The following sections describe some of the strategies legislators and courts have adopted to deal with the challenges arising out of digitalisation.

2 Charter of Fundamental Rights of the European Union (Consolidated version) [2016] OJ 2016/C 202/391.

3 Eleonora Rosati, Copyright Harmonization and CJEU Role and Action (2019) 22 seq identifies and analyses 98 cases from the CJEU which deal directly with copyright provisions issued between 1998 (when the first decisions concerning interpretation of the 1992 Rental and Lending Rights Directive were issued) and August 2018.

2.1 Legislating Digitalisation

Beginning in the early 1990s, the EU has been actively legislating in the field of IPRs and especially in the area of copyright. During these 30 years of lawmaking, special rules on new types of works which are predominantly digital (computer programs and databases) have been added, or new uses which have arisen with digital technologies or have changed radically due to digital technologies (internet, satellite and cable) or modalities of rights exploitation which have been made possible by the internet (online licensing and portability) have been dealt with.[4] No directive has been repealed, but new layers have been added.

One of the most important challenges to the legislator has been how to "future-proof" legislation making it adaptable to coming changes. This is an inherently complicated task, as technological development is a dynamic process, which implies that the technological possibilities constantly continue to provide new possibilities and challenges. The tension between static regulation and dynamic technology is systemic and inevitable. For EU law these problems are exacerbated by the fact that EU legislation is notoriously hard to change. For a directive or regulation to be amended and new legislation to be put into place, most of the 27 EU Member States have to agree.[5]

Every now and then, however, major legislative initiatives are undertaken at the EU level. One of the most spectacular ones is, of course, the rise of the protection of personal data which culminated with the adoption of the General

4 EU directives in the field of copyright include: Directive 2001/29/EC of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society [2001] OJ L 167/10 ("InfoSoc Directive"); Directive 2006/115/EC of 12 December 2006 on rental right and lending right and on certain rights related to copyright in the field of intellectual property [2006] OJ L 376/28 ("Rental and Lending Directive"); Council Directive 93/83/EEC of 27 September 1993 on the coordination of certain rules concerning copyright and rights related to copyright applicable to satellite broadcasting and cable retransmission [1993] OJ L 248/15 ("Satellite and Cable Directive"); Directive 2009/24/EC of 23 April 2009 on the legal protection of computer programs [2009] OJ L 111/16 ("Software Directive"); Corrigendum to Directive 2004/48/EC of 29 April 2004 on the enforcement of intellectual property rights [2004] OJ L 195/16 ("IPRED"); Directive 96/9/EC of 11 March 1996 on the legal protection of databases [1996] OJ L 77/20 ("Database Directive"); Directive 2006/116/EC of 12 December 2006 on the term of protection of copyright and certain related rights [2011] OJ L 372/12 ("Term Directive"); Directive 2012/28/EU of the Council of 25 October 2012 on certain permitted uses of orphan works [2012] OJ L 299/5 ("Orphan Works Directive"); Directive 2014/26/EU of 26 February 2014 on collective management of copyright and related rights and multi-territorial licensing of rights in musical works for online use in the internal market [2014] OJ L 84/72 ("CRM Directive"); Regulation (EU) 2017/1128 of 14 June 2017 on cross-border portability of online content services in the internal market [2017] OJ L 168/1; and Directive (EU) 2019/790 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC [2019] OJ L 130/92 ("DSM Directive").

5 Normally, a qualified majority is needed, that is, 55% of Member States, representing at least 65% of the EU population, vote in favour, see TFEU art 238.

Data Protection Regulation (GDPR) in 2016. The GDPR also took account of developments in case law. Most importantly, the "right to be forgotten" was developed by the CJEU in *Google Spain* based on the provisions in the Charter.[6] These principles are now regulated explicitly in GDPR Art. 17 ("the right to erasure") where the right has even been strengthened in the light of the special challenges in the online environment (point 65). In this way, feedback loops may exist between legislation and judicial practice. Often, however, "changes" are not transposed into the black letters of the law but have to be extrapolated from case law. For this reason, much depends on the ability of legislation to provide guidance for the development in case law from the CJEU and national courts and at the same to allow for flexibility.

2.1.1 New Subject-Matter: Sui Generis *Regulation or Adaptation of Existing Rules?*

One of the most basic challenges to legislators arising out of digitalisation has been how to protect new types of digital creations—whether to create new systems or whether to fit the new types into the already existing ones. The protection in IP law of computer programs and databases constitute two prime examples of these difficulties.

Originally, the inclination was to pursue new types of protection systems. For computer programs, WIPO proposed the Model Provisions on the Protection of Computer Software in 1978.[7] For databases the EU directive from 1996 inspired a similar development.[8]

The proposal on computer programs did not gain traction internationally, and during the 1980s copyright law became the favoured model.[9] Eventually, however, it was decided to address the challenges to copyright of digitalisation in a single legal instrument, viz. the WIPO Copyright Treaty (WCT) from 1996. The WCT obliges states to offer protection to computer programs and databases, to the "making available" on the internet of protected material, and to technological protection measures (TPMs) and digital rights management (DRM). Also, it was made clear that copyright protection extends to expressions and not to ideas, procedures, methods of operation or mathematical concepts as such.

6 Case C-131/12 *Google Spain SL og Google Inc v Agencia Española de Protección de Datos (AEPD) og Mario Costeja González* (CJEU, 13 May 2014) para 99.

7 WIPO, 'Model Provisions on the Protection of Computer Software' (1978) 14 M Rev of the WIPO 6.

8 See WIPO, 'Basic Proposal for the Substantive Provisions of the Treaty on Intellectual Property in Respect of Databases to be Considered by the Diplomatic Conference' CRNR/DC/6 <www.wipo.int/meetings/en/doc_details.jsp?doc_id=2487> accessed 17 May 2021; see also infra.

9 For WIPO see WIPO, 'Group of Experts on the Copyright Aspects of the Protection of Computer Software (Geneva, February 25 to March 1, 1985)' (1985) 21 M Rev of the WIPO 146; see also the anonymous text 'Topic 1: International IP Protection of Software: History, Purpose and Challenges' WIPO/IP/CM/07/WWW[82573] <www.wipo.int/meetings/en/doc_details.jsp?doc_id=82573> accessed 17 May 2021.

Similarly, the TRIPS Agreement provides for a comprehensive copyright system for the protection of both computer programs and databases.[10]

At the EU level, the approach towards digitalisation has been more ad hoc, which has led to a fragmented legal picture. In contrast to the model of the WCT, the EU (as it became) issued a Directive on the legal protection of computer programs in 1991 and a Directive on the legal protection of databases in 1996.

These directives illustrate the difficulties of *sui generis* rulemaking. The term "computer program" as it is used in the Computer Programs Directive, for example, also includes preparatory design work leading to the development of a computer program[11] and covers both source code and object code.[12] It does not, however, include the graphical user interface, which cannot be protected specifically by copyright in computer programs.[13] The user interface may, however, be protected separately depending on its content (picture or text) according to the non-harmonised rules in general copyright.[14] In this way, even though the Directive is meant to protect "computer programs" specifically, it does not provide for "full" protection for computer programs.

Furthermore, even though the Database Directive and Computer Programs Directive are limited to their specific subject-matters, they obviously have to deal with some of the same basic issues such as the "object of protection" or exhaustion. As for the content of the substantive provision, one would therefore expect the basic norms to be similar. However, important and inexplicable differences appear. For instance, why does the Database Directive not contain the limitation found in the Computer Programs Directive Art. 1 (and in the WCT) for "ideas and principles"? Should courts engage in a horizontal analysis and apply the limitation to databases *by analogy*?[15] Or should courts rely on the principle of *e contrario* analysis? In practice, the CJEU has relied on the WCT and TRIPS (see later) for the interpretation of the Computer Programs Directive, and in this way the international legal framework has offered some solace for the fragmented EU system. However, as will be seen later, in regards to exhaustion, the lack of coordination between the EU directives continues to cause problems.

10 See TRIPS art 10 on "Computer Programs and Compilations of Data".

11 Case C-406/10 *SAS Institute Inc v World Programming Ltd* (CJEU, 2 May 2012) para 36.

12 Case C-393/09 *Bezpečnostní softwarová asociace—Svaz softwarové ochrany v Ministerstvo kultury* [2010] ECR I-13971, para 35.

13 Ibid para 42.

14 Still, no general "copyright Directive" has been issued. In practice, however, the InfoSoc Directive (n 4) has served as the basis for the harmonisation of larger areas of copyright law including the central issues of originality, see infra.

15 This problem is acute. The *sui generis* protection offered by the Database Directive (n 4) to prevent "the repeated and systematic extraction and/or re-utilization of insubstantial parts may" (art 7) could arguably be used to deny access to non-substantial parts of the database, that is, to the "data" themselves even though this is hard to align with the Directive itself (recital 44) and TRIPS art 10(2).

The legal protection of computer programs has also given rise to difficulties in patent law. The European Patent Convention (EPC) Art. 52 provides that computer programs *as such* do not constitute inventions and can for that reason not enjoy protection under the Convention. Understanding this limitation, and in particular finding the fine line between patentable "computer programs" and unpatentable "computer programs as such", has proven to be most difficult in practice. To settle the matter it was proposed to amend the EPC and to repeal the limitation for computer programs. It was not the intention to expand the patentable subject-matter but to reflect the development in the practice of the EPO Boards of Appeal that had relied on the general principles of the EPC rather than the specific limitation to filter out computer programs with no technical effect from the Convention.[16] The result of the proposal would thus be to rely on the general principles rather than on the specific limitation. The proposal failed and the special rules were kept.

In the aftermath of the revision of the EPC, the EU proposed a Directive of the European Parliament and of the Council on the patentability of computer-implemented inventions.[17] The proposal contained very detailed rules on subject-matter, conditions for patentability, forms of claims and instructed the Members States to implement those provisions via their national and otherwise mostly unharmonised patent acts. This directive also eventually ran into the sand. We think luckily so. The idea of regulating a specific and contentious corner of patent law via detailed provisions, and to furthermore do so within the already institutionally complicated backwaters between the EPC, the EU and the national states was doomed to failure. The basic "instinct" of the EU legislator to deal with the challenges from digitalisation via specific and detailed rules reflects, however, the development in copyright described earlier.

2.1.2 Designing Flexibility

The InfoSoc Directive came into force in June 2001. The process which led to the Directive began in the 1990s and this in turn led to the first proposal from the Commission in 1997. This is just around the time the internet changed from a little-known computer network used by academics, with commercial actors entering the scene. Google was founded in 1998 and Facebook in 2004. In this way, most of the practices that we have come to associate with the "Information Society" and which the Directive was created to deal with, did not really exist at the time when the baselines of the Directive were formulated.

16 See the Administrative Council, 'Basic Proposal for the Revision of the European Patent Convention' MR/2/00, 43ff <http://documents.epo.org/projects/babylon/eponet.nsf/0/43F40380331CE97CC125727A0039243C/$File/00002a_en.pdf> accessed 17 May 2021.

17 Commission, 'Proposal for a Directive of the European Parliament and of the Council on the Patentability of Computer-implemented Inventions' COM (2002) 92 final; see definitions in art 2.

Even though the InfoSoc Directive came too early for the framers to know much of the technology and ways of communication and business which came to define many of the legal issues which the Directive would be called upon to resolve, it is clear that the framers were very much aware that something was afoot and that the Directive was being developed at a transformative period in time for the use of copyright protected material. Thus, at the same time as it became clear that the basic rules which had been enacted by the previous directives were to continue to apply, it was also stated that

> (25) The legal uncertainty regarding the nature and the level of protection of acts of on-demand transmission of copyright works and subject-matter protected by related rights over networks should be overcome by providing for harmonised protection at Community level. It should be made clear that all rightholders recognised by this Directive should have an exclusive right to make available to the public copyright works or any other subject-matter by way of interactive on-demand transmissions.

When read in conjunction with recital 20 it seems clear that the framers of the Directive were calling for a broad application of the traditional tools. In the face of the legal uncertainty regarding the technological and legal developments, rights should be interpreted in an expansive way. This is also the thrust of the statement in recital 4:

> A harmonised legal framework on copyright and related rights, through *increased legal certainty and while providing for a high level of protection of intellectual property*, will foster substantial investment in creativity and innovation, including network infrastructure, and lead in turn to growth and increased competitiveness of European industry, both in the area of content provision and information technology and more generally across a wide range of industrial and cultural sectors. This will safeguard employment and encourage new job creation.
>
> (emphasis added)

As seen from the perspective of right holders, an expansive interpretation of the rules of exclusivity with a view to providing a "high level of protection" should be applied.

As seen from the users' perspective, the response in the face of the uncertainty is rather different. As is made clear in recital 32, the Directive provides *for an exhaustive enumeration of exceptions and limitations to the reproduction right and the right of communication to the public*. The list is found in Art. 5(1)—(4). To bring the point even further, Art. 5(5) restates the three-step test and provides that:

> The exceptions and limitations provided for in paragraphs 1, 2, 3 and 4 shall only be applied in certain special cases which do not conflict with a normal

> exploitation of the work or other subject-matter and do not unreasonably prejudice the legitimate interests of the right holder.

Unlike the test as developed in the Berne Convention Art. 9(2) and as found in TRIPS Art. 13, the InfoSoc Directive uses the test as a "limitation of limitations and exception". The effect is a double-cap on limitations and exceptions.

Important limits on the wriggling room for national courts and lawmakers also follow from the general principles developed by the CJEU, such as the principles of *effet utile* or proportionality. It was for this reason that the CJEU in *Funke Medien* explained how the Member States' discretion in the implementation of the exceptions and limitations provided for in the InfoSoc Directive must be exercised within the limits imposed by EU law and that this means that the spaces seemingly left open by the Directive are in fact highly circumscribed by EU law.[18]

The closed list of limitations and exceptions in the InfoSoc Directive has proven to be highly problematic. First and foremost, the list makes copyright inflexible in the light of technological changes, and the inability of limitations and exceptions to "expand" alongside exclusivity constantly skews protection to the benefit of right holders. Pushing in the same direction, the CJEU has on several occasions made clear that limitations and exceptions should be interpreted narrowly.[19] Legally speaking, these strategies of the court have limited the "breathing space" of the limitations and exception.

Moreover, the effects of the limitations and exceptions depend on the ability of users to exercise their "users' rights". In this way users and right holders are in the same boat. According to the DSM Directive[20] Art. 17(7), Member States shall ensure that users are able to rely on the exceptions and limitations. Also, the Directive shall "in no way affect legitimate uses" and platforms shall inform users that they can use works under limitations and exceptions (Art. 17(9)). In this way, the DSM Directive provides users with procedural safeguards. As pointed out by one of us it is, however, far from clear how users should enforce their rights under the Directive.[21] Importantly, the DSM Directive fails to specify the legal

18 Case C-469/17 *Funke Medien NRW GmbH v Bundesrepublik Deutschland* (CJEU, 29 July 2019) paras 46 and 47; see also Case C-476/17 *Pelham GmbH and Others v Ralf Hütter and Florian Schneider-Esleben* (CJEU, 29 July 2019); and Case C-516/17 *Spiegel Online GmbH v Volker Beck* (CJEU, 29 July 2019).

19 For example, Case C-527/15 *Stichting Brein v Jack Frederik Wullems* (CJEU, 26 April 2017) paras 62 seq and C-265/16 *VCAST Limited v RTI SpA* (CJEU, 29 November 2017) paras 31 seq; see also Case C-435/12 *ACI Adam BV and Others v Stichting de Thuiskopie and Stichting Onderhandelingen Thuiskopie vergoeding* (CJEU, 10 April 2014) paras 20ff.

20 DSM Directive (n 4).

21 Sebastian F Schwemer and Jens Schovsbo, 'What is Left of User Rights?—Algorithmic Copyright Enforcement and Free Speech in the Light of the Art 17 Regime' in Paul Torremans (ed), *Intellectual Property Law and Human Rights* (4th ed, 2020) Wolters Kluwer, 569–89, available at SSRN: <https://ssrn.com/abstract=3507542> accessed 17 May 2021.

consequences of a platform's failure to live up to its obligations to ensure user rights. Also in this way, the EU copyright system reflects the traditional system known from the international framework and in particular TRIPS, which has for many years boosted enforcement of right holders' rights but has taken little notice of the interests of users of protected information. In this way, the DSM Directive can be criticised for taking a one-sided view on the problems of under-enforcement of copyright in the sense that it aims to strengthen right holders' interests but disregards users' interests. The lack of attention to the enforcement of the rights and interests of users undermines the effects of the limitations and exceptions.[22]

2.1.3 Assessment

If one compares the approach of the EU legislator to that of the WCT, the contrast is striking. The WCT represents a comprehensive and broad approach to the technological challenges. Importantly, this Treaty, in addition to extending protection, also points out how copyright should provide for "adequate solutions to the questions raised by new economic, social, cultural and technological developments" and that care should be taken to recognise both the "outstanding significance of copyright protection as an incentive for literary and artistic creation" and to maintain a balance between the rights of authors and the larger public interest".[23]

Arguably, the EU has not yet found a way to deal legislatively with the challenges which arise from the existing *acquis*. The DSM Directive which was adopted almost two decades after the InfoSoc Directive is meant to update the EU copyright *acquis* and to take up where InfoSoc left off. It too was adopted at a time which was characterised by "Rapid technological developments [which] continue to transform the way works and other subject matter are created, produced, distributed and exploited" (point 3). As "new business models and new actors continue to emerge. Relevant legislation needs to be future-proof so as not to restrict technological development" (ibid.).

Following in the tradition of EU lawmaking in the field of copyright, the DSM Directive does not challenge the existing framework. Instead it adapts and supplements the existing Union copyright framework, while keeping a "high level" of protection for copyright and related rights.[24] Interestingly, the Directive includes important provisions aimed at the exercise of copyright both in regards to collective management organisations and individual right holders. The latter Part 3 of

22 Ibid and more on this later.

23 WIPO Copyright Treaty (adopted 20 December 1996, entered into force 6 March 2002) 2186 UNTS 121 (ICCPR) Preamble.

24 For text and data mining, however, the Database Directive (n 4) and InfoSoc Directive (n 4) are amended to allow for text and data mining for purpose of illustration for teaching or scientific research. The reason stated is that this is needed to further "cross-border uses, which are becoming increasingly important in the digital environment" (point 5).

the Directive contains novel rules to protect individual right holders in contractual dealings (see e.g. Art. 20 which provides for a "Contract adjustment mechanism" and Art. 22 providing for a "Right of revocation"). Also, the Directive has recast the limitations and exceptions for the specific purposes of quotation, criticism, review, caricature, parody or pastiche as *unwaiveable Users' Rights*. These aspects of the Directive represent important and interesting developments which combine aspects of substantive rights and procedural law. The Directive, however, does little to alleviate the tensions which arise from the underlying directives.

2.2 Adjudicating Digitalisation

It is generally acknowledged that the CJEU has played a central role in the adaption of the copyright law *acquis*. As seen in the light of the previous discussions, this is hardly surprising. Given the difficulties in creating new rules or amending existing ones, much of the legal development necessarily falls on the Court. This is in itself an important observation, and dealing with the developments of the law by the CJEU constitutes a major methodological challenge to many national courts, also giving rise to broader debates about the legitimacy of the development of EU law.

The CJEU has been instrumental in developing information law in many different ways. With regard to copyright, the Court has more or less single-handedly developed a common EU-wide principle of originality,[25] redefined the rights of distribution[26] and communication,[27] the principles for ownership of copyright,[28] and interpreted the rules of limitations and exceptions in copyright in a way that leaves very little room for national variations.[29] In the following, however, we focus on just two examples: online exhaustion and hyperlinking. These are

25 Case C-5/08 *Infopaq International A/S v Danske Dagblades Forening* [2009] ECR I-6569 followed by, for example, C-403/08 and C-429/08 *Football Association Premier League Ltd and Others v QC Leisure and Others* and *Karen Murphy v Media Protection Services Ltd* [2011] ECR I-9083 (on football matches); Case C-145/10 *Eva-Maria Painer v Standard VerlagsGmbH* (CJEU, 7 March 2013) (on photographs); Case C-393/09 *Bezpečnostní softwarová asociace* (n 12) (on computer programs); Case C-406/10 *SAS Institute Inc v World Programming Ltd* (CJEU, 2 May 2012) (on computer programs); Case C-683/17 *Cofemel—Sociedade de Vestuário SA mod G-Star Raw CV* (CJEU, 12 September 2019) (on works of applied art); and Case C-469/17 *Funke Medien* (n 18) (on military status reports).

26 Case C-5/11 *Titus Alexander Jochen Donner* (CJEU, 21 June 2012); Case C 98/13 *Martin Blomqvist v Rolex SA and Manufacture des Montres Rolex SA* (CJEU, 6 February 2014); Case C-516/13 *Dimensione Direct Sales Srl and Michele Labianca v Knoll International SpA* (CJEU, 13 May 2015).

27 Joined Cases C-403/08 and C-429/08 *Football Association* (n 25); Case C-610/15 *Stitchting Brein v Ziggo* (CJEU, 14 June 2017); Case C-527/15 *Stichting Brein v Jack Frederik Wullems* (CJEU, 26 April 2017).

28 Case C-277/10 *Martin Luksan v Petrus van der Let* (CJEU, 9 February 2012).

29 Case C-476/17 *Pelham* (n 18); Case C-469/17 *Funke Medien* (n 18); Case C-516/17 *Spiegel Online* (n 18).

intrinsically linked to digitalisation but involve some of copyright's traditional concepts, which were not designed by the EU directives to deal with modern challenges but where solutions had to be invented by the CJEU, which in both instances had to "bend over . . . in order to fit what is essentially a square peg into a 'hexagonal hole'".[30]

2.2.1 Online Exhaustion

The principle of exhaustion regulates the relationship between holders of IP rights in a product and the buyer of such a product. According to the principle, as it has been developed in EU law, once a product has been put on the market in the EEA by the right holder or with his/her consent, the right holder loses his/her "right of distribution" and cannot control (via IPRs) the further resale of that product; the "first (legal) sale" exhausts (some of) the IP rights.

Originally, the exhaustion principle was developed in Germany around 1900[31] to prevent the enforcement via IPRs of abusive practices such as resale price maintenance in the sale of trademark protected goods.[32] Later on it came to serve as a limitation in law to a general right of distribution. In this way, the result became a statutory "package" consisting of a broad right of exclusivity and a corresponding limitation. The right of distribution and the exhaustion principle were conceived to work in tandem and as defined by IP *legislation* rather than by the "will of the parties" (contract).[33]

Importantly, following this legislative model, both exclusivity and limitation are statutory law. Therefore, it is not open to the party to "contract around" the principle. In other words, the law leaves the right holder with the choice of whether or not to put the product on the market. Once that decision has been

30 CL Saw, 'Linking on the Internet and Copyright Liability: A Clarion Call for Doctrinal Clarity and Legal Certainty' (2018) 49 IIC 536 (writing on hyperlinking, see later).

31 The literature is abundant; see (still) Friedrich-Karl Beier, 'Territoriality of Trademark Law and International Trade' (1970) 1 IIC 48 and as some of the latest analyses Reto M Hilty, 'Kontrolle der digitalen Werknutzung zwischen Vertrag und Erschöpfung [Control of Digital Use of Works between Contract and Exhaustion]' (2018) 120 GRUR 865 and Reto M Hilty, 'Legal Concept of "Exhaustion": Exhausted?' in Niklas Bruun et al. (eds), *Transition and Coherence in Intellectual Property Law—Essays in Honour of Annette Kur* (2021) Cambridge University Press.

32 Unlike in contract law (the principle of "privity of contracts") enforcement via IPRs is not limited to the parties to an agreement. If allowed to rely on IPRs to enforce contractual claims, right holders are able to bring action even against third parties such as the buyers of protected products. The rule of exhaustion prevents this and in this way limits the effects of the agreement to the parties; see more in Jens Schovsbo and Thomas Riis, 'Concurrent Liability in Contract and Intellectual Property Law: Licensing Agreements in Light of Case C-666/18 IT Development SAS' (2020) 69 GRUR Int 989.

33 As it has been the tradition in, for example, France and the United Kingdom, see Jens Schovsbo, 'Exhaustion of Rights and Common Principles of European Intellectual Property Law' in Ansgar Ohly (ed), *Common Principles of European Intellectual Property Law* (2010) Mohr Siebeck.

made, the legal effects of the marketing are basically predefined by the legislation and the buyer of the product has a right by law to resell the product. As seen from an EU perspective, the principle was developed by the CJEU in a series of judgements in the 1970s based on the rules of the free movement of goods in the (as it were) EC Treaty, and as such the principle was instrumental in securing parallel importation in IP protected goods between EC (later EEA) countries.[34] It has since been incorporated into EU law via directives and limitations, and a general principle now exists both in copyright, design and trademark law[35] based on the German model and driven by the central aim of securing the internal market.

At the time when the exhaustion principle was first developed in German law and applied by the CJEU in the cases regarding parallel importation, there was no doubt that the principle dealt with the distribution of *physical copies* of works: books, movies, branded goods, pharmaceuticals, etc. When asked in 2011 in *UsedSoft*[36] whether the exhaustion principle applied to computer programs in digital form it was therefore no surprise that the CJEU in its judgement first restated the baseline in international copyright law (i.e. the WCT), viz. that

> (para 7) . . . the expressions "copies" and "original and copies" being subject to the right of distribution and the right of rental under the said Articles, refer exclusively to fixed copies that can be put into circulation as tangible objects.

The reference to "fixed copies" clearly anchors exhaustion in the realm of transaction with physical copies of works such as books or CDs containing copyright protected computer programs. It was with this starting point in mind, that the Court next turned to the rule of exhaustion in the Computer Programs Directive Art. 4(2):

> The first sale in the Community of a copy of a program by the rightholder or with his consent shall exhaust the distribution right within the Community of that copy, with the exception of the right to control further rental of the program or a copy thereof.

34 The principle of exhaustion was first established in the 1974 Centrafarm decisions; see Case C-15/74 *Centrafarm BV and Adriaan de Peijper v Sterling Drug* [1974] ECR I-1147 and Case C-16/74 *Centrafarm BV and Adriaan de Peijper v Winthrop BV* [1974] ECR I-1183.

35 See by way of example Directive (EU) 2015/2436 of 16 December 2015 to approximate the laws of the Member States relating to trademarks [2015] OJ L336/1, art 15 ("Exhaustion") which limits the "right of distribution" provided for in art 10. In patent law a general principle does not exist. For biological material, a rule on exhaustion is found in Directive 98/44/EC of 6 July 1998 on the legal protection of biotechnological inventions [1998] OJ L213/13, art 10.

36 Case C-128/11 *UsedSoft GmbH v Oracle International Corp* (CJEU, 3 July 2012).

As seen in the light of tradition and the WCT, it would seem a foregone conclusion that the Court would not find the distribution via download of copies to imply exhaustion as no "tangible objects" were put into circulation. However, as is well known, the Court arrived at the opposite conclusion: By granting its users a non-exclusive and non-transferable user right for an unlimited period for the program in question, the right holder (the company Oracle) had in fact *sold a copy* of the program to the user. In such a case, the Court explained,

> it makes no difference . . . whether the copy of the computer program was made available to the customer by the right holder concerned by means of a download from the right holder's website or by means of a material medium such as a CD-ROM or DVD.
>
> (para 47)

Having established that the transaction constituted a "sale" in legal terms, the Court next explained that the distribution of the work (download from the cloud) which had begun as an act of "communication to the public" was "changed" into "an act of distribution" (para 52). Presented with the "sale of a copy" and a claim based on a "right of distribution", the Court concluded that exhaustions had taken place.[37] Since the transaction in *UsedSoft* involved the "sale of a copy" that Court was also able to sidestep the remark in point 29 of the InfoSoc Directive that "the question of exhaustion does not arise in the case of services and on-line services in particular".

In 2018, the CJEU was asked in *Tom Kabinet* whether the *UsedSoft* principles applied to e-books under the InfoSoc Directive. This time around, the Court declined to follow its ruling in *UsedSoft*. Or rather, it boxed the *UsedSoft* case to be exclusively about computer programs protected by the Computer Programs Directive. For e-books which are not protected under the Computer Programs Directive but according to the InfoSoc Directive, the Court explained that the "change" in para 52 of *UsedSoft* from communication to the public to distribution did not take place. To explain the difference the Court remarked that unlike the Computer Programs Directive the EU legislator had not intended by the InfoSoc Directive to assimilate tangible and intangible copies of works (para 55 et seq.) Furthermore, the Court explained that the economic realities are different for computer programs and for books. For books, a market for the sale of used e-books would seriously affect the sale of new physical copies of books whereas the market for software would not be much affected by the sale of used programs (para 58). In this way, an application of the exhaustion

37 See Ole-Andreas Rognstad, 'Legally Flawed but Politically Sound? Digital Exhaustion of Copyright in Europe after UsedSoft' (2014) 1 Oslo Law Review 1 (pointing out *inter alia* that it is problematic that the Court seems to think that this conclusion follows "inevitably" from the principle of exhaustion as this was developed from the physical world).

principle would not result in the intended balance between creators' and users' interests—the scale would tip.

As seen from a legal perspective the two decisions are very hard to align. Firstly, the central para 52 of *UsedSoft* on the "change" did in fact concern the InfoSoc Directive (and indeed the WCT) which was at stake in *Tom Kabinet*. At this point, *Tom Kabinet* comes close to overruling *UsedSoft*. Secondly, the argument that the legislator should have intended to treat physical and electronic copies differently in InfoSoc but not in the Computer Programs Directive constitutes a break with the basic principle in copyright that protection is *abstract* and covers the work in whatever forms that work is being presented. Also the proposition that the InfoSoc Directive should consider acts done in a digital context differently from acts done in the "physical world" goes against general principle of *technological neutrality*, according to which the same rules should apply online as apply offline (see more on this later).

UsedSoft can be described as being "sound in policy but flawed in law".[38] As seen from a more general point of view, that description illustrates the difficulties the Court faced when it had to apply the rules developed for physical products to digitised ones: Should it follow the "law" strictly speaking or try to fit the square peg into the round hole? The Court did both and thus failed twice. The combined effect of *UsedSoft* and *Tom Kabinet* is that two different principles of exhaustion exist at the same time: one for computer programs and one for other types of works. Such inconsistency is not just "irritating"[39] as seen from a dogmatic point of view. It also leads to legal uncertainty for instances regarding mixed works such as books containing computer programs. More generally, however, the Court's zigzag course illustrates the difficulty with applying the exhaustion principle in a digitised environment. As pointed out by Reto Hilty, the exhaustion principle was devised to deal with the question of resale of a copy. For computer programs the central issue, however, is access to use the program.[40] The binary model of the exhaustion principle (yes/no)[41] makes the decision of whether or not exhaustion has taken place contingent on the terms of the licensing contract between the right holder and the first party to whom the use is licensed. Exhaustion thus only takes place if that contract is a "non-exclusive and non-transferable user right for an unlimited period". This makes it rather simple for the right holder to contract around exhaustion, for instance by limiting the term of the contract. In this way, *UsedSoft* illustrates both the importance of the exhaustion principle to help draw the line between the rights and interests of the right holder and the

38 As per Rognstad, ibid.

39 Ansgar Kaiser, 'Exhaustion, Distribution and Communication to the Public—The CJEU's Decision C-263/18—Tom Kabinet on E-Books and Beyond' (2020) 69 GRUR Int 489, 494.

40 Hilty, 'Legal Concept of "Exhaustion"' (n 31) 278ff.

41 Liliia Oprysk, 'Secondary Communication under the EU Copyright Acquis after Tom Kabinet: Between Exhaustion and Securing Work's Exploitation' (2020) 11 J Intell Prop Info Tech & Elec Com L 200, 213.

first and subsequent users of a computer program[42] and how any effects of the exhaustion principle may well evaporate into the thin air of the software licensing agreement.[43]

2.2.2 Linking

It follows from the InfoSoc Directive Art. 3 that Member States shall provide authors with "the exclusive right to authorise or prohibit *any communication to the public of their works*".

The Directive is based on principles and rules already laid down in the directives in force at the time of the adoption in 2001 (para 20). Rather than making new rules, the Directive "develops those [known] principles and rules and places them in the context of the information society" (ibid.). As far as the author's right of communication to the public was concerned it is, furthermore, stated that this right

> should be understood in a broad sense covering all communication to the public not present at the place where the communication originates. This right should cover any such transmission or retransmission of a work to the public by wire or wireless means, including broadcasting.

As already explained, the InfoSoc Directive was devised in the mid-1990s. At that time, many of the "modern" forms of uses made possible by digitalisation which we today consider to be completely ordinary and uncontroversial had yet to emerge.[44] Linking constitutes a prime example of this. Around the time of the adoption of the Directive, national courts and legal doctrine struggled to fit linking into the copyright paradigm. The basic difficulty was whether to see the setting up of hyperlinks as an (active) act, which in itself violated copyright (communication to the public or even the reproduction right), or whether it was rightly to be understood as a *contributory act*. Given these uncertainties it

42 See in particular Hilty, 'Legal Concept of "Exhaustion"' (n 31).

43 It also follows from *UsedSoft* para 81 and 82 that the right holder cannot limit the effect of exhaustion by contract to restrict the ability of subsequent users from using their program. This reflects the traditional starting point that exhaustion is a "statutory creature" and that parties cannot contract around it. This, however, does not affect the ability of the right holder to tailor fit the agreement with the first user to "get around" exhaustion.

44 According to Wikipedia,

> [t]he first widely used open protocol that included hyperlinks from any Internet site to any other Internet site was the Gopher protocol from 1991. It was soon eclipsed by HTML after the 1993 release of the Mosaic browser (which could handle Gopher links as well as HTML links). HTML's advantage was the ability to mix graphics, text, and hyperlinks, unlike Gopher, which just had menu-structured text and hyperlinks.

was hardly a surprise that the EU legislator did not put its feet down firmly when adopting the InfoSoc Directive but left it for future case law to draw the line. As will be shown, this in turn led to a long period of fundamental uncertainty about the state of the law in what became a central part of modern copyright law.[45]

Traditionally, copyright infringement involves someone who engages actively with the work in making copies, distributing these or in communicating the work to the public either directly (e.g. performance) or indirectly (e.g. on-demand transmission). These forms of infringements presuppose active acts of the infringers themselves. By this token, Art. 3 prohibits the *act of* communication of the work to the public.

Linking differs from this schema. The person who sets up the link to protected material (music, text, films, etc.) does not thereby engage directly with the work but merely points the potential user the way to the work and thereby makes it easier to find. If the work to which the link refers is taken down, the link is "dead". Also there is no doubt that the person who uploads the work in the first place and those who download it (be that via the link or by independent effort) commit acts covered by the right holder's copyright by making the work available and/or making a copy (the reproduction right). In this way, traditional copyright analyses would arguably see linking as constituting a potential contributory infringement. Since contributory infringements were (and remain) outside of the EU copyright *acquis*, this analysis would also leave linking for national law.

The two central decisions from the CJEU on linking are *Svensson* from 2014[46] and *GS Media* from 2016.[47] At the time when *Svensson* was decided, the CJEU had already found in *ITV Broadcasting* (2013) that communication to the public includes two cumulative criteria, namely, an "act of communication" of a work and the communication of that work to a "public".[48] Before that, in 2006 the Court had stated in *SGAE* that for there to be an "act of communication", it is sufficient that a work is made available to a public in such a way that the persons forming that public may access it, irrespective of whether they avail themselves of that opportunity.[49] When *Svensson* was brought before the Court, it had already established a broad scope of exclusivity. Protection, however, still hinged on an active behaviour on the side of the alleged infringer—an *act* of communication.

In *Svensson*, however, the Court found a bridge from Art. 3 to linking. The case involved the providing of hyperlinks to protected material which had already been made (and remained) available for the general public by the right holders (i.e. to

45 Again the literature is abundant. See for an overview, for example, Saw (n 30).

46 Case C-466/12 *Nils Svensson m.fl. v Retriever Sverige AB* (CJEU, 13 February 2014).

47 Case C-160/15 *GS Media BV mod Sanoma Media Netherlands BV m.fl.* (CJEU, 8 September 2016).

48 Case C-607/11 *ITV Broadcasting Ltd and Others v TVCatchUp Ltd* [2013] (CJEU, 7 March 2013) paras 21 and 31.

49 Case C-306/05 *Sociedad General de Autores y Editores de España (SGAE) v Rafael Hoteles SA* [2006] ECR I-11519, para 43.

"legal material"). The Court found, first, that providing clickable links to protected works did "make the works available". Despite the indirect way in which linking works, it was to be considered as an "act". At the same time, however, the Court found that since the material to which the linking had been established was freely available on another website, the links did not make the works available "to the public" (i.e. the second prong of *ITV Broadcasting*).

Svensson represents a dramatic expansion of the reach of Art. 3: Even though linking was not foreseen by the legislator and despite the wording of the norm and the traditional interpretation, the Court found linking to be covered by the exclusivity. The ruling also explains why. Clearly the Court felt vindicated by the purposes of the Directive and the aim of establishing protection at a high level and the call for expansive interpretation. Also, by keeping links to legal material outside of the reach of copyright, the decision enabled internet users to continue to set up links to material which had already been made available by the right holders. The decision, however, left unanswered how to deal with links to material which was not already freely available for the public. The decision clearly seems to imply that linking is only permitted to material which is already freely available. The effects, however, of considering linking to other material to be covered by copyright would imply a general risk for everyone who makes links and also lead to big problems in establishing whether the materiel to which one sets up a link is legitimate or not. These factors in turn could cause a freezing effect on linking. Also by relying on the "public" as the connecting factor, the Court cast the net so wide as to include both the use by private and commercial persons. The consequence of *Svensson* could thus seriously limit the possibility for everyone to use hyperlinks. Since hyperlinking constitutes one of the core technologies of the internet, copyright could in this way seriously hamper the working of the entire internet as it had come to be known and used by the mid-2000s.

These elements were elaborated on by the Court in the subsequent *GS Media* case. In this case the Court not only expanded on its reasoning, it also turned its attention to the effect on users of the broad scope of exclusivity. As linking constitutes one of the very defining technologies of the internet as we know it, these effects are important to take into account, but had not been so by the InfoSoc Directive for the same reasons the position of right holders regarding linking had not been dealt with. At the time of the formulation and adoption of the InfoSoc Directive no one had really foreseen the effects of digitalisation on copyright and on the balancing of the interests of right holders and internet users.

GS Media concerned the setting up of hyperlinks to works which had not been made available to the public by the right holder. The Court first explained that the reason no communication to the public had taken place in *Svensson* was that no communication had taken place to a *new public* (para 41). Furthermore, the Court reasoned that,

> given that the hyperlink and the website to which it refers give access to the protected work using the same technical means, namely the internet, such a

> link must be directed to a new public. Where that is not the case, in particular, due to the fact that the work is already freely available to all internet users on another website with the authorisation of the copyright holders, that act cannot be categorised as a "communication to the public" within the meaning of Article 3(1) of [the InfoSoc Directive]. Indeed, as soon as and as long as that work is freely available on the website to which the hyperlink allows access, it must be considered that, where the copyright holders of that work have consented to such a communication, they have included all internet users as the public.
>
> (para 42)

Next, and citing the concern raised by *GS Media*, the Commission and several Members States, the Court turns to the effects of a "ban" on the balance which the InfoSoc Directive seeks to establish between that freedom and the public interest on the one hand, and the interests of copyright holders in an effective protection of their intellectual property, on the other (para 44). In that regard, the Court notes,

> the internet is in fact of particular importance to freedom of expression and of information, safeguarded by article 11 of the Charter, and that hyperlinks contribute to its sound operation as well as to the exchange of opinions and information in that network characterized by the availability of immense amounts of information.

Addressing next the specific concerns a limitation of hyperlinks via copyright may have for individuals who wish to post such links, the Courts turned to the *procedural aspects* of copyright infringement, viz. how to ascertain whether the website to which links are expected to lead, provides access to works which are protected and, if necessary, whether the copyright holders of those works have consented to their posting on the internet (para 47). To address that concern, the Court resorts to one of the oldest methods in the legal tool box—which party bears the "burden of proof"? If the person who posts the link does not pursue a profit, national courts should assume that he/she does not know and to cannot reasonably know, that that work had been published on the internet without the consent of the copyright holder (para 47). By including the subjective intention of the person who posted the links (the pursuit of profit) in the analyses, the Court has injected a subjective element into the analysis of the communication to the public right which is alien to traditional copyright law.

As can be seen, the Court applies a number of different methodological tools to arrive at this surprising and unforeseen conclusion. Firstly, the Court focused on the overall object and general purpose of the norm such as the "protection at a high level" and the need to strike a "balance between users and creator interests". Secondly, developing the norm required a number of different steps: first *Svensson* laid the groundwork, then, via a suite of other decisions, *GSM Media* provided the details. Thirdly, the Court relied on general principles of fundamental rights

to establish the parameters for the overall balancing of interests. Fourthly, it focused on procedural aspects (the burden of proof).

2.3 Summing Up

Building on the examinations and evaluations earlier on how digitalisation has thus far been addressed in legislation and adjudication, in the following, we will establish and elaborate on the normative content of a legal methodology of digitalisation which we relate to what we call the four methodological shifts in legal digitalisation:

- The shift from substantive law to procedural law,
- The shift towards globalisation,
- The shift towards horizontally based law,
- The shift from state-enacted law to contract and code.

3 Methodological Shifts in Legal Digitalisation

3.1 The Shift From Substantive Law to Procedural Law

The emergence of digital networks opens up the possibility of new types of abuses and infringements. This development has shifted the practical focus from substantive law to procedural law. In the digital realm, the crucial question is not so much whether a certain online act encroaches on the rights of others because often it is evidently so. The essential issue is the probability that wrongs can be remedied and result in actual executable legal sanctions. Basically, the issues relate to the means of enforcement, which again depends on the available remedies and legal procedures facilitating the possibility of being awarded a remedy.

The problems of enforcement, and in particular, cross-border enforcement of violations on digital networks, are many and it is difficult to find adequate solutions.[50] Modern legal discourse is deeply linked to a vision of procedure as instrumental to a distinct body of substantive law,[51] and there is a natural focus on substantive law because substantive law presents the rights and wrongs. Methodologically, the digital reality and the complex problems of enforcement calls for a reconsideration of the traditional distinction between substantive and procedural law.

50 For example, Alexander Peukert, 'Transnational Intellectual Property Governance on the Internet' in this book.

51 Robert G Bone, 'Mapping the Boundaries of a Dispute: Conceptions of Ideal Lawsuit Structure from the Field Code to the Federal Rules' (1989) 89 Columbia L Rev 1, 17, and D Michael Risinger, 'Substance and Procedure Revisited with Some Afterthoughts on the Constitutional Problems of Irrebuttable Presumptions' (1982) 30(2) UCLA L Rev 189.

The concept of a "right" can be described as referring to a protected sphere of autonomy or control.[52] In this understanding, the characterisation of a "right" is related to the degree of control or autonomy that a person has in respect of a specific good.[53] According to Alf Ross, one of the leading figures of Scandinavian legal realism, the concept of right marks the individual's autonomous self-assertion.[54] This academic position is rooted in that part of legal positivism referred to as analytical positivism which is associated with the Englishmen Jeremy Bentham and perhaps especially John Austin who defined "law" as "orders backed by threats". According to the analytical positivists, the legal order has no further binding power than that which is manifested in the legal order's external constraints. Also according to Hans Kelsen, it is the threat of coercive measures carried out by public authorities that differentiates legal norms from other norms.[55]

If rights are defined as interests that are protected by the implementation of legal sanctions and remedies, then from a theoretical perspective, the concept of "rights" is devoid of independent meaning. From a practical perspective, such a position is too far-reaching. The concept of "rights" in substantive law is a tool for the technique of presentation serving exclusively systematic ends.[56] In this way, the owner of a substantive right is given an expectation that in case of infringement of the right, the legal order will make coercive measures available to the right holder which conform to the representation of the substantive right. However, for legal as well as practical reasons, enforcement of rights is a blunt instrument and full conformity between the representation of the substantive right and the enforcement of the right can never be achieved. Alf Ross admonishes not to perceive substantive rights as phenomena that are valid in themselves, and as something different from the exercise of force (judgement and execution) by which the factual and apparent use and enjoyment of the right is effectuated. If substantive law is construed as independent and isolated from the procedural rules of enforcement,[57] in the words of Alf Ross:

52 Jules L Coleman, *Risks and Wrongs* (1992) Cambridge University Press, 336.

53 Jules L Coleman and Jody Kraus, 'Rethinking the Theory of Legal Rights' (1986) 95 Yale LJ 1335, 1339.

54 Alf Ross, *Om ret og retfærdighed: En indførelse i den analytiske retsfilosofi* [On Law and Justice: An Introduction to the Analytical Philosophy of Law] (3rd edn, 1972) Nyt Nordisk Forlag, 214; see for more and in English on Alf Ross' legal philosophy and its relevance in particular to IPR Ole-Andreas Rognstad, *Property Aspects of Intellectual Property* (2018) Cambridge University Press.

55 Dhananjai Shivakumar, 'The Pure Theory as Ideal Type: Defending Kelsen on the Basis of Weberian Methodology' (1996) 105 Yale LJ 1383, 1385ff.

56 Alf Ross, 'Tü-tü' (1957) 70 Harvard L Rev 812, 825; see also Rognstand (n 54), especially 55ff, 100ff and 123ff.

57 From a practical perspective, see Thomas O Main, 'The Procedural Foundation of Substantive Law' (2010) 87 Washington University L Rev 801, 802 ("The substantive implications of procedural law are well understood. Procedure is an instrument of power that can, in a very practical sense, generate or undermine substantive rights.").

> our terminology and our ideas bear a considerable structural resemblance to primitive magic thought concerning the invocation of supernatural powers which in turn are converted into factual effects.[58]

Accordingly, a substantive right is a fragment that should be construed in connection to the available legal sanctions and remedies and the procedural system in order to determine the validity of the right.[59] The point here is that digitalisation has considerably increased the discrepancy between the expectations in respect of law enforcement created by the representation of the substantive right and the actual possible enforcement of the right. When the enforcement of rights due to digitalisation is curtailed in a number of ways, so is the substantive right.

Obviously, enforcement problems in the digital world can be addressed at the legislative level, which has also happened, most clearly in the field of intellectual property law.[60] At the dogmatic level, the enforcement problems and the conceptualisation of "rights" as reflections of not only the available legal sanctions and remedies but also the practical difficulties of enforcement suggest a more expansive style of interpretation of enforcement measures. More specifically, a style of interpretation that is oriented at reconstructing the "substantive rights" to their pre-digitalisation level.

The challenge of digitalisation in this respect is closely related to the practical difficulties of enforcement in the digital world, and especially on digital networks (enforcement errors). First, legally protected goods and services are easily copied in perfect quality and can be distributed to a large number of potential infringers in very short time. Second, it is often difficult to identify and track down actual infringers, and even if the right holder succeeds in doing so, the infringers may be located in a jurisdiction that for all practical purposes does not offer the right holder legal redress. However, it should be taken into consideration that in certain delimited internet domains enforcement errors are addressed by internet platforms that implement measures for taking down content, either following notices (notice and take down) or automatically (algorithmic enforcement). The underlying policies and the actual practices of such internet platforms may counterbalance or even reverse enforcement errors (over-enforcement).

A simple example of an approach to enforcement errors based on the so-called "multiplier principle" can illustrate how an expansive style of interpretation can remedy the challenge—for example, illegal downloads and streaming of copyright protected works take place in very large numbers. Typically, it is difficult for the right holders to identify and track down the persons behind the illegal downloads and streaming. Even when this is possible, the required resources for prosecution are usually disproportionate to what the right holder can expect in the way of an

58 Ross (n 56) 818.

59 This section is based on Thomas Riis, *Enerettigheder og vederlagsrettigheder* [Exclusive Rights and Remuneration Rights] (2005) Jurist- og Økonomforbundet, 67–69.

60 Namely, IPRED (n 4).

award if the case is won because the harm done by each infringer in many cases is of minor importance. In this scenario, the relevant sanctions are damages and criminal sanctions. By and large, the rationale behind damages is prevention and restitution and the rationale behind criminal sanctions is prevention. If perhaps only 5% of illegal downloads and streaming are detected and prosecuted and the right holder is awarded damages for economic loss (prevention) and a reasonable royalty (restitution) in respect of the actual infringements of the case, neither prevention nor restitution is restored. The same applies to criminal sanctions in respect of prevention.

The economic incentives not to infringe the rights of others decrease the higher the probabilities that damages/fines for some reason or another are not effectuated in each case. The multiplier principle is a solution of a punitive nature that aims at restoring the prevention when awarding pecuniary sanctions. Originally, the principle has been used to estimate the social optimal pecuniary sanctions in cases of enforcement errors. The optimal pecuniary sanction adjusted for enforcement errors (T) is calculated using the following formula:

$$T = eS$$

where (e) is the multiplier that is calculated as 1/p; (p) being the probability that the infringement is detected, the infringer identified and tracked down and that a pecuniary sanction is actually effectuated. (S) is the pecuniary sanction that would have been the social optimal pecuniary sanction if no enforcement errors existed.[61]

Contrary to the traditional understanding of the multiplier principle, the legal methodology of digitalisation does not include an inherent rationale of social optimal sanctions. The rationale of this part of the methodology is to adjust enforcement in the digital world so that it conforms to enforcement in the analog world, and enforcement errors also exist in the analog world. Hence, (S) should be modified to designate the pecuniary sanction that conforms to the pecuniary sanction that would have been effectuated in the analog world with ordinary enforcement errors. Accordingly, if there is a 5% probability that a pecuniary sanction is effectuated in case of infringement in the digital world, and a 50% probability that a pecuniary sanction is effectuated in the analog world, the multiplier should not be 20 as suggested by the original understanding of the multiplier principle but only 10.

Arguably, many jurisdictions will not allow an automatic application of the multiplier principle. Therefore, the numbers game as illustrated by the earlier example is not decisive. The point is rather to acknowledge that more enforcement errors occur in the digital world and especially on digital networks, and as a point of departure to suggest that the existing large margin of discretion in the calculation of pecuniary sanctions are used to compensate for enforcement errors.

61 Richard Craswell, 'Deterrence and Damages: The Multiplier Principle and Its Alternatives' (1999) 97 Mich L Rev 2185.

3.2 The Shift Towards Globalisation

Digitalisation, and in particular digital networks, know no geographical borders, which creates complications. Obviously, globalisation is not created by digitalisation, but digitalisation has reinforced the global dimension. In a methodology of digitalisation, globalisation implies a stronger focus on global norms in national legislation as well as in the application of national law.

Two interrelated tendencies are relevant for the shift towards globalisation. The first tendency is regional or global harmonisation of substantive law and the ongoing effort to establish international legal norms that provide minimum protection. This first tendency is most clearly demonstrated by the development in the field of intellectual property law where the adoption of international treaties on minimum protection goes back more than 100 years before the emergence of digitalisation (see earlier). The reason for adopting these old treaties was precisely the rise of cross-border exploitation which created a need for protection in foreign markets. Today, the exchange across borders of goods and services protected by intellectual property has accelerated substantially.

At the legislative level, a legal methodology of digitalisation substantiates international rules. However, the scope for the adoption of international rules has inherent limitations due to the political complications and different needs among the countries involved. Truly global conventions such as the TRIPS Agreement is a one-size-fits-all legal instrument and is suited for the economic needs of the Global North developed countries rather than Global South developing countries.[62] As a consequence, at a certain level of protection further global norms are difficult to achieve and economic inequality between different geographical regions suggests that regional norms are more likely to succeed.

The second tendency is cross-fertilisation, which is relevant when global norms are unattainable. Cross-fertilisation comes in two types: voluntary and guided. Guided cross-fertilisation refers to situations where national laws include elements that create incentives for other states to adopt similar laws. An essential vehicle in guided cross-fertilisation is reciprocity clauses.[63] The United States enacted the Semiconductor Chip Protection Act in 1984 (SCPA 1984) and made protection in the USA of semiconductor chips made by non-American producers conditional on the passage of similar legislation in the country of the producer. As a result of the SCPA 1984, the Directive on the legal protection of topographies

62 For example, Jerome H Reichman and Rochelle Cooper Dreyfuss, 'Harmonization without Consensus: Critical Reflections on Drafting a Substantive Patent Law Treaty' (2007) 57 Duke LJ 85, 91ff, and Peter K Yu, 'Currents and Crosscurrents in the International Intellectual Property Regime' (2004) 38(1) Loy La L Rev 323, 381ff.

63 See Suzanne Scotchmer, 'The Political Economy of Intellectual Property Treaties' (2004) 20(2) J L Econ Org 415, 419; and Graeme B Dinwoodie, 'A New Copyright Order: Why National Courts Should Create Global Norms' (2000) 149 U Pa L Rev 469, 500ff.

of semiconductor products was passed in late 1986 in the European Union.[64] As pointed out previously, when the EU tried the same strategy of guided cross-fertilisation in respect of *sui generis* protection of databases, it failed.[65] In addition to copyright protection of databases, the EU Database Directive of 1996[66] provides for *sui generis* protection of databases. Pursuant to the Directive *sui generis* protection is available to database producers who are nationals of an EU Member State or who have their habitual residence or principal place of business within the territory of the EU. However, the EU Council may by agreement extend the *sui generis* right to databases produced in third countries.[67] According to the preamble of the Directive, the *sui generis* right should only apply to databases from third countries "if such third countries offer comparable protection to databases produced by nationals of a Member State or persons who have their habitual residence in the territory of the Community".[68] The reciprocity clause was primarily aimed at US database producers and a number of bills on *sui generis* protection of databases were presented in the US Congress but none of them were ever passed.[69]

Voluntary cross-fertilisation refers to situations where states adopt a regulatory framework by inspiration from another jurisdiction. Voluntary cross-fertilisation can be construed in Alan Watson's methodological framework on "legal transplants" which claims that legal changes in most cases are caused by imitation of foreign legal measures.[70] Alan Watson describes a "legal transplant" as "the moving of a rule or a system of law from one country to another"[71] and he traces the phenomenon back to Roman law, which has had a substantial impact on different European jurisdictions. It is not clear which underlying factors drive the emergence of legal transplants. Watson suggests that "accessibility" is an essential factor. Thus, legal measures that are easy to find and understand and are related to jurisdictions with high prestige are most likely to be transplanted into other jurisdictions.[72]

64 Council directive 87/54/EEC of 16 December 1986 on the legal protection of topographies of semiconductor products [1987] OJ L24/36.

65 Dinwoodie (n 63) 500.

66 Database Directive (n 4).

67 Ibid art 11.

68 Ibid recital 56.

69 See Mark J Davison, *The Legal Protection of Databases* (2003) 190–216; a similar reciprocity clause was found in Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281/31, art 25(1) which has been described as "a unique form of legal globalization, in which one jurisdiction induces other countries to adopt similar legal mechanisms, without coercion", cf Michael D Birnhack, 'The EU Data Protection Directive: An Engine of a Global Regime' (2008) 24 Comp L & Sec Rev 508.

70 See Ugo Mattei, *Comparative Law and Economics* (1997) 123ff.

71 Alan Watson, *Legal Transplants: An Approach to Comparative Law* (2nd ed, 1993) Univ of Georgia Pr, 21.

72 Ibid para 112ff.

Digitality creates legal problems that do not exist in the analog world. For example, in personal data law, the right to be forgotten would not have been a legal issue in the absence of comprehensive digital networks. Similarly, in copyright law, exhaustion of rights in digital copies and hyperlinks to copyright protected works only exist as legal conflicts in the digital world. It is common to these legal issues and many more creatures of digitality that they appear at approximately the same time when activities are migrating to digital networks. To a large extent they are not addressed in statutory law, and all jurisdictions eventually need legal rules to address such issues. In that situation, looking to foreign jurisdiction for a legal solution is a practical and probably also a rational approach.

One example of voluntary cross-fertilisation in the digital world is the safe harbour provision of the US Digital Copyright Millennium Act (DMCA) from 1998.[73] The safe harbour provision exempts internet service providers and other intermediaries from direct and indirect liability, and the same measures were adopted by the EU in Arts. 12–15 of the e-Commerce Directive.[74] Peter K. Yu characterises the pertinent provisions of the DMCA as "[t]he predominant template for . . . notice-and-takedown procedure".[75]

In adjudication (the dogmatic level) the shift towards globalisation suggests more receptiveness to case law from foreign jurisdictions and a willingness by national courts to rely on foreign case law within the limits established by national statutory law.[76]

Beyond those limits, understanding of foreign laws and comparative law are also essential, because the borderless environment of cyberspace triggers a number

73 17 USC s 512.

74 Directive 2000/31/EC of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market [2000] OJ L 178/1; for example, Rosa Julià-Barceló and Kamiel J Koelman, 'Intermediary Liability: Intermediary Liability in the E-commerce Directive: So far So Good, But it's Not Enough' (2000) 16 Comp L Sec Rev 231, 235.

75 Peter K Yu, 'Digital Copyright Reform and Legal Transplants in Hong Kong' (2010) 48 U Louisville L Rev 693, 710.

76 See the *Grimme Landmachinefabrik GmbH v Derek Scott* [2009] EWHC 2691 (Pat) [2010] 37 FSR 11 remarking *inter alia* that

> [b]roadly we think the principle in our courts—and indeed that in the courts of other member states—should be to try to follow the reasoning of an important decision in another country. Only if the court of one state is convinced that the reasoning of a court in another member state is erroneous should it depart from a point that has been authoritatively decided there. Increasingly that has become the practice in a number of countries, particularly in the important patent countries of France, Germany, Holland and England and Wales. Nowadays we refer to each other's decisions with a frequency which would have been hardly imaginable even twenty years ago. And we do try to be consistent where possible.

See in the same vein the German Bundesgerichtshof's Judgment BGH IIC 2011, 363 (English language version).

of choice-of-law analyses to find possible legal options.[77] The cross-border nature of conflicts thus enables a broader range of possible legal solutions. On this basis, Graeme Dinwoodie proposes that courts should decide international copyright cases not by choosing an applicable law, but by devising an applicable solution and, hence:

> A court faced with an international copyright dispute would not necessarily apply the copyright law of a single state to the contested issues. Instead, it would consider whether the international dimension implicated policies of other states or the international copyright system, and develop (and apply) a substantive rule of copyright law that best effectuates this range of policies.[78]

Globalisation creates a push towards cross-border enforcement and extraterritorial effect of rules. Extraterritorial effect can solve cross-border conflicts and can be included in legislation such as Art. 5 of the DSM Directive.[79] Pursuant to Art. 5(3), the use of works and other subject-matter for the sole purpose of illustration in digital and cross-border teaching activities shall be deemed to occur solely in the Member State where the educational establishment is established. Such a legal fiction in statutory law that corresponds to a country-of-origin principle, is obviously suited to mitigate the cross-border problems of globalisation.

In adjudication, extraterritorial effect can be achieved to a certain extent by expansive interpretation. In *Glawischnig-Piesczek* the CJEU held *inter alia* that Art. 15(1) of the e-Commerce Directive must be interpreted as meaning that it does not preclude a court of a Member State from ordering a host provider to remove information covered by the injunction or to block access to that information worldwide within the framework of the relevant international law.[80]

3.3 The Shift Towards Horizontally Based Law

Digitality creates new modes of interactions that enable new forms of communications, business models, etc. In this ongoing development, law has to adapt to the increasing and fast-moving complexity of reality. Technology neutrality is a

77 Peter K Yu, 'Currents and Crosscurrents in the International Intellectual Property Regime' (2004) 38 Loy La L Rev 323, 437; and Graeme B Dinwoodie, 'International Intellectual Property Litigation: A Vehicle for Resurgent Comparativist Thought?' (2001) 49 Am J Comp L 429, 440.

78 Graeme B Dinwoodie, 'A New Copyright Order: Why National Courts Should Create Global Norms' (2000) 149 Univ Pa Law Rev 469, 542ff.

79 DSM Directive (n 4).

80 Case C-18/18 *Eva Glawischnig-Piesczekv v Facebook Ireland Ltd* (CJEU, 3 October 2019); However, compare with Case C-507/17 *Google LLC v Commission nationale de l'informatique et des libertés (CNIL)* 24 September 2019. On extraterritorial effect, see also Alexander Peukert, 'Transnational Intellectual Property Governance on the Internet' in this volume, sect 2.1.

core value in ensuring consistency in the legal regulation. Basically, technology neutrality means that legal rules should apply to the same effect independently of technologies and that rules should neither require nor assume a particular technology. Furthermore, the rules should be forward looking.[81] In relation to digitality, neutrality implies that analog and digital phenomena should be regulated alike. Thus, technology neutrality is based on the more general principle that the law should strive to ensure that substantively similar activities are treated in the same way.[82]

As pointed out by Lionel Bentley, technologically neutral laws are sensible for at least two reasons. Firstly, in many cases, the legislature wants to regulate particular modes of behaviour, such as the dissemination of hate speech, and the means of communication is irrelevant. Secondly, a reason for promoting technologically neutral laws is to minimise, as far as possible, the circumstances in which laws become obsolete or ineffective or of dubious application when the technologies of expression or communication change (future proofing).[83] Since technologies develop rapidly, there is thus a tendency that technology-specific legislation always lags behind the technologies themselves.

Technology neutrality should not be misunderstood to mean that rules applicable to analog phenomena without further considerations should be extended to similar digital phenomena because the new technology (digitality) may distort the balancing of interests and values that the original rule ensured in the analog world.[84] An example is the reproduction right in copyright law. Article 2 of the InfoSoc Directive stipulates that Member States shall provide for the exclusive right to authorise or prohibit direct or indirect, temporary or permanent reproduction by any means and in any form, in whole or in part. The reproduction right applies to analog as well as digital copying. The broad scope of the harmonised reproduction right necessitated the mandatory exception to the reproduction right in Art. 5(1) on temporary acts of reproduction, which are transient or incidental and an integral and essential part of a technological process. Such temporary acts of reproduction, which are not relevant in relation to analog copying, take place in, for example, the processor of a computer or in the computer's memory and are not observable to the user but, nevertheless, are preconditions for the user to accessing the work. The exception in Art. 5(1), which de facto is only applicable to digital copying, should ensure the same balancing of interests between the copyright holder and the user of the protected work no matter whether the reproduction is digital or analog. Arguably, the EU legislator did not succeed in doing so since the result appears to be that the copyright holder is

81 Chris Reed, 'Taking Sides on Technology Neutrality' (2007) 4 SCRIPTed 263, 264.

82 Arthur Cockfield, 'Towards a Law and Technology Theory' (2003) 30 Manitoba LJ 283, 410.

83 Lionel Bently, 'Copyright and the Victorian Internet: Telegraphic Property Laws in Colonial Australia' (2004) 38 Loy La L Rev 71, 175–76; see also Reed (n 81) 275–78.

84 Reed (n 81) 266–67.

awarded a higher level of protection in respect of digital reproduction compared to analog reproduction.

This example illustrates that technologically neutral rules addressing the same issue may differ in their wording and content, in order to achieve the same effects when applied to these technologies.[85] As a consequence, assessing technology neutrality requires a broader perspective that includes the objective of the rules and that considers how the law can best protect interests and values when they are threatened or otherwise affected by technological developments.[86]

As an element in a legal methodology of digitalisation, the issue of technology neutrality should rather be construed as a shift towards legal decision-making based on a balancing of the underlying values and interests. Such an understanding conforms to what Carus Craig labels the expansive approach to technology neutrality or "prescriptive parallelism" according to which we should seek to apply the law to new technologies in a purposive manner that consistently advances the normative goals of the law.[87]

This approach provides for a flexible analysis. However, the flip side of flexibility is reduced predictability or legal uncertainty. How to balance flexibility and legal uncertainty must be assessed in the concrete cases and will not be further examined in this contribution. However, the approach and the factors in the assessment of this balance parallel the scholarly discussion on rules versus standards.[88]

In a simple general way, the normative goal of intellectual property law can be described as establishing the right balance between, on one hand, the interests of creators in appropriating the value of their creations for the purpose of providing incentives for further creations and, on the other hand, the interest of others to have access to the useful creations. In the same way, the rationale behind data protection law is to establish the right balance between protecting the personal integrity of individual persons and the interests of others to have access to the personal data.

The example earlier with the framing of the reproduction right and the exception for temporary acts of reproduction in the InfoSoc Directive illustrates how the EU legislator attempted to recalibrate the balancing of copyright holders' and copyright users' interests.

The concept of technology neutrality is typically associated with legislation but it expands to adjudication where it entails pronounced purposive or teleological interpretation of statutory rules.

For illustration, in Joined Cases C-509/09 and C-161/10 (*eDate Advertising*) the CJEU adopted such a purposive and expansive interpretation of Art. 7(2)

85 Reed (n 81) 267.

86 Cockfield (n 82) 398–99.

87 Carus J Craig, 'Technological Neutrality: Recalibrating Copyright in the Information Age' (2016) 17 Theor Inq L 601, 606 and 612–15.

88 For example, Louis Kaplow, 'Rules Versus Standards: An Economic Analysis' (1992) 42 Duke LJ 557.

of the Brussels I Regulation[89] on special jurisdiction in cross-border tort cases, substantiated by the fact that the dispute concerned online violations of personality rights. Pursuant to Art. 7(2) of the Regulation, a person domiciled in a Member State may be sued in another Member State in matters relating to tort in the courts for the place where the harmful event occurred or may occur. It is established in the case law of the Court in respect of offline violations of personality rights that the expression "place where the harmful event occurred" is intended to cover both the place where the damage occurred (place of effect) and the place of the event giving rise to it (place of action). In the case of defamation by means of a newspaper article distributed in several States, the rule means that the victim may bring an action for damages against the publisher before the courts of the State of the place where the publisher of the defamatory publication is established (place of action), which have jurisdiction to award damages for all of the harm caused by the defamation. Alternatively, the victim may bring an action for damages against the publisher before the courts of each State in which the publication was distributed and where the victim claims to have suffered injury to his/her reputation (place of effect), which have jurisdiction to rule solely in respect of the harm caused in the State of the court seized.[90] Referring to this criterion of Art. 7(2), in *eDate Advertising* the Court states:

> It thus appears that the internet reduces the usefulness of the criterion relating to distribution, in so far as the scope of the distribution of content placed online is in principle universal. Moreover, it is not always possible, on a technical level, to quantify that distribution with certainty and accuracy in relation to a particular Member State or, therefore, to assess the damage caused exclusively within that Member State.
>
> The difficulties in giving effect, within the context of the internet, to the criterion relating to the occurrence of damage which is derived from *Shevill and Others* contrasts . . . with the serious nature of the harm which may be suffered by the holder of a personality right who establishes that information injurious to that right is available on a world-wide basis.[91]

According to the Court, the previous interpretation of Art. 7(2) of the Brussels I Regulation would thus not enable the victims to enforce their personality rights with sufficient effectivity in respect of internet violations. Hence, the Court finds that the criterion for special jurisdiction in Art. 7(2) must be adapted in such a way that a person who has suffered an infringement of a personality right by

89 Regulation (EU) 1215/2012 of 12 December 2012 on jurisdiction and the recognition and enforcement of judgements in civil and commercial matters [2012] OJ L 351/1. Formerly, this rule on special jurisdiction was found in art 5(3) of the Regulation.

90 Case C-68/93 *Shevill and Others v Presse Alliance SA* [1995] ECR I-415, para 33.

91 Ibid paras 46–47.

means of the internet may bring an action in one forum in respect of all of the damage caused, and that place is where the alleged victim has his or her centre of interests, which usually will be identical to the victim's place of residence.[92] In this way, the Court in online cases of infringement applies a new rule that expands the scope of special jurisdiction pursuant to Art. 7(2) in order to ensure the same balancing of interests that has been established in the offline world, which is an example of prescriptive parallelism in adjudication.

3.4 The Shift From State-Enacted Law to Contract and Code[93]

The methodological shift from state-enacted law to contract and code is pushed forward by the same factors that underlie the shift towards horizontally based law—the challenge of addressing complexities and the need for providing flexibility.

It is reasonable to presume that demands on the law in the digital world are highly heterogeneous due to the multitude of different business models, user communities, transactions and so forth, which continuously come into existence and due to the diverse interests involved in these phenomena.

In order to meet those demands legal actors construct private regulatory models. In cases where it is not optimal for legal actors to rely on state-enacted law they may opt out and establish a private form of legal regulation, primarily by contractual means or by computer code (e.g. measures that restrict access to a website, geoblocking devices, etc.). In this context, "state-enacted law" is a common term for statutory law and case law. Contracting and code are efficiency-based responses to the one-size-fits-all nature of primarily statutory law. When the authoritatively determined regulation does not work for the best interests of the parties, private arrangements emerge to redefine the legal position and change the balance between the opposing interests.

On the face of things, contract and especially code may be said to negate the effects of some of the other methodological shifts.[94] Thus, geoblocking and territorial licensing counteract globalisation. In the same way, it can be argued that contracting for the purpose of redefining the legal position and changing the balance between the opposing interests may counteract horizontally based law thus leading to legal fragmentation.[95] In order to elaborate on the interrelationship between private legal arrangement and state-enacted law, the concept of "autonomy space" will be introduced.

92 Ibid para 48.

93 This section is based on Thomas Riis, 'User Generated Law Re-constructing Intellectual Property Law in a Knowledge Society' in Thomas Riis (ed), *User Generated Law* (2016) Edward Elgar.

94 Thomas Schultz, 'Carving up the Internet: Jurisdiction, Legal Orders, and the Private/Public International Law Interface' (2008) 19 Eur J Int L 799, 805, see also 828ff.

95 Contracting will not always counteract globalisation and leads to fragmentation, which user terms of social media and other global internet platforms illustrate.

State-enacted law defines a space within which legal actors may act autonomously, which will hereinafter be termed the *autonomy space*. In parts of state-enacted law where public policy protection plays a minor role, the autonomy space is wide, and in parts of state-enacted law where public policy protection is dominant the autonomy space is narrow. Outside the autonomy spaces, private parties cannot enter into a valid mutual agreement or other regulatory models stating that another set of legal rules ought to apply to them. In the field of information law, the autonomy spaces are wide. However, the autonomy spaces are confined by mandatory rules and inalienable rights, which are found in intellectual property law, and stricter conditions for recognising a valid agreement, which is a main principle in data protection law.

In many cases, it does not appear expressly from statute whether a specific rule is mandatory or optional. If that is the case, the courts must decide on the issue. For example, the CJEU held in *UsedSoft* (see earlier) that the rule on exhaustion in Art. 4(2) of the Computer Programs Directive[96] is mandatory and thus cannot be contracted out of. Probably the reason for the Court to narrow down the autonomy space in this case is an understanding that it is an important policy objective of the EU legislator that copies of computer programs can circulate freely within the EU once they have been put on the market by the copyright holder.

In a legal methodology of digitalisation, it is the point of departure that parties should be allowed to opt out of state-enacted law, simply because the state/legislator has inadequate information on legal actors' legal situations and needs that emerge within autonomy spaces, and that the legal actors' legal needs are highly heterogeneous. The shift from state-enacted law to contract and code supports a broad variety of private regulatory models and thus legal fragmentation. However, this methodological shift does not interfere with the three other methodological shifts: (1) from substantive law to procedural law; (2) towards globalisation; and (3) towards horizontally based law, because it is the legal framework of state-enacted law that defines the autonomy spaces and not vice versa.

The notion of wide autonomy spaces conforms to the idea of freedom of contract. Like freedom of contract, the widening of autonomy spaces is subject to limitations. The first group of limitations comprises regulatory models that violate moral norms or counteract other important policy objectives. The second ground comprises market failures. The traditional market failures are the creation of harmful effects on third parties (externalities), transaction costs, asymmetric information that enables the party with the most information to appropriate unfair advantages, and unequal distribution of bargaining power. An example of the latter could be the terms of use of large social media. The individual user of social media has in reality no bargaining power and the social media can dictate the terms. In such a situation, there may be reason for adjusting the autonomy space.

96 Software Directive (n 4).

In the context of legislation the methodological shift from state-enacted law to contract and code and the recognition of autonomy spaces imply that the legislator should aim at establishing wide autonomy spaces and only restrict them when important policy objectives or market failures are present. Also, the shift suggests that both national and international norms should not be understood in an overly rigid way but as leaving room for "experiments" either by users or legislators.[97]

The same applies in adjudication, where courts can contribute to the widening and clarification of autonomy spaces by preserving private regulatory models unless policy objectives or market failures suggest otherwise. For the same purpose, courts ought to be reluctant to hold that a specific rule is mandatory unless it is expressly stated so in statute.

4 Final Remarks

Copyright law provides a useful template for identifying, analysing and discussing general methodological challenges to law arising out of digitalisation. In particular, the following four shifts seem to be of a general and central importance:

- The shift from substantive law to procedural law,
- The shift towards globalisation,
- The shift towards horizontally based law, and
- The shift from state-enacted law to contract and code.

Both individually and when taken together these shifts represent challenges to the traditional assumptions and types of legislation, adjudication and application of law.

Normally, it is easier to indicate "what not to do" rather than "what to do". We find in particular that the legislative approach chosen by the EU in the field of copyright where rules have been piled on top of rules for 30 years is problematic in the light of the colossal technological changes which have taken place during the same period. More concretely, we also find that the InfoSoc Directive provides a less than optimal system for the complicated balancing of interests which is needed to future-proof copyright law. In particular, the combination of a starting point of a high level of protection for right holders with a narrow and closed list of limitations and exceptions provides for a one-way-only flexibility which does not leave enough breathing space for the law to develop balanced solutions.

We think, however, that the CJEU has so far also paid too little attention to the need to have flexible mechanisms and that its decisions need to keep a better eye on overarching principles. Fundamental rights norms are crucial in this regard and we are concerned that the Court may have limited their application too

97 Annette Kur and Jens Schovsbo, 'Expropriation or Fair Game for All? The Gradual Dismantling of the IP Exclusivity Paradigm' in Annette Kur and Marianne Levin (eds), *Intellectual Property Rights in a Fair World Trade System* (2011) Edward Elgar Publishing, 444.

much. Flexibility requires strong normative bench marks. The more open-ended the norms and the more room for manoeuver which is left to arbitrators, the stronger the need for external norms. Such a methodological approach reflects what we have termed "horizontally based law".

In addition to this methodological starting point, digitalisation reinforces a stronger focus on and a more active and expansive application of procedural law, including the available sanctions and remedies, due to a multitude of enforcement errors in the digital world. Furthermore, increasing globalisation arising from digitalisation is pushing legislators and courts to base their future law- and decision-making on a higher degree of receptiveness in constructing and applying foreign norms and decisions in national law. Finally, the emergence and dissemination of private regulatory models should be allowed to flourish provided that such models are not the result of market failures or do not contravene public policy objectives. If so, the public lawmakers (the legislator and courts) should adjust the autonomy spaces to ensure that the harmful effects of market failures are eliminated and public policy objectives are attained.

2 Transnational Intellectual Property Governance on the Internet

Alexander Peukert

1 Introduction

Intellectual property (IP) is a classical cyberlaw topic and a prime example of the conflict between global online communication and local laws.[1] Whereas literary and artistic works, brands and other IP subject matter can, in principle, be made available to a global audience at virtually no cost via the Internet,[2] IP rights (IPRs) are strictly territorial in nature. International IP treaties make it possible to acquire 190+ local IPRs in, for example, a motion picture or a well-known trademark, yet each local IPR is independent of all others and limited in its geographical scope to the territory of the IP jurisdiction granting it.[3] This fragmentation also bears on the rules of international jurisdiction and private international law.[4] IPRs requiring registration, such as patents, can be adjudicated in full only in the country of registration. Multistate copyright infringements may be decided by the courts in the defendant's domicile, but even these courts are bound to apply all

1 Cf Frank H Easterbrook, 'Cyberspace and the Law of the Horse' (1996) U Chi Legal F 207, 208 ("When asked to talk about 'Property in Cyberspace,' my immediate reaction was, 'Isn't this just the law of the horse?'"); Jane C Ginsburg, 'Global Use/Territorial Rights: Private International Law Questions of the Global Information Infrastructure' (1995) 42 J Copyright Soc'y USA 318. To be sure, the conflict between global commerce and local IPRs is also acute in offline settings; cf *Unwired Planet v Huawei* [2020] UKSC 37, 49–104 (allowing English courts to set global "FRAND" licensing conditions based on an alleged infringement of a standard-essential UK patent).

2 *Google Inc v Equustek Solutions Inc* [2017] SCC 34, [2017] 1 SCR 824 ("The Internet has no borders—its natural habitat is global"). But see Dan Jerker B Svantesson, *Private International Law and the Internet* (2016) 57–58 (relative borderlessness of the Internet).

3 Alexander Peukert, 'Territoriality and Extraterritoriality in Intellectual Property Law' in Günther Handl, Joachim Zekoll and Peer Zumbansen (eds), *Beyond Territoriality: Transnational Legal Authority in an Age of Globalization* (2012) Martin Nijhoff Publishers, 189–91.

4 See Alexander Peukert in European Max Planck Group on Conflict of Laws in Intellectual Property (CLIP), *Conflict of Laws in Intellectual Property, The CLIP Principles and Commentary* (2013) paras PRE:C33–39.

DOI: 10.4324/9781003283881-4

IP laws of the states for which protection is sought.[5] Since pleading and applying 190+ copyright laws is unfeasible for both parties and courts, it has been proposed in the literature to reduce the number of laws applicable to ubiquitous online copyright infringements to one, namely the law of the closest connection with the (direct) infringement, and, regarding the indirect liability of Internet service providers (ISPs), the law of the State of their center of business activity.[6] These proposals to overcome IP territoriality online have, however, not yet been taken up by any court or legislator.

It follows that a genuinely transnational governance of online IP activity necessitates "other rules" beyond formal IP laws, and the involvement of non-state actors.[7] IP rules become transnational when they are implemented across borders. At a minimum, they affect two IP jurisdictions, at the most the entire Internet and thus global communication. The purpose of this Chapter is to document and classify instances of such transnational IP "laws" of Western European and North American origin, with a particular focus on the territorial reach of the respective regimes.[8] It is structured according to the two basic options an IPR holder has available: She can either prohibit or authorize the use of her IP.[9] The following Section 2 reviews transnational IPR enforcement measures, and Section 3 briefly addresses global and local licensing practices. Based on this overview, the concluding section identifies three layers of IP governance on the Internet.

2 IPR Enforcement

Transnational IPR enforcement on the Internet occurs in two forms. One concerns formal court decisions (Section 2.1), the other self-regulatory measures implemented by intermediaries (Section 2.2).

5 See, e.g. *Boosey & Hawkes Music Publishers, Ltd v Walt Disney Co* [1998] 145 F3d 481, 491–92 (US court competent to adjudicate claim for damages for copyright infringement in at least 18 foreign countries under these foreign laws).

6 Annette Kur in European Max Planck Group on Conflict of Laws in Intellectual Property (CLIP), *Conflict of Laws in Intellectual Property, The CLIP Principles and Commentary* (2013) paras 3:603.C01–3:604.C22.

7 Cf Philip Jessup, *Transnational Law* (1956) Yale University Press, 2; Thomas Schultz, 'Private Legal Systems: What Cyberspace Might Teach Legal Theorists' (2007) 10 Yale J L & Tech 151.

8 To my knowledge, the only publication that explicitly addresses this issue, albeit not in systematic form, is Thomas Hoeren and Guido Westkamp, *Study on Voluntary Collaboration Practices in Addressing Online Infringements of Trade Mark Rights, Design Rights, Copyright and Rights Related to Copyright* (2016) 36. See also Kristofer Erickson and Martin Kretschmer, 'Empirical Approaches to Intermediary Liability' in Giancarlo Frosio (ed), *Oxford Handbook of Online Intermediary Liability* (2020) Oxford University Press, 105.

9 Cf TRIPS art 11.

2.1 Takedown Orders of Courts: De Iure and de Facto Effects

According to the territoriality principle, court ordered injunctions and other remedies only concern activities in the territory of the IP law(s) pleaded and applied.[10] In practice, however, a court order to cease and desist making a certain content available on the Internet has, even if only one national IPR/law was considered, automatic extraterritorial effects because Internet users in other countries also lose the possibility to access the respective source, irrespective of whether or not the content infringed IPRs under the laws of these third countries.[11]

If the defendant can show that the upload in question is legal under certain IP laws, the proper reaction of a court in line with the territoriality principle is to explicitly limit the injunction to the countries whose IP laws were pleaded and violated against, and to order the defendant to geo-block access to the content at stake from these infringement territories only.[12] For example, a German court ordered a U.S. operator of a website which provides access to works in the public domain under U.S. law to prevent German users from accessing the writings of Thomas Mann and others whose works are still protected by copyright under German law within Germany.[13] The conflict between independently owned, equally legitimate trademark rights in identical or similar signs (e.g. *Merck Germany v. Merck U.S.*) is also resolved by obliging both parties to implement geo-targeting and geo-blocking measures so as to avoid consumer confusion in the markets in which each trademark owner enjoys exclusivity.[14] A counterexample proving the territoriality rule is the infamous Canadian-U.S. jurisdictional conflict in *Google v. Equustek*. In this case, the Canadian Supreme Court explicitly ordered Google, on the basis and in furtherance of Canadian trade secrets law, to de-index certain websites not only from Google.ca but from any of its search results worldwide.[15] In a countermove, Google obtained a decision from a U.S. District Court declaring the Canadian global order to be unenforceable in the

10 Graeme Dinwoodie in European Max Planck Group on Conflict of Laws in Intellectual Property (CLIP), *Conflict of Laws in Intellectual Property, The CLIP Principles and Commentary* (2013) paras 2:604.C01-N04.

11 Marketa Trimble, 'The Territorial Discrepancy Between Intellectual Property Rights Infringement Claims and Remedies' (2019) 23 Lewis & Clark L Rev 501, 503–04.

12 Geo-blocking has generally been accepted to accommodate global online communication with local laws. See *Yahoo! Inc v La Ligue Contre Le Racisme Et L'Antisemitisme* [2006] 433 F3d 1199, 1216–17 (public law); Opinion of Advocate General Szpunar, Case C-18/18 *Eva Glawischnig-Piesczek* (CJEU, 3 October 2019) paras 100–01 (defamation); Case C-507/17 *Google LLC v Commission nationale de l'informatique et des libertés (CNIL)* (CJEU, 24 September 2019) para 70 (data protection).

13 Higher Regional Court Frankfurt am Main, 30.04.2019–11 U 27/18—BeckRS 2019, 11210—*Project Gutenberg*.

14 See Case C-231/16 *Merck v Merck* (CJEU, 19 October 2017); Alexander Peukert, 'The Coexistence of Trade Mark Laws and Rights on the Internet, and the Impact of Geolocation Technologies' (2016) 47(1) Int Rev Intellect Prop Comp L 60–87.

15 *Google Inc v Equustek Solutions Inc* (n 2) ("Google's argument that a global injunction violates international comity . . . is theoretical").

U.S. in view of the immunity of search engine operators under U.S. law.[16] At the same time, Google reterritorialized its search engine. Instead of allowing Internet users to circumvent the removal of search results by simply switching to another Google top level domain (TLD)—a possibility that concerned the Canadian Supreme Court and triggered its global response—Google now employs geolocation technologies that make certain that users see a version of the search results that is in accordance with the laws of the place from where the search is presumably conducted.[17] The Canadian global court order thus ultimately reinforced territorial fragmentation.

In most cases, however, the territorial overreach of takedown orders goes unnoticed. One reason for this is the quite advanced level of international harmonization in the area of IP. Cases where local IP laws diverge in meaningful ways are relatively rare. That, for example, current movies must not be made available on the Internet without prior authorization of the right holder is, by and large, a universally valid legal statement. In such clear cases, the practice of unrestricted takedown orders with de facto worldwide effects also appears legitimate. In hard cases of conflicts of IP laws or rights, however, cyberspace is split up via geoblocking along the real-world borders between IP jurisdictions.

2.2 Intermediaries' Enforcement Measures

The second, and practically much more important mode of transnational IPR enforcement on the Internet, concerns private self-regulation by intermediaries.

2.2.1 The Central Role of Intermediaries

Intermediaries providing services for online communication have for a long time occupied a central role in Internet governance in general and online IPR enforcement in particular. Firstly, "[n]othing happens online that does not involve one or more intermediaries" such as domain name registrars, access and host providers, search engines, advertising, and payment services.[18] Secondly, and in contrast to anonymous pirates of cyberspace, intermediaries are worthwile targets of enforcement

16 *Google v Equustek Solutions* [2017] WL 500834 (ND Cal). But see *Equustek Solutions Inc v Jack* [2018] British Columbia Supreme Court, [2018] 10 WWR 715 (Can) (dismissing an application to set aside or vary the global injunction). See also Robert Diab, 'Search Engines and Global Takedown Orders: Google v Equustek and the Future of Free Speech Online' (2019) <https://ssrn.com/abstract=3393171> accessed 15 September 2020; Michael Geist, 'The Equustek Effect: A Canadian Perspective on Global Takedown Orders in the Age of the Internet' in Giancarlo Frosio (ed), *Oxford Handbook of Online Intermediary Liability* (2020) Oxford University Press, 709.

17 *Equustek Solutions Inc v Jack* (n 16); *Google LLC v CNIL* (n 12) para 42.

18 Jacqueline D Lipton, 'Law of the Intermediated Information Exchange' (2012) 64 Fla L Rev 1337; Derek E Bambauer, 'Middlemen' (2012) 64 Fla L Rev F 64; Graeme Dinwoodie, 'Who Are Internet Intermediaries?' in Giancarlo Frosio (ed), *Oxford Handbook of Online Intermediary Liability* (2020) Oxford University Press, 37.

efforts who conduct a lawful business as part of the formal economy.[19] Thirdly, they offer a solution for the problem of the scale of copyright and other IPR infringements online, which are so numerous that they could never be adjudicated in state court proceedings.[20] Through the code with which intermediaries operate their services, they are able to enforce IPRs in many cases—in the case of Google search, billions—at relatively little cost. The answer to the problem of IPR infringements via digital network technologies is indeed "in the machine", and these machines are controlled by private intermediaries.[21]

Until very recently, however, online intermediaries have not been considered direct infringers.[22] It is not the intermediaries that make copyrighted works available to the public, sell counterfeit products and otherwise infringe IPRs, but their customers/users. Intermediaries are therefore liable for third-party infringements if at all only indirectly under additional requirements and to a limited extent. Standards vary according to the intermediary concerned and across IP jurisdictions,[23] but the basic dilemma and also the regulatory approach to intermediary liability is the same across the board. On the one hand, intermediaries' services are used in the course of IPR infringements, they are aware of illegal activity at least upon being notified accordingly, and they are in a position to do something about it. Thus, right holders and governments constantly pressure intermediaries to curb at least clear cases of piracy and counterfeiting. On the other hand, intermediaries provide per se neutral services that are widely used for perfectly legal and socially beneficial purposes. Consequently, intermediaries have been shielded from levels of liability that would amount to a general obligation to monitor their services or otherwise render their legitimate business model impossible.[24]

19 On the difficulties to pursue individual IPR infringers see Yochai Benkler, *The Wealth of Networks* (2006) 396; Anupam Chander, *The Electronic Silk Road* (2013) 87–112 ("pirates of cyberspace").

20 On the scale of cases as a characteristic feature of cyberlaw see David G Post, *In Search of Jefferson's Moose* (2009) 60–89.

21 Charles Clark, 'The Answer to the Machine is in the Machine' in Bernt Hugenholtz (ed), *The Future of Copyright in a Digital Environment* (1999) Kluwer Law International, 139; Maayan Perel and Niva Elkin-Koren, 'Accountability in Algorithmic Copyright Enforcement' (2016) 19 Stan Tech L Rev 473; Clement Salung Petersen and Thomas Riis, 'Private Enforcement of IP Law by Internet Service Providers: Notice and Action Procedures' in Thomas Riis (ed), *User Generated Law* (2016) Edward Elgar Publishing, 228, 239–40; Joanne Gray, *Google Rules* (2020) Oxford University Press, 118.

22 Council Directive 2019/790/EU of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC [2019] OJ L130/92 (DSM Directive) art 17 (online content-sharing service providers perform an act of communication/making available to the public when they give the public access to copyright-protected content uploaded by their users).

23 Matthias Leistner, 'Intermediary Liability in a Global World' (March 2, 2019) in Tatiana Eleni Synodinou (ed), *Pluralism or Universalism in International Copyright Law* (Forthcoming) <https://ssrn.com/abstract=3345570> accessed 16 September 2020.

24 Cf Lilian Edwards, *WIPO Report: Role and Responsibility of Internet Intermediaries in the Field of Copyright and Related Rights* (2005) WIPO, 7–8 <www.wipo.int/export/sites/www/copyright/en/doc/role_and_responsibility_of_the_internet_intermediaries_final.pdf> accessed 16 September 2020; Giancarlo Frosio (ed), *Oxford Handbook of Online Intermediary Liability* (2020) Oxford University Press.

For example, host providers and search engines have to expeditiously remove or disable access to IP-infringing content after a respective notification (notice and takedown, NTD). At the same time, they are neither liable vis-à-vis IPR holders until being notified of an infringement nor vis-à-vis their customers/users for good faith false positive takedowns.[25]

This framework opens up an "autonomy space", within which intermediaries are able to develop tailor-made IP policies for their services.[26] Such in-house solutions will generally be preferred to potentially disruptive, exogenous rules imposed by courts or legislators.[27] In developing their IP policies, intermediaries are not primarily guided by public policy goals but, as private corporations, by the aim to maximize profits. In the IP liability context, this means to navigate cost-efficiently between the Scylla of IP liability and the Charybdis of customers who are unsatisfied with an overly restrictive service. Regarding the territorial scope of IP policies, economies of scale militate in favor of service-wide, transnational standards instead of country-specific measures, implemented via costly geolocation technologies.[28] All these aspects support the emergence of private, transnational IP policies.

Yet, as the following examples demonstrate, the state has not left the stage.[29] Already by defining the standard of statutory IP liability, legislators and courts influence the content and territorial scope of intermediaries' IP policies. In

25 See 17 USC § 512(c), (g); Council Directive 2000/31 of 8 June 2000 on electronic commerce [2000] OJ L 178/1 (E-Commerce Directive) arts 14, 15 and Case C-324/09 *L'Oréal SA and Others* [2011] ECR I-6011, paras 106–44; arts 18.81–82 Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP).

26 Petersen and Riis (n 21) 228ff; Michael Andreas Kümmel, *Die Implementierung der Haftung von Host-Providern für Immaterialgüterrechtsverletzung* (2017) Dr. Kovac (documenting notice and takedown regimes of eBay, Amazon, Facebook and YouTube).

27 Matthew Sag, 'Internet Safe Harbors and the Transformation of Copyright Law' (2017) 93 Notre Dame L Rev 499, 542.

28 Joel R Reidenberg, 'Lex Informatica: The Formulation of Information Policy Rules Through Technology' (1998) 76 Tex L Rev 553, 577–79 ("Technologically implemented rules apply throughout the relevant network. As such, Lex Informatica reaches across borders and does not face the same jurisdictional, choice of law problem that legal regimes encounter when networks cross territorial or state jurisdictional lines."); P Bernt Hugenholtz, 'Codes of Conduct and Copyright Enforcement in Cyberspace' in Irini A Stamatoudi (ed), *Copyright Enforcement and the Internet* (2010) Wolters Kluwer, 303–04.

29 European Commission, 'Report on the Functioning of the Memorandum of Understanding on Online Advertising and Intellectual Property Rights' SWD(2020) 167 final/2, 4 (European Commission facilitates cooperation between IPR holders and online marketplaces); Michael D Birnhack and Niva Elkin-Koren, 'The Invisible Handshake: The Reemergence of the State in the Digital Environment' (2003) 8 Va JL & Tech 1–2; Uta Kohl, *Jurisdiction and the Internet* (2007) 265–70; Yochai Benkler, 'A Free Irresponsible Press: Wikileaks and the Battle over the Soul of the Networked Fourth Estate' (2011) 46 Harv CR-CL Rev 311 ("regulation by raised eyebrow"); Hannah Bloch-Wehba, 'Global Platform Governance: Private Power in the Shadow of the State' (2019) 72 SMU L Rev 27.

addition, the European Commission and other governments have for a long time beset intermediaries to accept ever more concrete IP codes of conduct.[30]

2.2.2 Intermediaries' Enforcement Measures and Their Transnational Effect

Intermediaries' enforcement measures and their transnational effect vary according to the type of service concerned and the geographical scope of application of self-regulatory rules.

2.2.2.1 DOMAIN NAME REGISTRARS

In the case of domain name registrars, the combined efforts of trademark owners and governments led to a very early and well-known global regime, namely the "Uniform Domain Name Dispute Resolution Policy" (UDRP), adopted by the Internet Corporation for Assigned Names and Numbers (ICANN) in 1999, which is still in force today in its original version.[31] The emergence of the UDRP is tightly bound to U.S. law and policy.[32] After it had become settled case law that registering a trademark as a domain name in order to sell it to the corresponding trademark holder constitutes trademark infringement,[33] the U.S. legislature in 1999 extended trademark protection to address the problem of non-U.S. "cybersquatters". The Anticybersquatting Consumer Protection Act (ACPA) allows for *in rem* civil actions against domain name registrars based in the U.S. for the

30 Cf E-Commerce Directive (n 25) art 16 (codes of conduct); DSM Directive (n 22) art 17(10) (best practices for cooperation between online content-sharing service providers and right holders); CPTPP (n 25) art 18.82(1)(a) (contracting parties shall incentivize cooperation between ISPs and copyright owners); Hugenholtz (n 28) 306; Natasha Tusikov, *Chokepoints: Global Private Regulation on the Internet* (2017); Martin Husovec, *Injunctions against intermediaries* (2017) University of California Press, 229ff; Salung Petersen and Riis (n 21) 230; Giancarlo Frosio, 'Algorithmic Enforcement Online' in Paul Torremans (ed), *Intellectual Property and Human Rights* (2020) Wolters Kluwer, 709.

31 See ICANN, Uniform Domain-Name Dispute-Resolution Policy (UDPR) <www.icann.org/resources/pages/help/dndr/udrp-en> accessed 16 September 2020 and, e.g. Laurence R Helfer and Graeme B Dinwoodie, 'Designing Non-National Systems: The Case of the Uniform Domain Name Dispute Resolution Policy' (2001) 43 Wm & Mary L Rev 141; Jens Schovsbo, 'The Private Legal Governance of Domain Names' in Thomas Riis (ed), *User Generated Law* (2016) Edward Elgar, 206. On the cheaper and faster "Uniform Rapid Suspension System" in the context of new gTLDs such as .bike, see ICANN, Uniform Rapid Suspension (URS) <www.icann.org/resources/pages/urs-2014-01-09-en> accessed 16 September 2020; James L Bikoff and others, 'The Uniform Rapid Suspension System: A New Weapon in the War against Cybersquatters' (2014) 6(3) Landslide 32.

32 Marketa Trimble, 'Territorialization of the Internet Domain Name System' (2018) 45 Pepp L Rev 623, 661–62.

33 *Panavision Int'l v Toeppen* [1998] 141 F3d 1316 (holding that pattern of offering domain names for sale to mark holders was "use in commerce" of the mark sufficient to violate Lanham Act).

forfeiture or cancellation of a domain name or the transfer of a domain name from a foreign domain name holder to the owner of the respective mark. Notably, the statute grants immunity to domain name registrars unless they act in bad faith or recklessly disregard their duties under the statute.[34]

Simultaneously, the privatization of the Internet was in full swing. In 1998, the U.S. Department of Commerce announced that the global Domain Name System was to be centrally controlled and coordinated by ICANN, a nonprofit California corporation, but that there should be competition between domain name registrars accredited by ICANN.[35] That, in turn, created the risk that non-U.S. cybersquatters could register trademark-protected signs with non-U.S. registrars beyond the reach of U.S. trademark law and the ACPA. In addition, the global Domain Name System highlighted the problem of conflicting trademark rights on the Internet. If the very same sign or confusingly similar signs can be trademark-protected in country A for company A, and in country B for company B, who is entitled to use the sign on the Internet?[36]

To address the looming enforcement and coordination problems, the U.S. government called upon the World Intellectual Property Organization (WIPO) to consult both trademark holders and members of the Internet community with the aim to develop recommendations for "a uniform approach to resolving trademark/domain name disputes involving cyberpiracy (as opposed to conflicts between trademark holders with legitimate competing rights)".[37] In accordance with this suggestion, the focus of the UDRP is on bad faith "cybersquatters". In a nutshell, the UDRP requires registrants and domain name applicants to submit to mandatory administrative proceedings in the event that a trademark holder asserts that (1) a registered domain name is identical or confusingly similar to a trademark, (2) the domain name holder has no rights or legitimate interests in respect of the domain name, and (3) the domain name has been registered and is being used in bad faith. If these requirements are met, a UDRP panel can order either the cancellation of the domain name or its transfer to the complainant, which is to be carried out by the registrant concerned after ten business days.[38] Through its inclusion in registration agreements of all ICANN-accredited registrars, the UDRP has become a global legal standard, binding upon all holders of generic and numerous country-code TLDs, irrespective of the domicile of the registrant and the other parties involved. The vast majority of many thousand

34 15 USC § 1125.

35 On the formation of ICANN see A Michael Froomkin, 'Wrong Turn in Cyberspace: Using Icann to Route Around the Apa and the Constitution' (2000) 50 Duke LJ 17, 50–51; US Department of Commerce, 'Management of Internet Names and Addresses' (1998) 63 FED REG 31,741 <www.govinfo.gov/content/pkg/FR-1998-06-10/pdf/98-15392.pdf> accessed 16 September 2020.

36 See *Merck v Merck* (n 14).

37 US Department of Commerce (n 35).

38 UDRP (n 31) paras 3, 4.

UDRP panel decisions has been in favor of trademark owners and has not given rise to an admissible review by state courts.[39]

From the perspective of traditional trademark law and its territorial fragmentation, the long-term success of the UDRP should still come as a surprise. The complainant only needs to show ownership of one single national trademark to be possibly allocated a generic TLD such as .com, which is useful for worldwide commercial activities.[40] Thus, the UDRP equips national trademarks with worldwide effects. This globalization of national trademarks is, however, acceptable because the UDRP only targets a limited set of simplistic cases. Firstly, the UDRP is only concerned with domain names and not with the content accessible via that domain. Secondly, the person having registered the domain in question must not have any rights or legitimate interests in respect of the name. Disputes between holders of equally legitimate national rights in identical/similar domains are beyond the scope of the UDRP and remain subject to the territorially fragmented system of IP law.[41] And thirdly, the registration must have occurred in "bad faith", for example, for the purpose of selling the domain to the complainant or for misleadingly generating website traffic.[42] There apparently is a stable, rough global consensus[43] that such bad faith "cybersquatters" do not deserve forbearance. Any valid national trademark suffices to expel them from the global domain name system.

The fragility and limits of this "consensus" became apparent, however, when U.S. copyright holders tried to get ICANN and its accredited registrars involved in a copyright enforcement scheme, according to which domain names for notified "pirate sites" would have been cancelled. If this plan had materialized, private IPR enforcement via the domain name system would have reached, for the first time, beyond the domain name/trademark level deep into the content layer.[44]

39 Laurence R Helfer, 'Whither the UDRP: Autonomous, Americanized, or Cosmopolitan?' (2004) 12 Cardozo J Int'l & Comp L 493, 494–95 (barely 1% of all UDRP panel rulings have been submitted for review by national courts); Annemarie Bridy, 'Notice and Takedown in the Domain Name System: Icann's Ambivalent Drift into Online Content Regulation' (2017) 74 Wash & Lee L Rev 1345, 1357–58 (in WIPO proceedings, registrants have prevailed in only 12% of cases); 'WIPO Conference—As the UDRP Turns 20: Looking Back, Looking Ahead' <www.wipo.int/portal/en/news/2019/article_0050.html> accessed 16 September 2020 (over 45,000 UDRP cases have been filed with WIPO's Arbitration and Mediation Center).

40 Cf para 1.2.6.1 URS (n 31) (the complaint has to show that the complainant holds "a valid national or regional registration and that is in current use").

41 Peukert (n 14) 60–87.

42 UDRP (n 31) para 4(b).

43 On the concept of "rough consensus and running code" see Post (n 20) 136–37; Gralf-Peter Callies and Peer Zumbansen, *Rough Consensus and Running Code* (2010) Hart Publishing, 135–36.

44 Bridy (n 39) 1345, 1346–49, 1359–62. The seizure/disconnection of domains by public authorities in the context of criminal proceedings remains unaffected; see Jack Mellyn, '"Reach Out and Touch Someone": The Growing Use of Domain Name Seizure as a Vehicle for the Extraterritorial Enforcement of U.S. Law' (2011) 42 Geo J Int'l L 1241, 1242–43; IACC (2017) <www.iacc.org/media/the-international-anticounterfeiting-coalition-and-city-of-london-police-partner-to-protect-consumer> accessed 16 September 2020 (announcing cooperation between the International AntiCounterfeiting Coalition (IACC) and the City of London Police Intellectual Property Crime Unit (PIPCU) to take down websites selling counterfeits through the IACC RogueBlock Program).

After a "trusted notifier" copyright enforcement program between the Motion Picture Association of America and two registry operators for new generic TLDs (one based in the U.S., the other in Abu Dhabi) had been publicly revealed, registrars, however, quickly backpedaled.[45] ICANN's current Registry Agreement with registrars of new generic TLDs requires registrars to prohibit new generic TLD holders from engaging in "piracy, trademark or copyright infringement . . . counterfeiting or otherwise engaging in activity contrary to applicable law", and to provide "(consistent with applicable law and any related procedures) consequences for such activities including suspension of the domain name".[46] There is, however, no out-of-court online dispute resolution system comparable to the UDRP in place to enforce these directives.

2.2.2.2 ACCESS PROVIDERS

To engage domain name registrars in the enforcement of copyright and other content-related laws would indeed be problematic because of the sweeping effects of a domain name cancellation, which de facto disconnects the server hosting the (allegedly) infringing websites from the Internet. By comparison, less effective and less far-reaching blocking orders against access providers, which can also be implemented via the domain name system,[47] are considered by the European Court of Human Rights as an "extreme measure" that "deliberately disregards the distinction between the legal and illegal information the website may contain, and renders inaccessible large amounts of content which has not been identified as illegal".[48]

Because of these concerns and the neutral, "mere conduit" role of access providers regarding the content their services transmit, these ISPs enjoy broad immunities and had for quite a while managed to avoid getting involved in IPR enforcement online.[49] That outsider position came under fire, however, with the advent of massive unauthorized peer-to-peer file sharing in the early 2000s, which copyright holders could not effectively curb by going after anonymous individual infringers.[50] In addition, in the fight against counterfeit goods sold on

45 See Annemarie Bridy, 'Addressing Infringement: Developments in Content Regulation in the US and the DNS' in Giancarlo Frosio (ed), *Oxford Handbook of Online Intermediary Liability* (2020) Oxford University Press, 632, 637–45.

46 Specification 11, section 3(a) Base New gTLD Registry Agreement (31 September 2017) <https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-31jul17-en.html> accessed 22 September 2020.

47 *Cartier International AG v British Sky Broadcasting Ltd* [2014] EWHC 3354 (Ch), [2015] RCP 7, para 25.

48 ECtHR Case 12468/15 *Flavus v Russia* para 37. But see German Federal Court of Justice, case I ZR 13/19, openJur 2020, 78064, paras 33ff.—Störerhaftung des Registrars (domain registrars indirectly liable for copyright infringements under the same conditions as access providers).

49 Cf 17 USC § 512(a); E-Commerce Directive (n 25) art 12.

50 Cf Alexander Peukert, 'Why Do "Good People" Disregard Copyright on the Internet?' in Christophe Geiger (ed), *Criminal Enforcement of Intellectual Property: A Handbook of Contemporary Research* (2012) Eward Elgar, 151.

the Internet, right holders increasingly spotlighted access providers as possible targets.[51]

An initial type of private enforcement schemes involving access providers were so-called "graduated response" procedures, which access providers from several countries adopted "voluntarily" after intense pressure by right holders and governments.[52] The concept of these programs was that copyright owners would report dynamic IP addresses used for illegal file sharing to access providers. The access provider whose subscriber had used the IP address at the relevant time then sent a warning to that user. After three to six warnings ("strikes"), access providers were to sanction their subscribers by throttling bandwidth or even by temporarily cutting off repeat infringers from the Internet.

These measures were not well received by the general public and have largely been abandoned.[53] Instead of going after individual Internet users, a second type of IPR enforcement measure involving access providers gained prominence: website blocking. In 2014, the CJEU held that EU Member States have to ensure that copyright holders can apply for an injunction against access providers to prohibit them from allowing their customers access to a copyright infringing website if such an order does not unnecessarily deprive Internet users of access to lawful information.[54] This ruling supports collaboration between right holders and access providers to make sure that all ISPs block certain websites, and that if the infringing content is moved to another domain, this new page will also be blocked.[55]

If implemented in these ways, website blocking can be an effective IPR enforcement measure.[56] Its geographical reach is, however, rather limited and rarely ever transnational. The reason is that, in contrast to domain cancellations by registrars, website blocking by access providers does not apply to the single source of the infringement but attaches to the recipients who try to access the source. In addition, only the customers of a particular access provider are affected by blocking measures. And since providing access to the Internet requires some control over physical infrastructure, access providers do business and have customers within clearly defined areas, typically within a nation state. Website blocking thus occurs country by country, based on the local IPR regime vis-à-vis local access providers and their customers.[57] In this case, the territoriality of IPRs conforms to the fragmentation of telecommunications markets.

51 This is true in particular for the UK. See *Cartier International AG v British Telecommunications Plc* [2018] UKSC 28; *Nintendo Co Ltd v Sky UK Ltd* [2019] EWHC 2376 (Ch).

52 Annemarie Bridy, 'Graduated Response American Style: "Six Strikes" Measured Against Five Norms' (2012) 23 Fordham Intell Prop Media & Ent LJ 1, 3–6; Rebecca Giblin, 'Evaluating Graduated Response' (2014) 37 Colum J L Arts 147.

53 See Christophe Geiger, 'Honourable Attempt But (ultimately) Disproportionately Offensive against Peer-to-Peer on the Internet (HADOPI)—A Critical Analysis of the Recent Anti-File-Sharing Legislation in France' (2011) 44 Intl Rev of Intell Prop and Comp L 457.

54 Case C-314/12 *UPC Telekabel Wien v Constantin Film Verleih* (CJEU, 27 March 2014) paras 32, 64.

55 See Hoeren and Westkamp (n 8) 269ff (Danish code of conduct); for Germany see https://cuii.info ("Clearing House Copyright on the Internet").

56 Ibid 269ff (20% drop in P2P file sharing in Denmark).

57 See e.g. Dirk Visser, 'Conclusions Sought: Blocking Orders—A View from the EU' in Ysolde Gendreau (ed), *Copyright in Action* (2019) 326–29 (describing how right holders achieved that the "Pirate Bay" website was blocked by all Dutch access providers).

2.2.2.3 HOST PROVIDERS AND SEARCH ENGINES

The two intermediaries examined earlier occupy very different roles in cyberspace. Whereas ICANN and its accredited registrars control the basic domain name system, access providers operate at the ends of the Internet. The geographical scope of the measures taken by these intermediaries differs accordingly. Domain name cancellations are effective across the entire Internet and thus globally, website blocking by an access provider only affects its customers (i.e. residents of a certain state).

Host providers and search engine operators control still other infrastructures. The former are able to directly interfere with IPR infringing communication by preventing uploads *ex ante*, by taking them down and by making sure they stay down.[58] Search engines, in contrast, can only reduce the findability of an illegal source by removing search results; the infringing websites themselves remain accessible.[59] The power of host providers and search engines to regulate online communication across borders and potentially even worldwide is nevertheless similar. Both are, roughly speaking, situated somewhere between domain name registrars and access providers. Their intermediary services are less basic than those of ICANN but more central than the peripheral operations of access providers.

Correspondingly, IP policies of host providers and search engines may, but need not necessarily, have transnational or even global implications.[60] The territorial effect of their IP enforcement measures depends upon technical, legal and economic circumstances. If applicable laws do not define the required or permissible geographical scope of removals or that question is unsettled,[61] host providers and search engines are left with an individual, "autonomous" decision whether to adopt and implement one single IP policy across the service or whether to reproduce the territorial fragmentation of IP and other laws by splitting up their service into country-specific versions with separate IP takedown/delisting policies. At the end of the day, this is a private business decision that can change

58 Cf 17 USC § 512(c); *L'Oréal v eBay International* (n 25) paras 125–44; DSM Directive (n 22) art 17(4).

59 17 USC § 512(d); Case C-131/12 *Google Spain v AEPD* (CJEU, 13 May 2014) paras 80–88; *Google Inc v Equustek Solutions Inc* (n 2).

60 Cf AG Szpunar (n 12) para 77 (Facebook Ireland does not deny that it is in a position to ensure such removal worldwide).

61 As in the case of EU law regarding the indirect liability of search engines for personality rights and data protection violations; cf Case C-18/18 *Eva Glawischnig-Piesczek* (CJEU, 3 October 2019) para 53 (EU law does not preclude a court of a Member State from "ordering a host provider to remove information covered by the injunction or to block access to that information worldwide within the framework of the relevant international law"); *Google LLC v Commission nationale de l'informatique et des libertés* (n 12), para 72 ("EU law does not currently require that the de-referencing granted concern all versions of the search engine in question, it also does not prohibit such a practice"). See also Proposal for a Regulation on a Single Market For Digital Services (Digital Services Act), COM/2020/825 final art 8(2)(b) (Member States shall ensure that "the territorial scope" of an order to act against illegal content, "on the basis of the applicable rules of Union and national law, including the Charter, and, where relevant, general principles of international law, does not exceed what is strictly necessary to achieve its objective").

over time and that is typically not publicly announced.[62] One already mentioned example concerns Google's search engine, which was, presumably also in light of court proceedings pending in various jurisdictions, restructured to the effect that it is not the user, by entering a particular top level domain such as .ca or .de, who determines the search result version displayed, but Google itself via geolocation technologies.[63] Host providers also sometimes use different domains for different countries, whereas others operate with a universal .com domain.[64]

In spite of the notorious lack of transparency in this realm, there are several reasons to assume that most IPR removals by host providers and search engine operators have service-wide and thus transnational effects. This is necessarily the case if a service that hosts a website takes that website down. Unless another host provider steps in, the content will become inaccessible for all Internet users worldwide. For example, a Dutch NTD code of conduct required the takedown of websites hosted in the Netherlands by Dutch providers if these were "evidently illegal" under Dutch copyright law.[65] Every element of this private ordering scheme is tied to the Netherlands—except for the effects of website takedowns, which are global.

Removals from market-dominant online platforms and search engines also significantly reduce illegal online communication. A service-wide measure of a big tech company might not be literally global (because the service may not be available in all countries, most notably China), but content delisted from, for example, Google search effectively disappears from the eye of the public in many countries.[66] Considerations of cost-efficiency will generally prompt online platform and search engine operators to implement IP removals across their services and thus also across IP jurisdictions. Accordingly, U.S. big tech companies have globalized their homegrown NTD procedures for all countries in which they operate.[67] In its "transparency report", Google states that its web form for copyright infringement notices "is consistent with the [U.S.] Digital Millennium Copyright Act (DMCA) and provides a simple and efficient mechanism for copyright owners *from countries/regions around the world*".[68] Facebook has likewise

62 Critical e.g. P Bernt Hugenholtz, 'Codes of Conduct and Copyright Enforcement in Cyberspace' in Irini A Stamatoudi (ed), *Copyright Enforcement and the Internet* (2010) Wolters Kluwer, 307; Gray (n 21) 127–33.

63 Supra (n 17).

64 European Commission, 'Report on the Functioning of the Memorandum of Understanding on the Sale of Counterfeit Goods on the Internet' SWD(2020) 166 final/2, 8.

65 Hoeren and Westkamp (n 8) 213.

66 *Google Spain v AEPD* (n 59) para 80.

67 Petersen and Riis (n 21) 235–36; Kümmel (n 26) 33–36 (concerning Facebook's copyright policies); Sharon Bar-Ziv and Niva Elkin-Koren, 'Behind the Scenes of Online Copyright Enforcement: Empirical Evidence on Notice & Takedown' (2018) 50 Conn L Rev 339, 352–53 (de facto global standard).

68 Google Transparency Report, 'Content Delistings Due to Copyright' <https://transparencyreport.google.com/copyright/overview?hl=en> accessed 23 September 2020 (emphasis added).

stated its intention to combat copyright and trademark infringement with a "*global* notice-and-takedown program".[69]

Although these statements only concern the uniformity of IP procedures, there is no reason to believe that takedowns resulting therefrom are implemented in a fragmented, country-specific way, for example only for the country from where the infringement notice was submitted. If there is only one IP policy, it will presumably be executed uniformly across the platform. Moreover, IP infringements are often also considered violations of the platforms' terms of service, which are, in the case of YouTube, "enforced consistently across the globe, regardless of where the content is uploaded. When content is removed for violating our guidelines, it is removed globally".[70] Repeat infringer policies, as implemented by most online marketplaces and user generated content (UGC) platforms,[71] necessarily produce this service-wide effect. If a subscriber's account is temporarily suspended or altogether terminated, that person simply cannot use the platform to make IPR infringing content available anywhere.

Although its geographical scope is not explicitly stated, the EU Memorandum of Understanding (MoU) "on the sale of counterfeit goods via the internet", agreed upon in 2011 between all major online marketplaces and numerous IPR holders, confirms that service-wide approach to IPR enforcement.[72] On the one hand, the MoU defines "counterfeit goods" as "non-original physical goods manufactured without the consent of the Rights Owner which infringe [a registered trademark, design right or copyright], pursuant to applicable Member State or EU law".[73] The European Commission also stresses that signatories of the MoU must comply with EU and national laws and reports that online platforms are concerned about the sometimes unclear geographical scope of the IPRs submitted as being infringed.[74] On the other hand, platform providers commit to implement NTD procedures so that notified offers become "unavailable to the general public through the Internet Platform", that is, service-wide.[75] Preventive measures, the precise layout of which remains at the discretion of platform providers, also have to prevent counterfeit goods from being offered or

69 Facebook Transparency, 'Intellectual Property' <https://transparency.facebook.com/intellectual-property> accessed 23 September 2020 (emphasis added).

70 Google Transparency Report, 'YouTube Community Guidelines Enforcement' <https://transparencyreport.google.com/youtube-policy/removals?hl=en> accessed 23 September 2020.

71 Cf European Commission (n 64) 16; IACC MarketSafe <www.iacc.org/online-initiatives/marketsafe> accessed 23 September 2020 (collaboration between trademark owners and Alibaba led to the permanent removal of 15,000 sellers from Alibaba's platforms).

72 EU Memorandum of Understanding (MoU) on the sale of counterfeit goods on the Internet, Ref Ares(2016)3934515–26/07/2016 <https://ec.europa.eu/growth/industry/intellectual-property/enforcement/memorandum-understanding-sale-counterfeit-goods-internet_en> accessed 23 September 2020.

73 MoU Counterfeit Goods (n 72) para 3.

74 European Commission (n 64) 15, 25.

75 MoU Counterfeit Goods (n 72) paras 5, 18.

sold "through their services".[76] The European Commission furthermore reports that the signatories of the MoU have set up dedicated internal teams responsible for IPR enforcement "globally".[77] It finally hopes to have facilitated a "standard" also for the "international level".[78]

Again as a kind of counterexample proving the rule of transnational enforcement, ISPs strongly oppose service-wide ("global") IP policies when it comes to measures beyond simple NTD procedures and discretionary preventive measures,[79] or when these programs are to be extended beyond clear copyright, trademark and design rights infringements (i.e. beyond "piracy" and "counterfeiting"). If big tech accepts such additional obligations at all, it only does so on a country-by-country basis.

For example, in 2007 Google and Facebook rejected the adoption of "Principles for User Generated Content Services", which included filtering obligations for the U.S. market.[80] A 2017 UK "Code of Practice on Search and Copyright" in which Google et al. voluntarily agreed to, *inter alia*, automatically demote "infringing websites" in the search results and prevent the generation of autocomplete suggestions leading consumers towards those sites, is explicitly limited to search results "returned to consumers in the UK".[81] YouTube's Content ID system, with which the company turned its copyright liability risk into a money-making machine, also functions country-specific. Under this program, registered copyright owners can submit video files to YouTube which then scans all user uploads against its reference database.[82] When content in a video on YouTube matches a work in the reference database, right holders receive an alert and can decide whether they want the content to be blocked, monetized or whether they prefer to track the video's viewership statistics. Any of these actions can be country-specific; for instance "a video may be monetized in one country/region and blocked or tracked in another".[83] Whereas YouTube advertises this private NTD+ system as a great success, it

76 Ibid, para 27.

77 European Commission (n 64) 16.

78 Ibid 38.

79 Cf MoU Counterfeit Goods (n 72) para 27 s 2 ("The measures taken by Internet Platforms shall be at their discretion").

80 See 'The Principles for User Generated Content Services: A Middle-Ground Approach to Cyber-Governance' (2008) 121 Harv L Rev 1387, 1400 (caveat for voluntary application of the principles "outside the United States").

81 See 'Code of Practice on Search and Copyright' [2017] <www.eff.org/deeplinks/2017/03/foia-uncovers-part-uk-shadow-regulation-search-engines-and-copyright#footnoteref1_emf9g2x> accessed 23 September 2020.

82 Taylor B Bartholomew, 'The Death of Fair Use in Cyberspace: YouTube and the Problem with Content ID' (2013) 13 Duke L & Tech Rev 66.

83 YouTube Help, 'How Content ID Works' <https://support.google.com/youtube/answer/2797370?hl=en> accessed 23 September 2020; Christina Angelopoulos and others, *Study of Fundamental Rights Limitations for Online Enforcement Through Self-regulation* (2016) 65.

intensively lobbied against the EU's move to make its adoption mandatory.[84] To give one final example, the transparency reports YouTube, Facebook and other large social media platforms are obliged to produce under a German Anti-Hate-Speech-Law demonstrate that this "Network Enforcement Act" is implemented only for users in Germany. If YouTube et al. are notified of an alleged violation of the German act, they apply, in a first step, their global community standards. Only if a post is found to be in conformity with this universal standard, is it, in a second step, measured against the German statute. If content passes community standards but fails German law, it is removed only for Germany but remains accessible in all other countries.[85]

2.2.2.4 FOLLOW THE MONEY: ADVERTISING AND PAYMENT SERVICES

IP infringers acting for profit not only depend on the services of domain name registrars and various ISPs, but furthermore on advertising and payment services. If no ads appeared on illegal streaming sites and no payment transactions were executed for counterfeiters, these actors would quickly be forced out of their illegal business. Although it is highly questionable whether advertisers, providers of online ad services such as Google AdSense, and payment processors such as PayPal are indirectly liable for IP infringements committed by their customers/partners, these intermediaries have in the second decade of the 21st century become the target of an IP enforcement strategy called "follow the money".[86]

In several countries, right holder associations, advertisers (brand owners) and providers of online ad and consumer tracking services have agreed to procedures that aim at avoiding the placement of ads on websites "which have no substantial legitimate uses".[87] To this end, right holders, sometimes in collaboration with public authorities such as the London Police Intellectual Property Crime Unit, compile a database of IP infringing websites and share this with advertisers, who in turn instruct online intermediaries (e.g. Google) to prevent

84 See DSM Directive (n 22) art 17(4)(b); YouTube Help, 'Updates on Article 17 (formerly Article 13)' <https://support.google.com/youtube/thread/17592587?hl=en> accessed 23 September 2020.

85 Lena Isabell Löber and Alexander Roßnagel, 'Das Netzwerkdurchsetzungsgesetz in der Umsetzung' (2019) Multimedia und Recht 71–72.

86 EU: European Commission, 'Towards a Modern, More European Copyright Framework' COM(2015) 626 final/11; European Commission (n 29) 3. US: Annemarie Bridy, 'Internet Payment Blockades' (2015) 67 Fla L Rev 1523, 1529–30; Erika Douglas, 'PayPal Is New Money: Extending Secondary Copyright Liability Safe Harbors to Online Payment Processors' (2017) 24 Mich Telecomm & Tech L Rev 45.

87 Section I 1, EU Memorandum of Understanding (MoU) on online advertising and IPR (2018) <https://ec.europa.eu/growth/industry/intellectual-property/enforcement/memorandum-of-understanding-online-advertising-ipr_en> accessed 23 September 2020; WIPO Advisory Committee on Enforcement, 'The Building Respect for Intellectual Property Database Project' (2019) WIPO/ACE/14/9, 2 ("pirate websites").

the appearance of their ads on these blacklisted outlets.[88] Despite the fact that ad intermediaries again operate at scale and therefore have an economic interest to apply such blacklisting practices across their services, the self-regulatory codes on point explicitly take a country-by-country approach. The memorandum facilitated by the European Commission is "limited for each signatory to services provided in the States that are Contracting Parties to the European Economic Area"; an Austrian ethics code only covers pirate websites directed to an Austrian audience, UK Good Practice Principles on point apply to websites targeting UK users, and so on.[89] This restrictive attitude towards IP policies in the advertising context stands in stark contrast to service-wide and thus "global" NTD procedures. It may reflect the much weaker legal case for holding advertisers and ad intermediaries accountable for IP infringements on third-party websites. Whereas there is a rough global consensus that host providers and search engines have to remove apparent IP infringements, there is no such agreement regarding the ad industry.[90]

This weakness has been remedied, however, by a remarkable intervention by the World Intellectual Property Organization (WIPO). After having secured a mandate from its member states, WIPO developed, and in 2019 started, the "WIPO ALERT" online platform, which functions as a global hub for national IP ad programs.[91] Upon signing a letter of understanding with WIPO, "Authorized Contributors" from any of WIPO's 193 member states can upload lists of copyright infringing website URLs to WIPO's database. Advertisers, advertising agencies and their technical service providers from any other WIPO member state can apply to become "Authorized Users" of WIPO ALERT. Following a check on their "bona fides", they can access and automatically implement the blacklists collected "from around the world".[92] As with the European Commission and other public authorities, WIPO describes its role as that of a neutral facilitator of legitimate enforcement practices. WIPO also expressly points out that it does not assert "that any particular site has, as a matter of law, infringed copyright". Rather, the blacklisted "sites of concern" are defined as "an online location which

88 Hoeren and Westkamp (n 8) 103ff (Austrian "ethics code"), 147ff (UK "Good Practice Principles for the Trading of Digital Display and/or Audio Advertising"); WIPO Advisory Committee on Enforcement (n 87) 2; Gray (n 21) 120–21. On the complex structure and functioning of the online ad industry cf Michail Batikas, Jörg Claussen and Christian Peukert, 'Follow the Money: Online Piracy and Self-Regulation in the Advertising Industry' (2019) 65 Int J Ind Organ 121–51.

89 EU MoU Advertising (n 87) 2; White Bullet Solutions, *Study on the Impact of the Memorandum of Understanding on online Advertising and Intellectual Property Rights on the online Advertising Market* (2020) 9; Hoeren and Westkamp (n 8) 111, 180; WIPO Advisory Committee on Enforcement (n 87) 2.

90 European Commission (n 29) 12 (signatories will look into how to duplicate and expand the MoU "if possible, outside the EU").

91 WIPO ALERT <www.wipo.int/wipo-alert/en/> accessed 23 September 2020.

92 WIPO Advisory Committee on Enforcement (n 87) 3–4, 7 ("the operation is entirely seamless and requires no human intervention").

is reasonably suspected by an Authorized Contributor of deliberately infringing or facilitating the infringement of copyright and related rights, *whether in its country of establishment or elsewhere*".[93] This definition is inspired by Sec. 115A of the Australian Copyright Act, which provides for blocking orders against access providers under the condition that "the primary purpose of the online location is to infringe . . . copyright (*whether or not in Australia*)".[94] WIPO accordingly maintains that in practice only "invariably flagrant facilitators of copyright infringement" are covered by the ALERT database and thus cut off from the global flow of advertising revenues.[95]

The second target of "follow the money" approaches are providers of online payment services like PayPal and credit card companies like Visa or Mastercard. These intermediaries are powerful because they are able to monitor suspicious merchants and link their activity across different banks. Whereas Europe appears to be the hot spot of efforts to get the highly diversified and geographically dispersed advertising industry on board,[96] the U.S. government has encouraged and supported an initiative called "RogueBlock®", which was launched in 2012 and now includes many of the biggest payment providers in the world. RogueBlock® was brokered by the Washington, D.C.-based International AntiCounterfeiting Coalition (IACC), a nonprofit organization devoted solely to combating product counterfeiting and piracy, whose membership comprises more than 250 companies and organizations from 40+ countries.[97] RogueBlock® offers IACC's members the possibility to report online sellers of counterfeit or pirated goods directly to credit card and financial service companies with the goal of facilitating prompt action against those merchants. According to the IACC, the program has terminated over 5,000 merchant accounts and impacted over 200,000 websites.[98] The geographical scope of the scheme is global in the sense that it does not matter where the "rogue" websites are hosted or the "rogue" merchants domiciled.[99] Instead, RogueBlock® is triggered as soon as goods offered through a website do not comply with IP laws in either the country of origin or the country of destination. Any transaction that is not in full "dual jurisdictional compliance" at the places of origin and destination is considered illegal. Merchants engaging in

93 WIPO Advisory Committee on Enforcement (n 87) 3–4 (emphasis added).

94 See sec 115A Copyright Act 1968, as of 1 January 2019 <www.legislation.gov.au/Details/C2019C00042> accessed 23 September 2020 (emphasis added) and WIPO Advisory Committee on Enforcement (n 87) 4 with fn 5.

95 See WIPO Advisory Committee on Enforcement (n 87) 7 (WIPO cooperating with the European Commission in this field).

96 Ibid 3–4.

97 Website of IACC <www.iacc.org/> accessed 23 September 2020.

98 IACC RogueBlock <www.iacc.org/online-initiatives/rogueblock> accessed 23 September 2020; Bridy (n 86); Aniket Kesari and others, 'Deterring Cybercrime: Focus on Intermediaries' (2017) 32 Berkeley Tech LJ 1093, 1128.

99 Hoeren and Westkamp (n 8) 346.

such illegal activity risk being cut off from the global payment system, even if their offerings are lawful at their domicile and/or in third countries.[100]

2.2.3 Summary

The review of intermediaries' IP enforcement measures and accompanying codes of conduct demonstrates that most of them are transnational in scope. From a legal perspective, this finding can be explained with the focus of all regimes on plain infringements (cybersquatters, piracy, counterfeiting, "rogue" merchants). Hard cases of conflicts of IP laws/rights are, instead, resolved in a country-specific way according to the territoriality principle. From a technological perspective, transnational measures typically attach to the source of the infringement (domain name cancellations, takedowns, termination of payment accounts). Measures that instead apply to the recipient's end of the communication (i.e. website and advertisement blocking) are generally local in effect, but WIPO's remarkable ALERT database aims to make advertisement blocking global, too. Ultimately, only website blocking by access providers remains tied to certain real-world territories. The reason is that access providers operate on the physical layer of the Internet, and this tangible infrastructure is located in a particular country.

3 Licensing IPRs

Instead of prohibiting the use of protected IP by enforcing their rights, right holders are alternatively free to grant licenses and thus authorize uses. Whereas the territoriality principle complicates transnational IP enforcement on the Internet, the existing legal framework is in fact conducive to global online licensing.

Firstly, the rules governing initial ownership of IPRs are by and large uniform around the world, ensuring that the same person, in particular the author of a work and the one who first files for a patent or other registered IPR, acquires the complete bundle of national IPRs. If the rules on initial ownership diverge (author versus employer/commissioner; first-to-file versus first-to-invent), the parties involved share an interest in avoiding a split of initial and subsequent chains of titles in the same IP. Accordingly, courts presume that all relevant rights have been implicitly transferred to one single entity.[101] That global right holder is, secondly, at liberty to exercise her "private"[102] territorial rights uniformly at a

100 Critical of this extraterritorial effect Bridy (n 86) (calling for a "zoning" of online payment blockades to only apply to transactions involving U.S. customers).

101 Cf German Federal Court of Justice, case X ZR 14/17, openJur 2019, 1813, paras 83–107 (concerning the transfer of a right of priority); Josef Drexl in European Max Planck Group on Conflict of Laws in Intellectual Property (CLIP), *Conflict of Laws in Intellectual Property, The CLIP Principles and Commentary* (2013) paras 3:201. C01-N24.

102 See preamble, TRIPS.

global scale, be it by producing and selling IP-protected products on the world market or by granting a worldwide license to one single licensee.

In practice, however, IPRs are often monetized on a country-by-country basis. A global "celestial jukebox" as imagined by Paul Goldstein in the early 1990s, where users could access any content from any place at any time in exchange for a (micro)payment, has yet to materialize.[103] According to a 2017 report by the European Commission on e-commerce in the EU, this is also true for the online commercialization of copyright-protected content in the "Digital Single Market". According to the Commission, a "majority of online digital content seems to be made available to users prevalently on a national basis, or for a territory covering two to four Member States, in the latter case when they share a common language".[104] The Commission further reports that "70% of digital content provider respondents restrict access to their online digital content services from other Member States".[105] Geo-blocking is implemented with regard to all types of digital content except for news products, and it is most prevalent in agreements for films, sports and TV series.[106] What is true for the EU Single Market is all the more true for the global market. Not surprisingly therefore, YouTube's Content ID program allows right holders from all over the world to control their content on the platform in a country-specific way so that "a video may be monetized in one country/region and blocked or tracked in another".[107] Shira Perlmutter, currently the Chief Policy Officer and Director for International Affairs at the U.S. Patent and Trademark Office and formerly a high-ranking IP executive in the music and movie industries, also believes that "territoriality will endure for the foreseeable future".[108]

Aside from the online music sector, where national collective management organizations are important players who bridle at giving up their national monopolies,[109] the global legal framework is, as explained, not the prime reason for the persistence of territorial licensing and geo-blocking. Instead, right holders split up geographical markets because they consider this the optimal business

103 Paul Goldstein, *Copyright's Highway: From Gutenberg to the Celestial Jukebox* (2003) Stanford Law and Politics, 132ff.

104 European Commission, 'Final Report on the E-commerce Sector Inquiry' SWD(2017) 154 final/255–56.

105 Ibid.

106 Ibid.

107 Supra (n 83).

108 Shira Perlmutter, 'Making Copyright Work for a Global Market: Policy Revision on Both Sides of the Atlantic' (2014) 38 Colum JL & Arts 49, 67–68; Tarja Koskinen-Olsson, 'Multi-Territorial Licenses' in José Maria Torres Caicedo (ed), *Dissemination and Management of Works of Authorship on the Internet* (2018) Creative Media Partners, 377–85 (trend towards multi-territorial licensing).

109 See Council Directive 2014/26/EU of 26 February 2014 on collective management of copyright and related rights and multi-territorial licensing of rights in musical works for online use in the internal market [2014] OJ L 84/72, arts 23–32 (setting out rules in support of multi-territorial licenses for online rights in musical works).

decision. Product and price differentiations indeed respond to divergent local demand and purchasing power and thus promise maximum profits.[110] Geoblocking to this end is furthermore supported by laws that prohibit the circumvention of technological protection measures.[111]

Authorized global access is, conversely, never coupled with a direct payment requirement. Instead, the right holder provides access for anyone in any country for free and may, as the case may be, try to monetize her Open Content indirectly, in particular via advertising. Content categories that are particularly often distributed in this way include news, academic writings, software and various types of non-professional UGC. Numerous licensing standards are available for this mode of distribution, notably various Free and Open Source Software and Creative Commons licenses.[112] Where no such formal license is adopted, courts interpret the free availability of copyright-protected content as an implied authorization by the right holder of foreseeable, commonly accepted Internet re-uses such as the copying and making available of pictures by search engines.[113] Both formal and implied Open Content licenses authorize uses in all countries, that is, globally.

In sum, authorizations to use protected IP across the entire Internet are less prevalent than one might expect. Markets for fee-based services remain territorially fragmented. Global lawful access is practically limited to Open Content, which typically does not include the most popular and in that sense valuable works.[114]

4 Conclusion

This chapter has brought together a dizzying array of IP governance practices on the Internet, whose varying geographical scopes are caused by a complex mixture of legal, technical and economic factors. It is, however, possible to condense useful conclusions from this review for the law of global digitality ("cyberlaw") in general and IP law in particular.

110 William W Fisher III, 'Property and Contract on the Internet' (1998) 73 Chicago-Kent L Rev 1203.

111 World Copyright Treaty (adopted 20 December 1996, entered into force 6 March 2002) 2186 UNTS 121 (WCT) arts 11, 12; WIPO Performances and Phonograms Treaty (adopted 20 December 1996, entered into force 20 May 2002) 2186 UNTS 203 (WPPT) arts 18, 19; Tatiana Eleni Synodinou, 'Geoblocking in EU Copyright Law: Challenges and Perspectives' (2020) 69 GRUR International 136.

112 See Axel Metzger (ed), *Free and Open Source Software (FOSS) and other Alternative License Models* (2016) Springer.

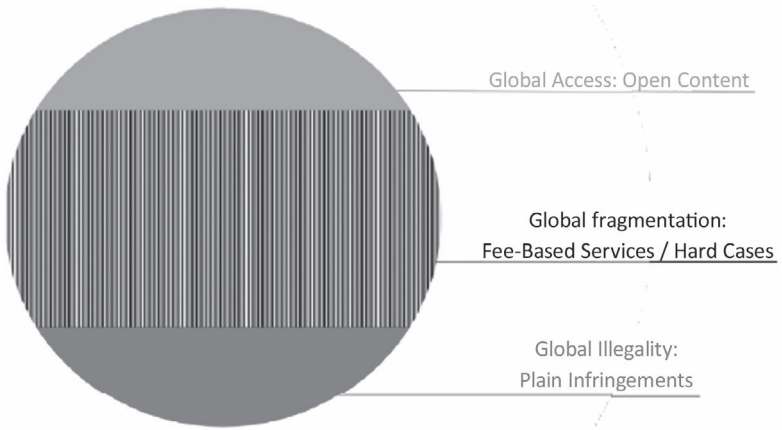
113 German Federal Court of Justice, case I ZR 69/08, openJur 2010, 528, paras 36ff (commercial picture search implicitly authorized); Case C-466/12 *Nils Svensson v Retriever Sverige AB* (CJEU, 13 February 2014) paras 23ff (hyperlinks).

114 On this distinction see Alexander Peukert, 'Copyright and the Two Cultures of Online Communication' in Paul LC Torremans (ed), *Intellectual Property Law and Human Rights* (4th edn, 2020) Wolters Kluwer, 387.

Firstly, this chapter confirms but also qualifies the widely held assumption that code is the dominant mode of cyberspace regulation.[115] It is true that all effective forms of regulating online communication are executed via software. In some cases examined herein, the functionality of the code also has an impact on the geographical scope of the measure. Thus, domain name cancellations necessarily have global effects, whereas the blocking of a website by an access provider can only affect its customers, all of whom reside in a certain region. But if code can be implemented either globally or locally, technology is not determinative as to the geographical scope of IP policies online. Host providers such as Facebook and YouTube operate with service-wide and geographically targeted IP enforcement algorithms at the same time. From a legal point of view, code therefore remains an accessory tool.[116]

Secondly, the chapter demonstrates that private ordering is the primary mode of transnational IP governance on the Internet.[117] Aside of quantitatively insignificant and legally dubious takedown orders of courts with de facto global effects, all instances of transnational IP regulation have been found to be based upon "voluntary" self-regulation by private actors, namely right holders and various intermediaries. Only if and in so far as these actors are willing to execute their rights or their control with regard to Internet infrastructure in a cross-border manner will the territorial fragmentation of IP law be overcome. At the same time, states step back into the nevertheless important role of a facilitator, in whose shadow private actors define their online IP policies.

Finally and most importantly, this chapter brings to light three layers of global Internet governance in the area of IP, which can be represented graphically like this:



115 Cf Lawrence Lessig, *Code and Other Laws of Cyberspace* (1999) Basic Books, 3–60; Reidenberg (n 28), 554–55; Mireille Hildebrandt, *Smart Technologies and the End(s) of Law* (2015) Edward Elgar, 214–15 (legal protection by design).

116 Hildebrandt (n 115) 214–15.

117 Joel R Reidenberg, 'Governing Networks and Rule-Making in Cyberspace' (1996) 45 Emory LJ 911, 921; Monroe E Price and Stefaan G Verhulst, *Self-Regulation and the Internet* (2004) Kluwer Law International, 10–22; Niva Elkin-Koren and Eli M Salzberger, *The Law and Economics of Intellectual Property in the Digital Age* (2013) Routledge, 149–82.

The layer on the top concerns Open Content, which is subject to a global norm, namely its free accessibility irrespective of the locus of the right holder, the user and any intermediary involved. The layer on the bottom also depicts a global norm, this time the illegality of plain IP infringements on a commercial scale. It includes the cancellation of domain names registered by "cybersquatters" not having any rights or legitimate interests in respect of the domain name, the blocking of websites not containing a substantial amount lawful information, takedowns of apparently infringing uploads and search results, the blacklisting of websites for advertising purposes whose primary purpose is to infringe, and the termination of payment accounts of "rogue" merchants selling counterfeit or pirated goods.[118] The intermediate layer pertains to licensed, fee-based services and hard cases of conflicts of IP laws/rights. In these markets and legal disputes, territorial fragmentation and thus shades of gray reign.

The fact that the three modes of communication and regulation prevail worldwide indicates that they enjoy a high level of legitimacy. The Open Content layer and the market layer derive their legitimacy from the worldwide recognition of IPRs as territorially limited, private rights. One hundred and sixty-four WTO and 193 WIPO member states share the view that it is, as a rule, up to the right holder to decide who may use protected IP, under which conditions, and where. If that person finds it proper to grant all Internet users free access to its IP or if she, alternatively, prefers to employ geo-blocking technologies and sell digital goods in certain markets only, so be it. Under the concept of private property, both decisions are equally legitimate. It follows that IP and other laws affecting global digitality should not distort the equilibrium between the open, participative Internet on the one hand and fragmented markets for IP on the other by threatening the very existence of any of these cultures of communication.[119]

More contentious is the legitimacy of global enforcement measures against cybersquatters, counterfeiters, pirates and other "rogue" actors. From an IP perspective, the extraterritorial reach of cancellations, takedowns and blockings, which are supported only by one or few possibly unspecified IP laws, is problematic.[120] Self-regulatory procedures with worldwide effects also raise concerns as regards their lack of transparency and the difficulty to attribute responsibility to the private and public actors involved.[121] It is feared that far-reaching measures like website blocking can lead to "privatized censorship of online material and other interferences with fundamental rights without a clear legal way of

118 Supra 2.2.2.

119 Peukert (n 114) 414.

120 Peukert (n 3) 189–228; Trimble (n 11) 541.

121 Hugenholtz (n 28) 319 ("democratic deficit"); Derek E Bambauer, 'Against Jawboning' (2015) 100 Minn L Rev 51, 60–61; Perel and Elkin-Koren (n 21); Bloch-Wehba (n 29) 79. But see Perlmutter (n 108) 67–68 (arguing that "the long-term future may be in the direction of more general principles in public rules, with more nimble and detailed adaption of those principles through private ordering").

redress or appropriate safeguards such as due process".[122] False positives indeed occur, in particular in the course of billions of host provider and search engine takedowns.[123]

In contrast, several self-regulatory IP policies targeting cybersquatters, counterfeiters, pirates or rogue merchants acting on a commercial scale have been smoothly operating for years without producing many complaints about false positives.[124] This fact indicates that the regimes in place are supported by a "rough" global consensus, which is generally sufficient for transnational cyberlaw.[125] And indeed, effectively all states agree that making a current motion picture available on the Internet or selling a product under a well-known trademark without the authorization of the respective right holders is illegal.[126] Regarding "copyright piracy on a commercial scale" and "wilful trademark counterfeiting", Art. 61 of TRIPS even obliges all WTO members to provide for criminal procedures and penalties including imprisonment and/or monetary fines sufficient to provide a deterrent. In light of this international law *acquis*, private global enforcement measures against hardcore IP infringements also appear acceptable.

122 Angelopoulos and others (n 83) 2; Maria Lillà Montagnani, 'Virtues and Perils of Algorithmic Enforcement and Content Regulation in the EU—A Toolkit for a Balanced Algorithmic Copyright Enforcement' (2020) 11 Case W Reserve JL Tech & Internet 1, 28ff.

123 Cf *Lenz v Universal Music Corp* 801 F 3d 1126 (9th Cir 2015); Bar-Ziv and Elkin-Koren (n 67); Toni Lester and Dessislava Pachamanova, 'The Dilemma of False Positives: Making Content Id Algorithms More Conducive to Fostering Innovative Fair Use in Music Creation' (2017) 24 UCLA Ent L Rev 51.

124 Supra (n 39) (UDRP court reviews); European Commission (n 64) 26–27 (setting out the need to provide internal complaint-handling systems).

125 Callies and Zumbansen (n 43).

126 Trimble (n 11) 540–41.

Part II
Data Protection/Privacy

3 The More the Merrier

A Dynamic Approach Learning From Prior Misgovernance in EU Data Protection Law

Indra Spiecker gen. Döhmann

1 Introduction[1]

Data protection law could be considered to be the core legal regime of internet and digitalisation research. After all, it arose as a completely new field of regulatory approach to a technological development unknown until then—automated data processing and automated decision-making. As such, it can be compared to other legal areas which also addressed new technological phenomena, for example atomic energy or genetic engineering law.

However, the question remains whether the original setting and content of data protection law is still in sync with today's approach to regulation of the consequences of the use of digital tools, services and the necessary data processing accompanying our increasingly digitalised world. Maybe, so the hypothesis in the following chapter, learning about ubiquitous computing, big data, cloud computing, high-speed volume processing or artificial intelligence has altered the approach on how to control data processing and automated decision-making, and so we find a new legal regime.

This hypothesis could easily be affirmed considering the rhetoric when, in 2018, the European General Data Protection Regulation (GDPR)[2] took effect and the prior Data Protection Directive (DPD)[3] gave way. "The new framework is ambitious, complex and strict"[4] and "radical",[5] it "replaces the archaic Data

1 Due to the character of the chapter as an overview, an extensive catalogue of literature has been avoided.

2 Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1.

3 Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] *OJ L 281/31.*

4 Warwick Ashford, 'D-Day for GDPR is 25 May 2018' [2016] ComputerWeekly <www.computerweekly.com/news/450295538/D-Day-for-GDPR-is-25-May-2018> accessed 21 May 2021.

5 Larry Downes, 'GDPR and the End of the Internet's Grand Bargain' [2018] Harvard Business Review <https://hbr.org/2018/04/gdpr-and-the-end-of-the-internets-grand-bargain> accessed 21 May 2021.

DOI: 10.4324/9781003283881-6

Protection Directive 95/46/EC"[6] and it "is set to force sweeping changes in everything from technology to advertising, and medicine to banking".[7] At the same time, the EU DPD in place until then was described as "no longer relevant to today's digital age".[8]

However, a closer look at the present regulatory regime of data protection law in comparison to its onset may reveal a more differentiated result in analysis and thus help to better understand the effects of global digitality. The present analysis concentrates on a European approach, looking in particular at the GDPR and to what extent it addresses new phenomena and whether it construes new instruments and new goals.

2 The Historical Approach to Data Protection Law—An Overview

2.1 Goals

Data protection law has addressed four major goals from its beginning:

Firstly, it discovered automated decision-making as a new subject for regulation. In the 1960s, in particular State administrations, but also private entities realized a growing need for new information in an increasingly complex world that called for new information technology and new information processing to master these challenges.[9] New production devices, credit and loan business models and marketing needs in the private sector as well as a demand for governance and planning in the administrative area called for more information and better use of existing information and thus for new ways of organising and structuring data.[10] As automatisation of data processing was intended to make

6 Mihaela Lica Butler, 'GDPR Goes into Effect in May 2018. Is Your Business Compliant?' [2018] Carmelon Digital Marketing <www.carmelon-digital.com/articles/gdpr-general-data-protection-regulation/> accessed 21 May 2021.

7 Alex Hern, 'What is GDPR and How Will It Affect You?' [2018] The Guardian <www.theguardian.com/technology/2018/may/21/what-is-gdpr-and-how-will-it-affect-you> accessed 21 May 2021.

8 Andrew Rossow, 'The Birth of GDPR: What Is It and What You Need to Know' [2018] Forbes <www.forbes.com/sites/andrewrossow/2018/05/25/the-birth-of-gdpr-what-is-it-and-what-you-need-to-know/> accessed 21 May 2021.

9 Spiros Simitis and others, in Spiros Simitis/Hornung/Spiecker (eds), *Kommentar Datenschutzrecht. DSGVO mit BDSG* (1st edn, 2019) Introduction para 6; Jürgen Kühling and Johannes Raab, in Jürgen Kühling and Benedikt Buchner (eds), *Datenschutz-Grundverordnung Kommentar* (1st edn, 2017) Introduction para 37; Alan F Westin, 'Science, Privacy, and Freedom: Issues and Proposals for the 1970's: Part I—The Current Impact of Surveillance on Privacy' (1966) 66 Colum L Rev 1003, 1003; Spiros Simitis, 'Reviewing Privacy in an Information Society' (1987) 135 U Pa L Rev 707, 709ff.

10 Simitis/Hornung/Spiecker (n 9) Introduction para 7ff; Martin Selmayr and Eugen Ehmann, in Martin Selmayr and Eugen Ehmann (eds), *Datenschutz-Grundverordnung Kommentar* (2nd edn, 2018) Introduction para 9; Spiros Simitis, 'Reviewing Privacy in an Information Society' (1987) 135 U Pa L Rev 707, 709ff.

data available for multiple purposes, it quickly became obvious that information was now devoid of context and thus devoid of control of the subject of the information.

Secondly, based on this understanding, availability of data and the technical ability to make use of it created an imbalance of power until then unknown.[11] Whoever has the tools to collect and use available data, may then make use of this information for influencing decisions. As a consequence, individuals could become objects of (potentially positively) private and administrative planning, governance and (potentially negatively) manipulation and control. Thus, the core of data protection is to regulate the informational power asymmetry.

Thirdly, data protection required the regulation of data processing and thus clear enforceable legal rules. Behind this is the understanding that the impact of data processing can be so burdensome on individuals and their legal and societal interests that only a legislative act could ensure proper protection.[12] Other tools, in particular self-regulation of, for example, the private information technology industry would not suffice.

Finally, it had become clear that the processing of data was not a single act restricted to certain areas of life. Rather, data protection needed to address all areas where information technology and thus automated data processing was taking place.[13] This required umbrella regulation binding every act of data processing.

2.2 Instruments

Pursuing these four goals, the first data protection regulatory regimes—in particular in Hessia in Germany in 1970 as the world's first data protection law, but also in the European DPD in 1995—included particular instruments to achieve them. Among the many issues one could potentially raise here, only two will be pointed out in particular:

Firstly, these early data protection legal regimes were viewed in the tradition of technology law, thus making use of established principles and structures of this field of law. Automated decision-making was considered to be a new technology with unknown consequences that needed regulation and control, similar to atomic energy, emissions or chemicals. One consequence of this model function of technology law resulted in data protection laws acting from

11 Cf Simitis/Hornung/Spiecker (n 9) Introduction para 22; Orla Lynskey, *The Foundations of EU Data Protection Law* (1st edn, 2016) 1; cf Lorna Stefanik, *Controlling Knowledge—Freedom of Information and Privacy Protection in a Networked World* (1st edn, 2011) 29; Walter Schmidt, 'Die bedrohte Entscheidungsfreiheit' (1974) 29 JuristenZeitung 241, 246.

12 Cf Simitis/Hornung/Spiecker (n 9) Introduction para 17; Selmayr and Ehmann (n 10) Introduction para 18, 21; Schmidt (n 11).

13 Simitis/Hornung/Spiecker (n 9) Introduction para 19.

a preventive standpoint. They followed the principle of precaution as known in technology law. Rather than setting up new rules for liability or duties of care to govern from a secondary law approach, they focused on regulating the processing of data at its origin on the primary level. Thus, the results of data processing, the decisions following from the access to and use of data, were not typically addressed.[14]

Secondly, concerns about the frequent use of automated decision-making arose first in regard to the availability of data and information technology in the hands of the State. The reason for this can be understood in the availability and the state of art of the information and communication technology itself: In the 1960s and 1970s, only very few players had a need and the resources to make use of existing data processing tools. One should also not forget that information technology was often pushed forward by secret services and other State actions. If states increased their power over citizens, so the conclusion was, it was a highly threatening situation for human rights and the democratic idea.

Therefore, data protection laws at first primarily addressed the balancing of public interests favouring State access to and use of data and individual rights guaranteeing individual freedom and autonomy. Consequently, early influencing decisions such as the census decision of the German Constitutional Court in 1983 concentrate on limiting the power of the State while ignoring potential power shifts towards private entities due to the use of information technology and data processing. Private use of these technologies was, overall, addressed less frequently and less intensely. In consequence, the rise of the internet in the 1990s and the rise of private actors in data processing including ubiquitous access to data processing services, hard- and software has often been neglected.

3 Reaction of Today's Data Protection Law to the Challenges of Global Digitality

When looking at these beginnings of data protection one could conclude that little has changed. All of the previously mentioned goals of data protection law are still valid, the GDPR is based on them, and it seems—to answer the general question of this book—that data protection may prove to be a stronghold in legal regimes where digitalisation has not changed the existing approach to regulation much. This would even seem consistent with the finding that data protection from its beginning addressed digitality. Thus, one could easily state that global digitality has surpassed data protection, and rightly so.

14 Simitis/Hornung/Spiecker (n 9) Introduction para 17; Kühling and Raab (n 9) Introduction para 38.

However, when looking more closely at the individual provisions of the GDPR as the successor to the previous DPD, we do find some activity in regard to the special effects of digitalisation. After all, the GDPR is a reaction to some experiences on the basis of prior data protection law, of its ineffectiveness and its minimal and contradicting enforcement.[15] One may also add that the GDPR now reflects a better understanding of the value and qualities of information, the economic effects of its characteristic as a so-called "common good", as well as the particular importance of the internet cumulating, for instance, in "winner-takes-all" markets.[16]

A reaction to the enforcement deficit can be identified in a number of norms of the GDPR. Also, some findings of economics (information as a public good; the network effects of information infrastructure and social platforms) have clearly been the foundation of some norms (e.g. in data portability, Art. 20 GDPR). Also, we observe a reaction to globalisation in the distribution of information and use of information technology, and thus the need to regulate beyond national borders (e.g. in the market principle of Art. 3 para. 2 GDPR as well as some decisions of the CJEU, such as *Google Spain*, 2014).[17]

Based on these few general remarks about early data protection law, the following analysis will look at the dominant present regulatory regime in data protection, the GDPR. When looking at individual regulatory goals and tools, the comparison to the prior regulatory regime will be undertaken.

3.1 Core Regulatory Goals

The recitals of the GDPR provide a number of goals. No. 2 explicitly states that

> the Regulation is intended to contribute to the accomplishment of an area of freedom, security and justice and of an economic union, to economic and social progress, to the strengthening and the convergence of the economies within the internal market, and to the well-being of natural persons.

Considering this vast amount of goals, one could declare that by trying to achieve all of them, the GDPR will fail to achieve any of them. However, when looking closer, one can identify a few core principles the GDPR wants to achieve and does indeed undertake great efforts to achieve them.

15 Jan Philipp Albrecht, in Simitis/Hornung/Spiecker (n 9) Introduction para 185ff; Jan Philipp Albrecht and Florian Jotzo, *Das neue Datenschutzrecht der EU* (1st edn, 2017) 50 para 1; Kühling and Raab (n 9) Introduction para 73.

16 Cf Indra Spiecker gen. Döhmann, 'Information Management' in Peter Cane and others (eds), *The Oxford Handbook on Comparative Administrative Law* (1st edn, 2021) Oxford University Press, 677, 679ff; Rupprecht Podszun and Stephan Kreifels, 'Digital Platforms and Competition Law' [2016] EuCML 33, 38.

17 Case C-131/12 *Google Spain SL og Google Inc v Agencia Española de Protección de Datos (AEPD) og Mario Costeja González* (CJEU, 13 May 2014).

3.1.1 Data Protection as a Safeguard of Democracy

The GDPR identifies as a core regulatory need the regulation of the importance of information for the division of power and thus to avoid power asymmetry based on information. In order for natural persons to be able to execute their freedoms, the political, economic and societal conditions must be construed in a way that allows them to be effective. The amount of information present about an individual, and in close connection to this the individual's knowledge about the information present about her, determines how a business partner, the administration or a third party will assess the individual and make decisions about her. An individual, who is not aware of what is known about her, loses the possibility of self-protection, to give additional information contradicting or strengthening what is already known and to enter into a fair bargain. This individual will not be able to assess her own reactions and the reactions of the other party. In the end, out of insecurity and uncertainty, individuals may refrain from enacting their freedoms if they are unable to assess potential consequences. The newer terminology describes this as "chilling effects": Freedoms and liberties still exist, but their functional enactment is hindered by the circumstances.[18]

Chilling effects not only impact the individual, but the free and democratic society as such. The German Constitutional Court stated this very early on in its ground-breaking census decision.[19] A democratic society can only exist if its members are free to participate and free to enact their freedoms. This constitutes a sphere where the individual is neither under State nor private surveillance. Data protection is then the backbone of a democratic society and guarantees the chance of truly exercising one's fundamental rights.[20]

The GDPR does not explicitly state this relationship between data protection and democracy openly. However, it is well woven into the text and the intention of the Regulation.[21] In recital No. 1, the Regulation sees its foundation foremost in the protection of Art. 8 of the EU Charter and Art. 16 of the Treaty on the Functioning of the European Union (TFEU). The GDPR clearly connects to the DPD, and despite the sometimes polemic description does not fundamentally overhaul the existing data protection regime but rather aims at solving problems not covered by the prior Directive. Recitals Nos. 5, 6 and 7 clarify that the intention of the GDPR is not to loosen the grip of the DPD on data processing but rather to continue, strengthen and fortify its impact.

18 With empirical evidence Jon Penney, 'Chilling Effects: Online Surveillance and Wikipedia Use' (2016) 31 Berkeley Technol L J 117.

19 BVerfGE 65, 1 (43).

20 Indra Spiecker gen. Döhmann, 'Fragmentierungen: Kontexte der Demokratie—Parteien, Medien, Sozialstrukturen' (2018) 77 VVDStRL 9, 55; Benedikt Buchner, in Kühling and Buchner (n 9) art 1 para 13; cf Marie-Theres Tinnefeld, 'Meinungsfreiheit durch Datenschutz—Voraussetzung einer zivilen Rechtskultur' 1 (2015) ZD 22, 22ff.

21 Simitis/Hornung/Spiecker (n 9) Introduction para 235; Spiecker gen. Döhmann (n 20).

What remains open, however, is how far the understanding of data protection as a backbone of freedom and democracy has been intensified and the measures taken to protect it more effectively due to developments on a global scale in comparison to the DPD. After all, global digitality presumes that there have been effects on existing regulatory regimes due to the increased and enlarged use of digital products, infrastructure and services.

What is obvious is the influence of some spectacular events on the EU's regulatory impulse to modernise data protection—most notably the revelations in the course of the NSA scandal in early 2013, but also the decisions of the CJEU in *Google Spain*[22] and *Data Retention*.[23] Nevertheless, these events took place *after* the EU had already decided to reform data protection law in 2009.[24] So, these events have strengthened the impulse that there is a need to protect individuals, and the NSA scandal, *Google Spain* and *Data Retention* have illustrated how quickly the power may shift to few players in the market and to a few States.

The material on the reform process, which started prior to these events, strengthens the understanding that the EU saw changes in the original direction of impact and a need to react. They provide information that the EU did indeed react to some of the changes due to the globality of digitalisation: The European Commission names among other challenges data transfer and a higher enforcement efficiency.[25] The internationalisation of data transfer and data processing, the existence of some global players, in particular in some fields of digitalisation, and the need to protect against these potential aggressors obviously was one of the reasons for action.

3.1.2 Power Asymmetry

The GDPR is also triggered in a more general perspective to react to power asymmetry on the basis of information.[26] Access to information and access to information and communication technology allow for the systematic personalisation and knowledge about individuals and their decisions. Often, knowledge and attributions about persons are construed in a way and with results that

22 Case C-131/12 (n 17); Tobias Herbst, in Kühling and Buchner (n 9) para 67ff; Jan Philipp Albrecht and Florian Jotzo (n 15) 53 para 7.

23 Joined Cases C-293/12 and 594/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärtner Landesregierung and Others* (CJEU, 8 April 2014).

24 The Stockholm Programme—an open and secure Europe serving and protecting citizens (2010) OJ C115/01.

25 Commission, 'Communication from the Commission of the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions. A Comprehensive Approach on Personal Data Protection in the European Union' COM (2010) 609 final 4.

26 Gerrit Hornung and Indra Spiecker gen. Döhmann, in Spiros Simitis/Hornung/Spiecker (n 9) art 1 para 31.

these persons themselves would never be able to produce as they lack technological and other resources and also the access to them. As a consequence, any entity capable of accessing personal data and of making use of this data receives uncontested power over the individual. The individual, however, is unable to control the data present about her and consequently about any assessments or decisions on this basis. This is in particular true as decisions typically do not reveal which information was used. This entity can be the State, or it can be a private entity.

The DPD and the beginnings of data protection focused in particular on the State and few private actors for reasons of resources. Automated data processing was accessible only to large entities with significant resources and with a large demand of information processing. The GDPR, however, enlarges the perspective. It explicitly takes the availability of information technology in the private sector into focus because of the unprecedented spreading of digital tools and services[27] and thus reacts to the development of digital technology.

While State data processing is exempted to a certain extent because of the dormant opening clause of Art. 6 para. 1 lit. c) and e) GDPR, in Art. 2 para. 2 lit. c) the GDPR fully expands to any private data processing if it is not only for personal or household reasons. Even a quick look through the provisions of the GDPR reveals that much of its regulatory impact has changed focus and is now primarily directed towards private actors, for example, the new chapter on certification applies only to the private sector. Many of the recitals make clear that the GDPR focuses on private data processing. For example, contractual situations are often mentioned in which data processing takes place, or in recital No. 85 the specification of potential risks lists situations which typically occur in the private sector.

Nevertheless, the GDPR continues to address State data processing as well, and the parallel passing of the Directive for the purposes of prevention, investigation, detection, etc.[28] clarifies that the GDPR enacts more than just a simple legal act of the EU but rather is a building block of a digital strategy in which data protection plays an important role—addressing both the Member States and private entities.

Therefore, the attention of data protection law has more clearly integrated data protection against private and state actors; digital globality has taken the EU to a different understanding which has led to a more focused regulatory regime towards private entities without lowering the measures against state actors.

27 Cf Spiros Simitis/Hornung/Spiecker (n 9).

28 Directive 2016/680/EC of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, [2016] OJ L 119, 89.

3.1.3 GDPR as Unifier

Recital No. 9 names another reason for the GDPR: It reacts to the consequences of fragmented data protection laws and fragmented enforcement within the EU. While the beginning of the regulation of data processing focused on national approaches and thus individual national law, the DPD addressed a broader audience. It used the interior market clause of Art. 95 of the earlier EC Treaty as an argument to create similar data protection standards in all Member States: The internal market for information (i.e. personal data) should become harmonised. As a number of European States did not have any data protection laws at the time of passing the DPD,[29] this meant the adoption and transfer by those States which already had normative standards for automated decision-making in place and a new regulatory regime for those States which had no standards at all.

Globalisation was, at the time of the passing the DPD, of little importance. The internet did not yet exist in the way we know it today, so data transfer was possible, but with much higher technological hurdles, and also with much less ubiquity in means and addressees as we know today. In 1995, the worldwide acting information companies, mainly with headquarters overseas, were just beginning to develop.

The GDPR, however, recognises changed circumstances. Recital No. 6 explicitly explains that the "scale of the collection and sharing of personal data has increased significantly", and that personal data is now available globally. With this, the GDPR recognises that it has become almost impossible to regulate data processing on a national level and that even regulation on a supranational level encounters difficulties in setting standards and enforcing them. The distribution of data via the internet, internationally available services such as apps, operating systems, hard- and software including the globalised telecommunications infrastructure, and the reliance in many areas of life on mobile services all are intertwined in one interconnected, often (but not necessarily so) interoperable network of information technology. Within this system, data flows frequently and is continuously stored, shared, recombined and altered. A national, even a supranational regulation naturally reaches the limits of control because the different steps of data processing do not necessarily take place within one regulatory regime but are governed by different legal approaches. Consequently, a great uncertainty arises especially among law-abiding controllers regarding which rules are binding for them and which level of data protection they have to guarantee. Often, obligations contradict each other and thus create a choice between Scylla and Charybdis.

In reaction to much of the data processing of European citizens taking place outside the EU, the GDPR enlarges its territorial scope in comparison to the

29 Spiros Simitis/Hornung/Spiecker (n 9) Introduction para 88; Martin Selmayr and Eugen Ehmann (n 10) Introduction para 57; Jochen Schneider, in Jochen Schneider (ed), *Handbuch EDV—Recht* (5th edn, 2017) Dr. Otto Schmidt, A para 46.

DPD. This aspect of the GDPR as a unifier will be discussed later in the chapter on territorial scope (3.3.2). However, the effect goes beyond enlargement of territoriality: Art. 3 para. 2 GDPR also makes clear that the EU considers its legal standard as binding worldwide for every controller. One can also conclude from the standards for data transfer outside the EU that the GDPR is considered to be the gold standard: Although it is sufficient to have an adequate standard of protection under Art. 44 et seq. GDPR for enabling personal data to be processed outside the EU, the CJEU has upheld and fortified its decisions on when adequacy can be assumed in prominently striking down both the so-called Safe Harbor Agreement[30] and the so-called Privacy Shield.[31] Both agreements were the basis of transatlantic data transfer which came to a halt due to these decisions.

As a result of the strengthened self-esteem of EU data protection law, international actors have reacted. From an outsider's viewpoint, the GDPR has a unique selling point in being the most comprehensive and citizen-protecting data protection law so far, offering one of the few tools to create a level playing field in information law. Therefore, it is not surprising that the international interest in the GDPR is big, and that quite a few influential States have taken political action on the basis of the GDPR. Naming the big three—California, Japan and Brazil—which have all passed GDPR-inspired and often look-alike regulations, illustrates this convincingly. Even States with little democratic interest but with highly rated economic interests in doing business with the EU have adjusted, even if only pro forma or only in regard to the private and not the public sector.

In the end, the GDPR so far—and the process is dynamic and not yet finished—has started a global process of raising the awareness of data protection once more. It may even serve as a unifier: Within the EU, this is certainly true, globally, one will have to see.

3.2 Core Regulatory Instrumental Approach

The approach of the GDPR in comparison to that of the first regulatory regimes in data protection law has changed. It has already been pointed out that the regulation of private entities (businesses, etc.) has become an important factor, while State regulation is still prominent but due to the particularities of EU competence law not as prominent. The protection of personality and autonomy as the backbone of democracy is in part now addressed in other regulations, such as

30 Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441) [2000] OJ L 215/7.

31 Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-US Privacy Shield (notified under document C(2016) 4176) [2016] OJ L 207/1.

media law or hate speech regulation. Nevertheless, data protection still remains an important tool to protect these core freedoms.

This chapter will illustrate changes in two core regulatory instruments: It shows that the precautionary principle is in some regards reformulated as a risk-based approach. The GDPR also introduces more openly a consumer protection approach and uses data protection law as a new tool and vehicle for control of fair markets and fair trade.

3.2.1 Precautionary Principle Versus Risk-Based Approach and the Concept of Technological Neutrality

The early data protection legal regimes followed a technology law-based approach (i.e. foremost the precautionary principle but also other instruments such as state control by authorities). They embraced the idea that any type of data protection could cause risks. The statement of the German Constitutional Court in its ground-breaking 1983 census decision is typical of this: "There is no irrelevant data".[32] Consequently, the DPD stated that any type of data processing needed a justification; otherwise, it was considered to be illegal and lack legitimate grounds. This approach has often been described as making use of the standard approach of law-and-order from administrative law, the concept of the principle of prohibition with the reservation of permission:[33] A private activity is forbidden, but the State can allow it on legitimate grounds for particular superior legal interests, among them individual freedoms and liberties.

It should be noted, however, that this interpretation had some flaws from the beginning: First, private entities, which were also addressed by the DPD, act under the principle of freedom. Different from the State, they need no justification for any action but just the opposite: The State has to justify infringement of fundamental rights of private entities which a law-and-order regulatory regime clearly constitutes. Such a principle of prohibition would thus only be easy to establish if it addressed merely the State, as it is bound by the rule of law.[34] Thus, the State needs a legal ground for restrictions of the liberties of citizens (i.e. any infringement of data processing). But for private entities and persons, such a general principle of prohibition requesting a permission from the State authorities would be considered to be an intense interference with their basic freedoms. A pragmatic argument against such an interpretation is also that the DPD never included an active and full procedure for permission. This would have reduced

32 BVerfGE 65, 1 (16, 43).

33 Heinrich Wolff, in Stefan Brink and Heinrich Wolff (eds), *BeckOK Datenschutzrecht* (35th edn, 2020) C.H.Beck, Basics para 18; Heinrich Amadeus Wolff, in Peter Schantz and Heinrich Amadeus Wolff (eds), *Das neue Datenschutzrecht* (1st edn, 2017) C.H.Beck, D para 389; Jan Philipp Albrecht and Florian Jotzo (n 15) 50 para 2; Jürgen Kühling and Johannes Raab, (n 9) Einführung para 52ff.

34 In Germany, Grundgesetz (GG) art 20 sec 3.

data processing activities to a minimum, and neither of the early (and also the present) data protection legal regimes intended this.[35]

True is, however, that the requirement of justification newly enshrined in the DPD turned the general approach to data processing around. Now, private entities and States had to control their activities and *ex ante* perform at least a rough test as to whether their data processing was legal under the DPD and the transposition into law by Member States. As the application of the DPD was broad ("any personal data"), this meant a considerable effort on the part of data processors. This need for preventive measures was enlarged even further by the fact that the DPD did not distinguish between certain types of data processing or grant privileges to particular data processing. Rather, "technological neutrality" was the declared regulatory strategy: The DPD was designed to be applicable to any data processing in general, as the latent possibility of recombination of data poses a continuous threat to any data.[36]

The GDPR in general upholds this approach but it does not embrace it as strictly as did the DPD.[37] Rather, it has included a number of provisions in which it assumes that there are specific types of data processing which can be considered to be riskier than others in regard to the concepts of data protection. Here, a more risk-based approach can be identified, even if it has not been taken over within the GDPR completely.[38] In consequence, there will be a development in the coming years where riskier operations will be controlled and regulated further while other types of data processing will not gain as much attention from controllers and supervisory authorities.

One of these provisions illustrating the additional risk-based approach can be found in Art. 35 GDPR, the so-called "data protection impact assessment".[39] Article 35 introduces an instrument for early warning,[40] by which the controller is required to assess the riskiness of a data processing and consequently proactively install measures to reduce the risks. The controller may also have

35 Cf Alexander Roßnagel, in Spiros Simitis/Hornung/Spiecker (n 9) art 5 para 35ff; different view: Peter Schantz, in Schantz/Wolff (n 33) art 5 para 5; Philipp Kramer, in Martin Eßer and others (eds), *Auernhammer: Datenschutz-Grundverordnung: Bundesdatenschutzgesetzt und Nebengesetze: Kommentar* (7th edn, 2020) Carl Heymanns, art 5 para 10.

36 Gerrit Hornung and Indra Spiecker gen. Döhmann, in Spiros Simitis/Hornung/Spiecker (n 9), Introduction para 242; Jochen Schneider, in Jochen Schneider (ed), *Handbuch EDV—Recht* (5th edn, 2017) Dr. Otto Schmidt, A para 31.

37 Gerrit Hornung and Indra Spiecker gen. Döhmann, in Spiros Simitis and others (n 9) Introduction para 242.

38 Ibid para 242.

39 Moritz Karg, in Spiros Simitis and others (n 9) art 35 para 1; Axel Freiherr von dem Bussche, in Kai-Uwe Plath (ed), *DSGVO BDSG Kommentar* (3rd edn, 2018) Dr. Otto Schmidt, art 35 para 1; Silke Jandt, in Jürgen Kühling and Benedikt Buchner (n 9) art 35 para 1.

40 Moritz Karg, in Spiros Simitis and others (n 9) art 35 para 2; Bertram Raum, in Martin Eßer and others (n 35) art 35 para 2; Mario Martini, in Boris P Paal and Daniel A Pauly (eds), *Datenschutz-Grundverordnung* (3rd edn, 2021) C.H.Beck, art 80 para 1.

to consult the supervisory authorities. Article 35 para. 3 GDPR enumerates a number of data processing types which are per se considered to be of high risk, among them profiling (lit. a)) or data processing in regard to special categories of data (lit. b)). Article 35 para. 4 GDPR also requires that supervisory authorities publish lists of those data processing types which fall under the obligation of undergoing an Art. 35 GDPR risk assessment. The authorities are also enabled by Art. 35 para. 5 GDPR to publish an equivalent list of processing types not considered to be risky in the sense of Art. 35 para. 1 GDPR. These lists do not only specify the obligations of controllers in regard to these listed activities, but also serve as examples for interpretation of other, not listed processing types.

The legal definition of particular risky data processing types, as well as the possibility to define activities as not risky, derogates from the original principle that it is the concise circumstances which produce risks for the liberties and freedoms of individuals, and thus any data processing has to be judged individually. Under Art. 35 GDPR, however, the exact controller, the concise purposes and the specific data processing technology now only matter once the threshold of a risk assessment has been undertaken.

3.2.2 Data Protection Law as Consumer Protection and Fair Competition Law

A change of the core regulatory approach can also be identified in regard to the regulatory regime and the regulatory goals of EU data protection law. The DPD was originally a technology-regulation tool aiming at controlling an emerging technology. It employed the characteristic instruments, the precautionary principle being the most prominent one, establishing an *ex ante* regulatory regime and supervisory authorities among others. Controllers were required to test their data processing activities prior to undertaking them: On a primary level, controllers fell under obligations to restrict their activities. Today, the principle of legality in Art. 5 para. 1 and Art. 6 para. 1 GDPR are at the centre of this understanding.

The DPD did not distinguish between the different groups of actors other than between data controllers (including data processors) and data subjects. Data subjects per se were considered to be caught in informational power asymmetries in comparison to data controllers. The particular circumstances in which these power asymmetries arose were not part of the regulatory design.

This is now different with the GDPR—at least some provisions identify different subgroups of protection-worthy situations. Elements of consumer protection law and competition law have been introduced, most prominently in the provision of Art. 20 GDPR regarding the right to data portability.[41] A majority of current EU directives define the consumer as a "natural person who is acting for

41 Cf Alexander Dix, in Spiros Simitis and others (n 9) art 20 para 1; Hans-Georg Kamann and Martin Braun, in Martin Selmayr and Eugen Ehmann (n 10) art 20 para 3; Tobias Herbst, in Jürgen Kühling and Benedikt Buchner (n 9) art 20 para 4.

the purposes which are outside his trade, business and profession".[42] Consumer protection law addresses a fundamental problem, mostly in contractual circumstances: Consumers find themselves often in situations where they do not bargain from an equal position, especially with large corporations and industries in business transactions. These transactions typically concern their private lives, but they are inherently disadvantaged. Thus, consumer protection law aims at protecting consumers from serious risks and threats that they are unable to tackle as individuals; at empowering them to make choices based on accurate, clear and consistent information; and finally at enhancing their welfare and effectively protecting their safety as well as their economic interests.[43] The EU has a longstanding tradition of protecting consumer interests.

Although the GDPR does not explicitly name the "consumer" as a subgroup of data subjects, the core goals of data protection to counteract informational power asymmetry and of consumer protection law to counteract power asymmetry on the marketplace are naturally closely linked. This holds true even if data protection law does not take economic effects as a starting point as does consumer protection law. Data protection law is thus larger in application as it takes into account effects of informational power asymmetry on any type of decision. Nevertheless, some of the instruments of data protection law can be observed similarly in consumer protection law, especially strengthening organisational control of conditions, assisting consumers/data subjects to make better choices and effectively pursue their rights against unfair practices. It is thus not surprising that supervisory authorities have already identified a connection between data protection and consumer protection prior to enactment of the GDPR.[44]

The new Art. 20 GDPR is the final open link of data protection to consumer protection. It addresses the very special problem of the so-called "lock-in effect", in particular observed with networks and platforms, most prominently with the social networks.[45] The provision establishes a new right for data subjects to request from controllers the receipt of personal data and the transfer of this data to another controller. This right has been criticised as being too narrow

42 Jane Valant, 'Consumer Protection in the EU. Policy Overview' (European Parliament (EPRS), 4 September 2015 <www.europarl.europa.eu/RegData/etudes/IDAN/2015/565904/EPRS_IDA(2015)565904_EN.pdf> accessed 22 May 2021.

43 Ibid 3.

44 Cf for Germany the resolution of the German National Data Protection Conference: 'Entschließung Marktmacht und informationelle Selbstbestimmung, 88. Konferenz der Datenschutzbeauftragten des Bundes und der Länder, 08./09. Oktober 2014' 23ff <www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/88DSK_Marktmacht.html?nn=5217228> accessed 23 May 2021; for the EU art 29-Working Group Guidelines on the Right to Data Portability (2017) WP 242 rev 01, 4.

45 Alexander Dix, in Spiros Simitis and others (n 9) art 20 para 1; Gerrit Hornung, 'Eine Datenschutz-Grundverordnung für Europa? Licht und Schatten im Kommissionsentwurf vom 25.1.2012' (2012) 3 ZD 99, 103; Tobias Herbst, in Jürgen Kühling and Benedikt Buchner (n 9) art 20 para 2.

to really counteract the "lock-in effect" as Art. 20 GDPR does not require interoperability.[46]

Nevertheless, Art. 20 GDPR opens the door to data protection law as a tool to correct dysfunctionalities on the market of information goods and services. The provision thus openly includes instruments of market design which change the rules of business.

The "lock-in effect" creates an obstacle to effective competition; it creates high burdens on market entry. Being a countermeasure, Art. 20 GDPR actively links data protection law to competition law. The discussion of the relation between the two legal regulatory regimes has—at least in Germany and Europe—so far been addressed more from the side of competition law. Most prominently, the issue has been raised by the Federal Cartel Office (Bundeskartellamt), Germany's highest competition authority: In a decision against Facebook, it used data protection law effects as the core argument for a rule against the company's practice of recombining user data from different sources inside and outside the corporate group.[47] Data protection law with its goal of the highest effectiveness of protection of the data subject's rights does not bar additional safeguards from other legal regimes. Recital 146 of the GDPR thus declares that data protection liability exists "without prejudice to any claims for damage deriving from the violation of other rules in Union or Member State law".

The enlargement of the regulatory regime towards additional consumer safeguarding can be identified as a reaction to global digitality: Internationally operating IT companies have enlarged the power asymmetry not only towards data subjects in general, but in consumer relations in particular.

3.3 Content Regulation

Having so far elaborated on the general principles, the regulatory approach and core goals of the GDPR, it is fair to state that new EU data protection law has extended the concepts of data protection under conditions of globality. A further look at particular actions within the individual provisions of the GDPR will show further reactions in detail.

3.3.1 Enforcement Deficit

Among the impulses on the part of the EU to reform the existing data protection regulatory regime was the desire for a better harmonised, if not even unified, legal

46 Alexander Dix, in Spiros Simitis and others (n 9) art 20 para 1; Tobias Herbst, in Jürgen Kühling and Benedikt Buchner (n 9) art 20 para 3.

47 'Bundeskartellamt Prohibits Facebook from Combining User Data from Different Sources' (2019) <www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html;jsessionid=7630FEA430282799A5AF10176B4F668B.1_cid362?nn=3591568> accessed 22 May 2021; BGH GRUR 2020, 1318.

status enforcement of the existing legal status in comparison to the DPD.[48] In the course of time, it had become obvious that, in particular, the enforcement mechanisms provided by the DPD and the transposition into law by Member States were not sufficient to provide for execution of the provisions to effectively protect personal data.[49]

The reasons for this were many. It was unclear which tasks, competences and powers the supervisory authorities had. Some involved parties and States were of the opinion that the DPD did not grant to supervisory authorities the power to enact individual rules and to enforce them; other Member States had established extensive competences and powers. This, but also different traditions, understandings and interpretations, led to diverging assessments and decisions of supervisory authorities in the Member States on similar or even the same data processing types. This created uncertainty and reduced the effectiveness of enforcement. This effect was intensified on an international level due to the effect of "data protection law shopping", especially by large and internationally operating companies in search of a minimally enforcing Member State interpretation of the DPD. In particular, large international information corporations had pushed enforcement through and cooperation between supervisory authorities to the limit. They had designed corporate and technical structures to avoid application of the DPD or only limited data processing being under the regime of the Member State and DPD jurisdiction.

Especially this latter fact is directly linked to the effects of the global digitality: As most of the digitalised services are offered internationally and the most important companies are headquartered outside the EU, any enforcement deficit is also a straightforward result of the globalised, mostly internet-based digitalisation system. It is also directly linked to the applicability of the DPD and Member State data protection law. This will be dealt with next.

In addition to this, violations of the DPD and Member State law were often hardly sanctioned. For example, in Germany, liability for breach of data protection laws was factually non-existent, as German law in general allows recovery only for material damages and thus typically does not grant data subjects effective damages for personality or informational rights' violations. The possibility of levying fines was often restricted in the Member States. Thus, secondary law often had no governing effect to effectively sanction violators.

In reaction to these legal problems, the GDPR takes great efforts in reform in order to provide effective enforcement. The efficiency of supervisory authorities has been strengthened and their competences and powers have been clearly stated in the enumeration of Art. 55 et seq. GDPR. In order to unify the assessment of data processing types, the European Data Protection Board (EDPB) formalised the idea of the Art. 29 Working Group under the DPD. The consistency

48 COM (2010) 609 final (n 25) 4.

49 Cf Moritz Karg, in Stefan Brink and Heinrich Wolff (n 33), art 80 para 6; Eike Michael Frenzel, in Boris P Paal and Daniel A Pauly (n 40).

mechanism, Art. 63 et seq., together with the creation of a leading supervisory authority, establishes a procedure by which binding decisions among the different authorities are made possible and in some instances are even mandatory.

In order to effectively detect data protection violations, the rights of data subjects have been enlarged in comparison to the DPD, and in Art. 12 et seq. GDPR information rights have been described more precisely. Damages, including immaterial damages, are now explicitly addressed in Art. 82 para. 1 GDPR. Also, Art. 80 GDPR newly provides for representation of data subjects in enforcement procedures similar to a representative action.

It should also be noted that enforcement-related obligations are strengthened additionally by the duty to demonstrate legality as stated in the new Art. 24 para. 1 GDPR: This requires every controller to document properly that any processing is performed in accordance with the GDPR. Thus, even potential procedural problems are addressed.

3.3.2 Territorial Scope

One important aspect of the problem of a lack of strict and foreseeable enforcement was the restriction of the mostly territorial scope of data protection law within the EU. The DPD followed a principle of territoriality, that is, any—but also only—data processing taking place within the EU was regulated under EU law. This principle was accompanied by the principle of establishment, that is, any data processing performed in the context of the activities of an establishment in the EU had to act in accordance with the DPD and the transposition into law by Member States.

This, however, proved to be problematic in all cases where data subjects offered their data to controllers outside the EU who did not have an establishment within the EU. Many international controllers had thus created establishments within the EU by which their marketing and business activities were performed, but the core data processing was taking place outside the EU. By this approach, many international companies were able to avoid the regulatory impact of EU data protection law.

The GDPR reacts to this development by forsaking the principle of territoriality in favour of the so-called "marketplace rule", Art. 3 para. 2 GDPR. The marketplace rule makes EU law applicable to anyone offering goods or services to individuals in the EU—regardless of a financial or contractual obligation involved—or monitoring the behaviour of persons within the EU. Thus, neither territoriality nor establishment are mandatory, and thus a material relationship with the EU in processing is no longer necessary.

This change is of particular importance for the effects of global digitality, and this is so for two reasons. The first reason is the obvious one: The GDPR, as opposed to the DPD, now applies to any data processing that addresses natural persons within the EU and thus deviates from the prior principle of territoriality. Now it is no longer necessary to actually prove a data processing within the EU in order to call for protection from the GDPR.

The second aspect revealed by this new Art. 3 para. 2 GDPR is a remarkable development in the handling of digital goods and services. By applying the marketplace principle, the legislator paralleled the application of EU law in regard to virtual goods and services and their effects with non-virtual goods and services. Both now follow the legal regime that anything—material products as well as virtual services—entering the EU are required to adhere to EU standards: A US car must fulfil all requirements of EU product and safety regulations; this is now likewise the case with any online service offered to someone in the EU.

Thus, we can observe a shift on the part of the EU to master not only its own marketplace but to react to international companies having conquered successfully the turf of digital services and goods—an aspect that the EU was not strongly committed to under the DPD.

3.3.3 Enforcement of the Enforcement

The GDPR actively seeks to master the enforcement deficit which had arisen under the DPD. As illustrated, a number of tools have been selected in order to not only formulate material standards but also to assure that these standards are binding and enforced.

However, one aspect the GDPR does not address and thus continues to follow the lead of the DPD is in the "enforcement of the enforcement" (i.e. how to ensure that any type of measure any controller has been obliged to take is actually taken). Also, there is a lack of instruments on how to enforce sanctions of any kind, foremost fines and damages.

Here, the GDPR continues to rely on general legal provisions (i.e. rights of access and information, etc.), in general international and Member State procedural and enforcement law, and the established venues for enforcement (i.e. courts and then enforcement agencies). This means, however, that any of the instruments of the GDPR, which need further enforcement or control, will run into the same difficulties as known in other areas of law, as well. It is international law which governs to what extent internationally operating entities can truly be forced to adhere to rules within the EU.

3.3.4 Internet Regulation

It will only be touched on briefly that the GDPR also does not address the internet and its specific problems with respect to data protection explicitly. Many new regulatory tools are obviously a reaction to the development of the internet and its ubiquity. However, the technology-neutral approach of the Regulation is probably best seen in the refusal to state a specific content regulation.

Just how difficult it is to reach a mutual understanding in this regard is illustrated by the not-concluded debate about a new ePrivacy Regulation, which was meant to provide exactly such internet-specific regulation on the basis of the GDPR. Despite many efforts by several presidencies within the EU, no compromise has been reached thus far. So, the GDPR remains the essence of data

protection without addressing the specificity of internet regulation. Here, global digitality has arrived in theory, but not in practice.

4 Conclusion and Outlook

The conclusion of this first and short analysis, restricted to some general ideas and instruments in EU data protection law, is the following: Data protection law has not turned into a "new" law in the course of increased and of global digitality. Rather, one can observe the field as a dynamic area of law which has adjusted in some parts to developments over the past 30 years and in particular to the increased international operations in information technology. However, sovereignty and international law take its toll: The EU has expanded its substantive law approach and the immediate enforcement of it by several instruments, but not the actual "enforcement of the enforcement". Overall, data protection law remains the most comprehensive information law there is—and the GDPR, following in the footsteps of the DPD, is a powerful tool to regulate digitality also on a global scale. This is true not the least because of its model character, which many States worldwide have started to align with when intensifying their own data protection efforts.

4 Giving the Invisible Hand a Relatively Free Hand

Data Privacy in the US and the Unfortunate, but Lawful, Commodification of the Person

Ronald J. Krotoszynski, Jr.

1 Introduction: The Myriad Cultural and Legal Difficulties of Safeguarding Informational Self-Determination Against Non-Government Actors in the US

Arriving at a truly global consensus on how best to protect personal data will constitute an exceedingly difficult undertaking if the United States is to play a meaningful part in this project to advance global digitality. As this chapter will explain, the reasons for this are both legal and cultural. US law, at the federal level, does not feature strong statutory protection for informational self-determination and offers only limited constitutional protection of confidential personal information. This legal state of affairs, in turn, reflects a broader cultural fact—in the US, most citizens are simply not very concerned about exercising control over their personal information (including how it is collected, stored, and commodified).[1] In Europe, by way of contrast, ordinary people are fiercely concerned about exercising autonomy and control over their personal data—and both politicians and bureaucrats have responded to widespread and deeply seated concerns about informational privacy.[2]

US law does not currently maintain any sort of generalized protection of personal data at the federal level. To the extent that personal data enjoy legal protections at the federal level, these protections are, at best, incomplete and scattershot.[3]

1 See Ronald J. Krotoszynski, Jr, *Privacy Revisited: A Global Perspective on the Right to Be Left Alone* (2016) Oxford University Press, 23–25 (observing that "most U.S. lawyers, judges, and academics, and citizens think of rights almost exclusively as running against the state rather than against non-governmental actors (such as publicly traded corporations)" and noting that "[t]his same phenomenon exists with respect to privacy rights in the United States" meaning that "in the United States, we tend to think of privacy rights running against the state rather than against each other").

2 Ibid 23–24, 150–60.

3 See Daniel J Solove, *The Digital Person: Technology and Privacy in the Information Age* (2004) NYU Press, 67–72 (discussing and describing various federal statutes that protect privacy and personal data).

DOI: 10.4324/9781003283881-7

One could even say that personal data protection in the US resembles a Swiss cheese—because it's full of "holes" or gaps in its coverage. As Professor Daniel Solove, a well-regarded US privacy law scholar, has explained "the federal privacy statutes form a complicated patchwork of regulation with significant gaps and omissions."[4]

Privacy law is also largely reactive rather than proactive in the US.[5] Instead of thinking holistically about what a sensible privacy policy at the national level would require, Congress tends to use its Commerce Clause power[6] to protect privacy in highly specific contexts—often after the absence of data privacy in a particular context, such as with respect to a person's video rental records or driver's license data,[7] enters the national discourse.[8] The result is a mish-mash of policies with little coherence with regard to the subjects regulated or the interrelationship of the laws with each other. What's more, this potpourri approach just is not very effective at securing personal data. As Professor Colin Bennett laments, "[t]here may be a lot of laws, but there is not much protection."[9]

4 Ibid 71. Of equal importance, Solove observes that "many of Congress's privacy statutes are hard to enforce." Ibid. These laws, unlike the GDPR, often do not provide an easy-to-use means of identifying and seeking redress for privacy violations.

5 See Colin J Bennett, 'Convergence Revisited: Toward a Global Policy for the Protection of Personal Data' in Philip E Agre and Marc Rotenburg (eds), *Technology and Privacy: The New Landscape* (1997) The MIT Press, 99, 113 (describing data protection law in the US as "reactive rather than anticipatory, incremental rather than comprehensive, and fragmented rather than coherent").

6 US Const, art I, § 8, cl 3 (providing that "[t]he Congress shall have power. . . . To regulate Commerce with foreign Nations, and among the several States, and with the Indian Tribes").

7 Video Privacy Protection Act 1988, Pub L 100–618, 102 Stat 3195 (codified at 18 USC §§ 2710–2711 (2018)); Driver's Privacy Protection Act 1994, Pub L 103–322, 108 Stat 2099 (codified at 18 USC §§ 2721–2725 (2018)).

8 See Neil Richards, *Intellectual Privacy: Rethinking Civil Liberties in the Digital Age* (2015) 132–33, 167 (noting that after *The Washington City Paper* obtained and published Supreme Court nominee Robert Bork's video rental records during the pendency of his nomination before the Senate "a horrified Congress quickly passed the VPPA, perhaps fearing that disclosure of more interesting film preferences should politicians be targeted next"). The VPPA is colloquially known, in fact, as the "Bork Bill." Ibid 132; see Solove (n 3) 69 ("After reporters obtained Supreme Court Justice nominee Robert Bork's videocassette rental data, Congress passed the Video Privacy Protection Act (VPPA) of 1988, which has become known as the Bork Bill."). Writing in 2004, Professor Solove argues that the VPPA has a very narrow scope of application, Solove (n 3) 132, whereas Richards, writing over a decade later, opines that the federal courts have interpreted the VPPA quite broadly to apply to audio-visual formats beyond VCR videocassette tapes "and to cover not just physical media but also streaming online video services such as hulu.com," Richards (n 8) 133. In a common law system, it should not be surprising that the courts would generalize a narrowly written statute to achieve the broader aims and purposes that Congress had in mind when it enacted the VPPA. See infra text and accompanying notes 90 to 102.

9 Bennett (n 5) 113.

The legal and cultural problems that would need to be overcome in order for the US to participate in the development of a global law of data privacy are even broader and more entrenched than general social indifference to informational self-determination.[10] The US Constitution, which includes a very broadly construed free speech guarantee,[11] would pose a substantial obstacle to the adoption and enforcement of limits on the collection, storage, and use of personal data held by entities such as Facebook, Google, and Twitter.[12] Even if the problems of political economy could be addressed successfully, leading Congress to enact a comprehensive federal privacy law that resembles the EU's General Data Protection Regulation (GDPR),[13] a serious risk would exist that the federal courts would invalidate the new federal law on First Amendment grounds (either completely or in substantial part).

In 2011, in an obscure case involving a Vermont privacy law, the Supreme Court held that restrictions on the sale of physicians' prescribing practices for marketing purposes constituted an unconstitutional content-based speech regulation.[14] In other words, in the US, the collection, storage, and commercial exploitation of personal data constitutes a form of "speech."[15] Because of this, privacy regulations might well be subject to very demanding judicial scrutiny—"strict scrutiny"—and could be held unconstitutional because the law unduly limits the

10 See ibid 113–14 (noting the difficulty of securing comprehensive federal privacy legislation in the US and observing that it would be quite easy to imagine a world in which "there could very well be data-protection legislation in every advanced industrial country (and some others besides) with the exception of the United States").

11 US Const, amend I ("Congress shall make no law . . . abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances").

12 The Supreme Court has held that the First Amendment's Free Speech Clause protects intentionally false speech. *US v Alvarez* 567 US 709 (2012). It also has held violent video games, sold to minors, constitutes a form of protected "speech." *Brown v Entm't Merchs Ass'n* 564 US 786 (2010). So too, speech that is intentionally offensive and targeted to impose grave emotional harm enjoys robust First Amendment protection, *Snyder v Phelps* 562 US 443 (2011), as does an outrageous parody intended to embarrass, shame, and humiliate its subject, *Hustler Magazine, Inc v Falwell* 485 US 46 (1988). In Germany, the outcome of all of these cases would likely have been quite different, notwithstanding the Basic Law's express protection of free speech. See Ronald J. Krotoszynski, Jr, *The First Amendment in Cross-Cultural Perspective: A Comparative Legal Analysis of the Freedom of Speech* (2006) 112–14 (discussing the Federal Constitutional Court's ruling and reasoning in the *Strauss Caricature Case*, which held that Article 5 of Germany's Basic Law did not convey constitutional protection on a satirical cartoon of Bavaria's governor, Strauss, as a rutting pig having sex with local judges).

13 Council Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (2016) OJ L119/1 [hereinafter GDPR].

14 *Sorrell v IMS Health Inc* 564 US 552 (2011).

15 See Jane Bambauer, 'Is Data Speech?' (2014) 66 Stan L Rev 57, 60–63, 70–83.

freedom of speech by prohibiting data miners from "speaking" (i.e. redistributing the data that they collect and store).[16]

Of course, the US is, like Germany, a federal state.[17] State governments have a general police power to regulate to protect the health, safety, welfare, and morals of their residents.[18] This general police power could encompass the adoption, at the state level, of comprehensive privacy protections. To date, however, only one state, California, has adopted a state law that has a comparable scope of coverage to the GDPR.[19] California has often served as a national leader—for example on addressing air pollution.[20] Because of this, we might expect to see other states follow California's lead and adopt comprehensive data protection laws. This approach, however, also will result in a law of personal data protection that resembles a Swiss cheese—it will be full of holes—but for different reasons than those that explain why current federal privacy laws and regulations constitute an incoherent patchwork.

State laws would govern data protection only within the state's own territory; privacy rights would vary widely as one crosses a state line. Moreover, the

16 See Ashutosh Bhagwat, 'Sorrell v. IMS Health: Details, Detailing, and the Death of Privacy' (2012) 36 Vt L Rev 855, 856, 868–74. Professor Bhagwat describes the implications of the Supreme Court's holding in *Sorrell* for comprehensive privacy protections in the US as "dramatic and troubling." Ibid 856.

17 See US Const amend X ("The powers not delegated to the United States by the Constitution, nor prohibited by it to the States, are reserved to the States respectively, or to the people").

18 Bernard Schwartz, *A Commentary on the Constitution of the United States: The Rights of Property* (1963) Macmillian, 44–47 (observing that the Constitution leaves the police power with the states, rather than the federal government, although the federal government's enumerated powers authorize it to adopt federal laws to promote police power objectives); see *Hamilton v Kentucky Distilleries & Warehouse Co* 251 US 146, 156 (1919):

> That the United States lacks the police power, and that this was reserved to the States by the Tenth Amendment, is true. But it is none the less true that when the United States exerts any of the powers conferred upon it by the Constitution, no valid objection can be based upon the fact that such exercise may be attended by the same incidents which attend the exercise by a State of its police power, or that it may tend to accomplish a similar purpose.

19 California Consumer Privacy Act 2018, Cal Civ Code §§ 1798.100ff [hereinafter CCPA]. The state legislature enacted the CCPA in 2018 and its provisions entered into force on January 1, 2020. For an overview of the CCPA and a history of its enactment, see Russell Spivak, 'Too Big a Fish in the Digital Pond?: The California Consumer Privacy Act and the Dormant Commerce Clause' (2020) 88 U Cin L Rev 475.

20 See David Vogle, *California Greenin: How the Golden State Became an Environmental Leader* (2018) Princeton University Press, 4 (observing that "[n]o other state has enacted so many innovative, comprehensive, and stringent environmental regulations over such a long period of time"). In fact, "[c]ompared to all other states as well as the federal government, California has been a national leader" in fashioning and enforcing government policies designed to safeguard and protect the environment. Ibid. Professor Vogel posits that California is now playing the role of regulatory pioneer with respect to personal data protection in the US). Ibid.

federal courts generally have held that the states may not apply their regulations on an extraterritorial basis to activity that occurs in another state.[21] Thus, California could not require companies operating even in neighboring states to observe California's privacy rules. So long as any state maintains a privacy law that is less protective than California, businesses that collect, store, and sell personal data will opt to incorporate in those jurisdictions and maintain their servers there.[22] There is also some chance that because the CCPA will affect the practices and rules governing data collection, retention, and transfer so broadly, it might be invalid on federalism grounds for violating the dormant aspect of the Commerce Clause.[23]

Other perfectly legal avenues also exist for dominant social media platforms to undercut the efficacy of a state personal data privacy law—notably including a choice of law clause in a terms of service (TOS) agreement coupled with mandatory arbitration of any disputes arising under the TOS. A service provider could declare that the law of a less-privacy protective state would govern the

21 *Midwest Title Loans, Inc v Mills* 593 F3d 660, 666–69 (7th Cir 2010) (invalidating on dormant Commerce Clause grounds an Indiana state law that attempted to regulate the terms of loans made to Indiana residents both within Indiana and also contracted in other states because "[t]o allow Indiana to apply its law against title loans when its residents transact in a different state that has a different law would be arbitrarily to exalt the public policy of one state over that of another" in violation of the Commerce Clause); see *Healy v The Beer Institute* 491 US 324, 336–37 (1989) (invalidating a Connecticut law that required beer wholesalers to charge Connecticut buyers prices no higher than the prices offered to purchasers in any state bordering Connecticut because "a statute that directly controls commerce occurring wholly outside the boundaries of a State exceeds the inherent limits of the enacting State's authority and is invalid regardless of whether the statute's extraterritorial reach was intended by the legislature" and explaining that "[g]enerally speaking, the Commerce Clause protects against inconsistent legislation arising from the projection of one state regulatory regime into the jurisdiction of another State").

22 Many corporations have corporate charters issued by Delaware because the state has long maintained strongly pro-management corporation laws. So too, many credit card companies are based in South Dakota because South Dakota state law contains very lax consumer protections and empowers credit card companies to adopt and enforce usurious consumer lending terms. Citibank, for example, has chartered its credit card operations in South Dakota because of the state's "unusually lax approach to banking laws." Amy Sullivan, 'How Citibank Made South Dakota the Top State in the U.S. for Business' (*The Atlantic*, 10 July 2013) <www.theatlantic.com/business/archive/2013/07/how-citibank-made-south-dakota-the-top-state-in-the-us-for-business/425661/> accessed 28 October 2020. In fact, over $2.5 trillion in bank assets are located in South Dakota.

23 Spivak (n 19) 478 (noting that because of the CCPA's broad scope and the "tremendous burden" it places on entities that "traffic in data," the law "engenders substantial dormant Commerce Clause concerns"); see Jeff Kosseff, "Ten Reasons Why California's New Data Protection Law is Unworkable, Burdensome, and Possibly Unconstitutional" (*Tech & Marketing Law Blog*, 9 July 2018) <https://perma.cc/629U-JE8P> accessed 28 October 2020 (arguing that the CCPA violates the dormant Commerce Clause because it could force companies that do not wish to comply with this law to refrain from doing business within California or, alternatively, lead to a raft of inconsistent state data privacy regulations that unduly burden interstate commerce in personal data).

use of its service—and under the Federal Arbitration Act,[24] require that any disputes be subject to arbitration, rather than civil litigation. A choice of law clause coupled with arbitration could effectively nullify a state privacy law (such as California's)—much as these provisions effectively nullify many state civil rights and labor laws.

Even with respect to state laws that effectively protect personal data within the state's borders, the federal Constitution, and the First Amendment, will limit the ability of state governments to restrict what entities who collect, analyze, mine, and manipulate personal data do with it. Because data collection, storage, and manipulation all constitute "speech" for purposes of the First Amendment,[25] a state law that limits or prohibits the collection and use of personal data will potentially be subject to a serious constitutional challenge.

In sum, a general culture that seems largely indifferent to personal data privacy with respect to non-governmental entities, combined with a legal system that has stacked the deck in favor of data collectors, will make it very difficult for the US to adopt and enforce global legal privacy standards—at least if those standards resemble those set forth in the GDPR. This is not to say that personal data goes entirely unprotected in the US. The US is not without any federal protections of personal data.[26] Some very specific federal laws confer relatively narrow statutory protection on specific kinds of data, such as an individual's personal credit information (Fair Credit Reporting Act),[27] medical history (Health Insurance Portability

24 Federal Arbitration Act, Pub L 68–401, 43 Stat 883 (codified as amended at 9 USC §§ 1–16 (2018)). The Supreme Court has held that judicial review of arbitral awards is exceedingly modest and that neither federal nor state courts may expand the grounds on which to review and overturn an arbitral award. See *Hall Street Associates, LLC v Mattel, Inc* 552 US 576 (2008). Even if an arbitration panel arguably failed to apply governing law properly, the award will generally stand if challenged in federal court. What is more, in the United States, arbitration panels often simply issue decisions without detailed statements of reasons—which makes ascertaining the precise basis for the panel's decision difficult, if not impossible to review on the merits.

25 See Bambauer (n 15) 60–63, 70–83 (arguing that existing Supreme Court precedents protect "knowledge creation" activities under the First Amendment and positing that data collection, processing, and manipulation all constitute this kind of speech activity and accordingly merit, and will likely receive, robust protection under the First Amendment); see also Bhagwat (n 16) 867 (positing that "[u]nder current law, the sale of specific information, including prescriber-identifying information, constitutes speech fully protected by the First Amendment" and "for a restriction on the disclosure of data to survive a constitutional challenge, it must survive strict scrutiny"). In fact, well-regarded free speech scholars also have theorized that the federal courts will deem algorithmic programs to be "speakers" for purposes of the First Amendment and proceed to afford their "speech" strong First Amendment protection. Toni M Massaro and Helen Norton, 'Siri-iously: Free Speech Rights and Artificial Intelligence' (2016) 110 Nw U L Rev 1169. From this vantage point, when Google produces search results, Google is "speaking" and the program's speech (the search results) could enjoy the same First Amendment protection as a nominating speech at a state political party convention.

26 Solove (n 3) 67–72.

27 15 USC § 1681ff (2018).

and Accountability Act),[28] and student records (Family Educational Rights and Privacy Act).[29] Indeed, a federal law called the Video Privacy Protection Act of 1988 (VIPPA)[30] requires companies that rent VCR tapes (if any still exist) and DVDs to treat records related to such borrowing as confidential and prohibits releasing such records to third parties without the express consent of the person to whom the records relate. Although written with a very specific 1980s-era technology in mind—video cassette tapes—the federal courts have interpreted the VPPA creatively and expansively to reach new formats for distributing audio-visual content (including rental records for streaming services such as Netflix and Hulu, but perhaps oddly still excluding old-fashioned physical books).[31]

It would be quite fair, and entirely accurate, to describe federal data privacy regulation in the US as something of a patchwork.[32] Legal protections exist with respect to very specific kinds of personal data; comprehensive personal data protection regulations simply do not. Accordingly, the existence of general privacy laws in some states (notably including California) should not be taken as evidence that most residents of the US enjoy comprehensive personal data protection comparable to the protection afforded under the GDPR. In fact, notwithstanding some states adopting comprehensive privacy regulations that limit the collection and redistribution of personal data, the current overall picture at the federal level of government is bleak and the prospects for serious reform highly uncertain.

2 The First Amendment Will Make Comprehensive Personal Data Protection Laws Difficult to Enact and Enforce

Privacy and speech exist in some tension with each other.[33] To the extent that privacy laws limit or proscribe the dissemination of information, they impede the exercise of freedom of speech (as well as freedom of the press).[34] More than any other jurisdiction, the United States conveys broad and deep protection on the freedom of speech. It also bears noting that the federal courts define speech with extraordinary breadth to include the collection, storage, and transfer of data.[35] A speaker's motive for disseminating information does not generally affect its protected status;[36] a bad motive, such as causing embarrassment or humiliation,

28 42 USC 1320d-6 (2020).
29 20 USC §§ 1232g (2018).
30 18 USC §§ 2710–2711 (2020).
31 Richards (n 8) 133.
32 Solove (n 3) 67 (noting that "Congress has passed a series of statutes narrowly tailored to specific privacy problems" but never "a general directive for providing for comprehensive privacy protection"); see Bennett (n 5) 113 (observing that "[t]here may be a lot of laws, but there is not much protection").
33 Krotoszynski (n 1) 182–88.
34 Ibid 1, 173–75.
35 *Sorrell v IMS Health, Inc* (n 14) 563–71.
36 *Hustler Magazine, Inc v Falwell* (n 12) 53–54.

will not render the socially transgressive speech unprotected.[37] Indeed, even intentionally false speech enjoys robust protection under the First Amendment.[38]

The Supreme Court of the United States has held that the use of data —including gathering, storing, and manipulating data—constitutes a form of "speech" for purposes of applying the First Amendment. With respect to any data that relates to a public official, a public figure, or a matter of public concern a privacy law would be subject to judicial invalidation because it burdens "speech" related to the process of democratic deliberation. Whether adopted by the federal or a state government, data privacy protections would have to be viewpoint and content neutral and otherwise very narrowly drawn to avoid violating the freedom of speech (which, in the United States, unlike most of the wider world, includes surprisingly robust protection for commercial speech).[39] Accordingly, the First Amendment will seriously complicate any efforts to harmonize privacy regulations in the US with those in the EU and elsewhere.

Constitutional constraints on information privacy laws that do not implicate public officials, public figures, or matters of public concern exist—but are a function of the Commerce Clause and federalism. Congress may constitutionally regulate any economic or commercial activity that, if aggregated across the national economy, substantially affects interstate commerce. Congress has regulated, for example, the commercial sale of driver's license data[40] and the Supreme Court has upheld this law as applied not only to private parties, but also to state governments that possess and wish to sell driver's license data.[41]

Federal regulatory power, however, is something of a two-edged sword. Under the Constitution's Supremacy Clause,[42] a federal law that regulates particular subject matter will preempt state laws on the same subject. Thus, if Congress were to enact a relatively weak general data privacy law, such a law would likely preempt stricter state law enactments (such as California's CCPA). Even if compliance with both the federal and state law would be theoretically possible, a federal law has

37 Ibid 53 (observing that "in the world of debate about public affairs, many things done with motives that are less than admirable are protected by the First Amendment"); ibid (consistent with this approach, although "a bad motive may be deemed controlling for purposes of tort liability in other areas of the law, we think the First Amendment prohibits such a result in the area of public debate about public figures").

38 *US v Alvarez* (n 12) 718 (holding that [a]bsent from those few categories where the law allows content-based regulation of speech is any general exception to the First Amendment for false statements").

39 *Expressions Hair Design v Schneiderman* 137 S Ct 1144, 1150–51 (2017) (holding that restrictions on advertising surcharges for the use of credit cards constituted a speech, not conduct, regulation that triggered enhanced First Amendment scrutiny); see *Central Hudson Gas & Elec Corp v Pub Serv Comm'n* 447 US 557, 565–66 (1980) (holding commercial speech enjoys robust First Amendment protection and providing a four part test for analyzing the constitutional validity of commercial speech regulations).

40 The Driver's Privacy Protection Act 1994, 18 USC §§ 2721–2725 (2018).

41 *Reno v Condon* 528 US 141, 148–49 (2000).

42 US Const art VI.

preemptive effect if the means it uses differ from those used in the state law.[43] In other words, a conflict in the means used to achieve the same policy objective will lead a reviewing court to find implied conflict preemption of the state law. More specifically, if Congress wanted to preempt California's CCPA, it could do so by enacting a weaker federal privacy law governing personal data privacy.

The First Amendment makes safeguarding personal data more difficult because collecting, storing, and selling data constitutes "speech" in the United States. This does not mean, however, that any and all privacy laws would stand on constitutionally thin ice. The existing limited privacy protections in federal statutory law have not been, and are not likely to be, invalidated on First Amendment grounds. However, were the federal government or a state government to adopt something akin to the right to be forgotten, that requires a search engine to de-index information that comes within the broad scope of "matters of public concern" in the US, such a law would face a high probability of judicial invalidation on First Amendment grounds. On the other hand, however, a law that restricts the collection and redistribution of personal data that does not relate to public officials, public figures, or matters of public concern would not raise the same First Amendment problems.

3 The Patchwork Quilt of Federal Statutory Privacy Protections and the First Amendment

Despite the looming presence of the First Amendment, and a political community that is generally indifferent to informational privacy, a number of federal statutes exist and protect informational privacy in several discrete contexts, including regarding student academic records, medical records, financial and banking records, and, oddly enough, video tape rental records. These statutes avoid constitutional problems because they do not regulate information that relates to a public official, a public figure, or a matter of public concern.[44] When information relates solely to matters of private concern, the First Amendment usually will not present an obstacle to laws that protect the information from disclosure.[45]

The Family Educational Rights and Privacy Act (FERPA) protects student academic records and prevents both public and private educational institutions from disclosing a student's academic records.[46] The law is intended to protect students from unconsented-to disclosure of their educational records. It encompasses both mundane matters such as academic performance (grades) and also disciplinary records (for misconduct or academic dishonesty).[47] Along similar lines, the Health Insurance Portability and Accountability Act of 1996 (HIPPA)

43 *Gade v National Solid Wastes Management Assn* 505 US 88, 98–99 (1992).
44 *Snyder v Phelps* (n 12); *Hustler Magazine, Inc v Falwell* (n 12).
45 *Dun & Bradstreet, Inc v Greenmoss Builders, Inc* 472 US 749 (1985).
46 20 USC § 1232g (2018).
47 Daniel J Solove and Paul M Schwartz, *Information Privacy Law* (2018) 1007–13.

imposes restrictions on the creation, maintenance, and dissemination of personal medical records.[48]

The Fair Credit Report Act of 1970 (FCRA) prohibits the involuntary disclosure of personal financial information—including a person's credit history.[49] Like the GDPR, the FCRA also requires a company that maintains personal financial records to delete or correct erroneous information when such information is brought to the credit reporting agency's attention.[50] The FCRA also contains a "right to be forgotten." After a period of time (generally seven years but ten years in the case of a bankruptcy petition), bad credit history information must be deleted from a person's credit report.[51] This duty to delete true, but dated, adverse credit information includes non-payment of debts and even filing for personal bankruptcy.

Some federal privacy laws are remarkably narrow in their scope and are the product of highly visible breaches of informational privacy that generated public outrage. During Robert Bork's confirmation hearing for a seat on the Supreme Court of the United States, opponents of the nomination obtained Bork's video cassette rental records and put this information on the public record. The Video Privacy Protection Act of 1988[52] represents Congress's response to this event—and protects against the disclosure, without consent, of a person's audio-visual borrowing records. In total, around twenty federal privacy laws are currently on the books,[53] and include provisions of the Cable Communications Policy Act of 1984, the Computer Fraud and Abuse Act of 1986, the Digital Millennium Copyright Act, the Electronic Communications Privacy Act of 1986, and the Privacy Act of 1974.[54]

Each of these laws has the effect of limiting the disclosure of personal information without prior, express consent. Would a First Amendment challenge to one or more of these enactments succeed? Probably not.

The Supreme Court has made clear that the First Amendment limits the legal protection that state law may provide for personal reputation and dignity. Starting with *New York Times Co. v. Sullivan*,[55] the Supreme Court held that the First Amendment protects even false statements about public officials in order to ensure that public debate about matters of public concern is "uninhibited, robust,

48 See Janine Hiller and others, 'Privacy and Security in the Implementation of Health Information Technology' (2011) 17 BU J Sci & Tech 1, 11–18 (providing an excellent overview of HIPPA's privacy protections for personal health information and the administrative regulations implementing them).

49 15 USC §§ 1681–1681x (2018).

50 15 USC § 1681i (2018).

51 Ibid § 1681c.

52 18 USC §§ 2710–2711 (2018).

53 Solove (n 3) 67 ("Since the 1970s, Congress has passed over 20 laws pertaining to privacy.").

54 Krotoszynski (n 1) 17–18; see Solove (n 3) 67–71 (discussing several major federal privacy statutes).

55 376 US 254 (1964).

and wide-open."[56] In a series of subsequent cases, the Justices expanded this rule to cover public figures and even private figures who become enmeshed in matters of public concern.[57] However, despite the Supreme Court steadily expanding the *Sullivan* standard, to encompass privacy torts such as intrusion upon seclusion,[58] it squarely held that both the federal and state governments may protect information that relates solely to matters of private concern from involuntary disclosure.[59]

The key precedent, *Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc.*, involved an erroneous credit report that damaged a company's ability to obtain credit. The publisher, Dun & Bradstreet, claimed that the First Amendment provided a shield against liability for its erroneous, but innocent, reporting on Greenmoss Builders' credit worthiness. The Supreme Court squarely rejected Dun & Bradstreet's claim, observing that "speech on matters of purely private concern is of less First Amendment concern"[60] and, accordingly, "[i]n light of the reduced constitutional value of speech involving no matters of public concern, we hold that the state interest adequately supports awards of presumed and punitive damages—even absent a showing of 'actual malice.'"[61] Thus, if a federal or state law regulates information disclosure where the information does not relate to a public official, a public figure, or a matter of public concern, the First Amendment will not be strongly implicated and the statute should not be judicially invalidated for infringing the rights of speech and press.

The federal laws that protect privacy in specific circumstances relate to personal records rather than to activities such as web surfing habits or purchases on the internet. One could even think of the records as constituting a kind of personal property, with the federal privacy laws conveying ownership, in the form of control, to the person about whom it pertains.[62] What about more general information such as geolocation data or web surfing habits? Could a federal law protect

56 Ibid 270:

> Thus we consider this case against the background of a profound national commitment to the principle that debate on public issues should be uninhibited, robust, and wide-open, and that it may well include vehement, caustic, and sometimes unpleasantly sharp attacks on government and public officials.

57 See, for example, *Philadelphia Newspapers, Inc v Hepps* 475 US 767, 771–79 (1986) (discussing and applying the *New York Times v Sullivan* line of precedents and holding that a plaintiff must prove a defamatory statement is false in order to recover if the statement relates to a public official, public figure, or matter of public concern).

58 *Snyder v Phelps* (n 12).

59 *Dun & Bradstreet, Inc v Greenmoss Builders, Inc* (n 45).

60 Ibid 759.

61 Ibid 761.

62 See Abraham Bell and Gideon Parchomovsky, 'The Privacy Interest in Property' (2019) 167 U Pa L Rev 869, 872–75 (arguing that many important privacy interests are properly understood as property interests and positing that privacy protections would be improved and enhanced if courts were to "reinstate privacy's pride of place in the law of property").

against the involuntary transfer of such information—without the person's affirmative consent?

The *Sorrell* decision, discussed previously, suggests that targeted privacy protections that only limit specific kinds of uses of personal data might raise First Amendment problems. A patient arguably should enjoy control over her physician's prescription data—even if that data is held by a pharmacy or a health insurance company. Yet, the Supreme Court held that a ban on the sale of such information for marketing purposes constituted a content-based restriction of speech that triggered strict judicial scrutiny.[63]

One possible distinction between Vermont's law and the federal privacy enactments is that the Vermont law was highly targeted and protected privacy in a very limited way; the piecemeal federal privacy laws are generally applicable and prohibit disclosure of information to third parties categorically (rather than only for specific speakers or particular purposes). In this sense, then, they are not "speaker-based" because the privacy protection will apply regardless of the person or entity seeking to distribute the information and are not "content-based" because the protection applies regardless of the precise reason that holders of personal data wish to release it to third parties without the prior consent of the persons to whom it relates. On the other hand, however, a privacy law that includes exemptions for law enforcement or medical research purposes would incur an increased risk of judicial invalidation. Simply put, selective protection of privacy interests implicates the First Amendment because *Sorrell* treats selective privacy protection as a form of content discrimination.

4 Constitutional Data Privacy Rights, the State Action Doctrine, and the Scope of Constitutional Rights in the US

Despite the widespread perception that no constitutional right to informational self-determination exists in the US, this is actually not the case. What is more, the Supreme Court of the United States recognized a right to informational privacy even before the German Federal Constitutional Court's (deservedly) famous *Census* Case.[64] As this part will explain, the key difference between the US and Western Europe is not the existence of a constitutionally protected interest in informational self-determination, but rather the scope of that right. In the EU, within the Council of Europe, and in the domestic law of jurisdictions like Germany, the government incurs an obligation not only to respect constitutional rights, including privacy rights, but also a duty to secure these rights more

63 *Sorrell v IMS Health, Inc* (n 14) ("On its face, Vermont's law enacts content- and speaker-based restrictions on the sale, disclosure, and use of prescriber-identifying information. The provision first forbids sale subject to exceptions based in large part on the content of a purchaser's speech.").

64 *Whalen v Roe* 429 US 589 (1977).

generally within society. In the US, by way of contrast, constitutional rights apply only against the government and do not create obligations to regulate non-state actors to secure fundamental rights more broadly within society.

As it happens, a right to informational privacy actually does exist under the US Constitution. The Supreme Court first recognized such an interest in 1977. In *Whalen v. Roe*, the Supreme Court rejected a constitutional challenge to a New York state law, the Controlled Substances Act, that required physicians to report prescriptions for addictive painkillers (for which an illicit market exists) to the New York State Department of Health.[65] The statute imposed information reporting requirements on prescribing physicians and created a program within state government to store, analyze, and track prescriptions for potentially addictive pain killers.[66]

Both physicians and patients objected that New York's collection and storage of this sensitive personal medical information could and would lead to privacy breaches if the state agency failed to store the information properly and ensure its confidentiality. To avoid this possibility, the challengers argued that the state should not be permitted to collect and store this information in the first place. They asserted that the right of privacy that protects reproductive autonomy should be extended to reach confidential personal medical information.

The argument was an entirely plausible one. The Supreme Court recognized a general right of privacy in its landmark 1965 decision in *Griswold v. Connecticut*.[67] *Griswold* invalidated a Connecticut state law that prohibited married couples from seeking, obtaining, and using contraceptives for the purpose of birth control. A few years later, in 1972, the court extended this interest in reproductive autonomy to unmarried couples.[68] Perhaps most famously, in 1973, the Supreme Court extended *Griswold*'s right of privacy to encompass the decision to seek and obtain a non-therapeutic abortion.[69] Accordingly, by 1977, the concept of a constitutional right of privacy, as an aspect of the liberty protected under the Due Process Clauses of the Fifth Amendment[70] and Fourteenth Amendment,[71] was well-grounded in the existing case law.

In *Whalen*, the Justices unanimously rejected the constitutional challenge to the New York state law because it advanced an important government objective (reducing the abuse of prescription pain medicines) and contained adequate safeguards against either accidental or intentional release of the personal medical data

65 Ibid 592–93.
66 Ibid 593–95.
67 381 US 479 (1965).
68 *Eisenstadt v Baird* 405 US 439 (1972).
69 *Roe v Wade* 410 US 113 (1973).
70 US Const amend V (providing that "no person shall . . . be deprived of life, liberty, or property, without due process of law").
71 Ibid amend XIV (providing that no state shall "deprive any person of life, liberty, or property, without due process of law").

(the records were stored securely and access to these records strictly limited).[72] Nevertheless, Justice John Paul Stevens, writing for the court, acknowledged that the Constitution protects a privacy interest in personal medical records. He emphasized that "[w]e are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files."[73] He explained, however, "[r]ecognizing that in some circumstances that duty arguably has its roots in the Constitution, nevertheless New York's statutory scheme, and its implementing administrative procedures, evidence a proper concern with, and protection of, the individual's interest in privacy."[74]

Thus, a constitutional privacy interest in avoiding unwarranted disclosure of personal data exists under the US Constitution—but provided that a government program that collects and stores data has a legitimate purpose, and has sufficient substantive and procedural safeguards in place to avoid unwarranted disclosures of the personal data, the government's data collection program is constitutional. Subsequent cases, notably including *NASA v. Nelson*,[75] which the Supreme Court decided in 2011, have affirmed the general principle that when the government possesses confidential personal information, sufficient safeguards must exist to protect against its involuntary disclosure to third parties.[76] Thus, US law mirrors that of the CJEU under decisions such as *Digital Rights Ireland*[77] and *Tele2Sverge*.[78] It is certainly true that the Supreme Court has not yet invalidated a federal or state law because it violates a person's interest in informational privacy, but the government must ensure that when it collects and stores confidential personal data, disclosure of the data can occur only to advance legitimate government purposes, and these records must be securely maintained with access strictly and carefully controlled to avoid unwarranted disclosures.

Given that a constitutional right of informational privacy exists in the United States, one might then ask why no general federal privacy law exists. In Western Europe, governments have a duty not only to refrain from violating constitutional

72 *Whalen v Roe* (n 64) 604–05.
73 Ibid 605.
74 Ibid.
75 562 US 134 (2011).
76 See ibid 138:

> We assume, without deciding, that the Constitution protects a privacy right of the sort mentioned in *Whalen* and *Nixon*. We hold, however, that the challenged portions of the Government's background check do not violate this right in the present case.

77 Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Others v Minister for Communications, Marine and Natural Resources* (CJEU, 8 April 2014).
78 Joined Cases C-203/15 *Tele2 Sverige AB v Post-och telestyrelsen* and C-698/15 *Secretary of State for the Home Department v Watson* (CJEU, 21 December 2016).

rights, such as Articles 7[79] and 8[80] of the European Charter and Article 8 of the European Convention,[81] but also a general duty to secure these interests more broadly within society.[82] This duty to safeguard fundamental rights against private abridgements means that in Europe, governments have an affirmative obligation to enact and enforce data privacy laws that constrain non-governmental actors (including other persons and corporations).

In the US, however, constitutional rights only run against the state itself—not against non-government entities.[83] Under the state action doctrine, constitutional rights will apply to private entities only when they meet one of four tests for "state action."[84] The doctrine of secondary effect, or Drittwirkung (the application of constitutional rules to non-governmental entities), is commonplace in the jurisprudence of the CJEU, the ECtHR, and in the domestic jurisprudence of constitutional courts in places like the Federal Republic of Germany—but it has no salience in the US.

In the US, it is possible to challenge private law rules on the theory that the government establishes and enforces these rules, and they must accordingly be consistent with constitutional constraints.[85] However, the Constitution and Bill of Rights have no direct or indirect application to a private company like

79 Charter of the European Union, 2000/C, 364/01, art 7 ("Everyone has the right to respect for his or her private and family life, home and communications.").

80 Ibid art 8(1) (providing that "[e]veryone has the right to the protection of personal data concerning him or her"); ibid 8(2) (providing that personal data "must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law" and stipulating that "[e]veryone has the right of access to data which has been collected concerning him or her, and the right to have it rectified").

81 European Convention for the Protection of Human Rights and Fundamental Freedoms, Rome, 4.XI.1950, art 8 ("Everyone has the right to respect for his private and family life, his home and his correspondence.").

82 *X & Y v Netherlands* (1985) 8 Eur HR Rep 235, 239–40 para 23, 241, para 27, 242, para 30.

83 *National Collegiate Athletic Assn v Tarkanian* 488 US 179, 191–99 (1988) (holding that only state actors are subject to constitutional limitations and concluding that the NCAA is not a state actor).

84 See *Brentwood Academy v Tennessee Secondary Schools Athl Ass'n* 531 US 288 (2001); see also Ronald J. Krotoszynski Jr, 'Back to the Briarpatch: An Argument in Favor of Constitutional Meta-Analysis in State Action Determinations' (1995) 94 Mich L Rev 302.

85 *New York Times v Sullivan* 376 US 254, 265 (1964):

> Although this is a civil lawsuit between private parties, the Alabama courts have applied a state rule of law which petitioners claim to impose invalid restrictions on their constitutional freedoms of speech and press. It matters not that that law has been applied in a civil action and that it is common law only, though supplemented by statute.

In other words, "[t]he test is not the form in which state power has been applied but, whatever the form, whether such power has in fact been exercised." Ibid.

McDonald's or Marriott; the government has no duty to secure constitutional interests broadly within the general society. Thus, despite the Supreme Court's recognition of a privacy interest in confidential personal data against the government itself, no generalized right to informational self-determination, of the sort the Federal Constitutional Court recognized in the *Census* Case[86] or the CJEU in *Google Spain*[87] exists under the US Constitution with respect to non-state actors. For non-government entities to be regulated, Congress would need to enact a statute.

In sum, the US Constitution does protect a right of informational self-determination. This interest is an aspect of the right of privacy and also implicates the First Amendment's protection against compelled speech. However, these rights bind only the state itself and have no direct or indirect application to non-governmental entities. For a right of informational privacy to apply to non-governmental entities, including other persons and corporations, positive legislation, at the federal, state, or local level would have to be enacted. What is more, a legislative body's decision to enact, or not to enact, such laws would be entirely discretionary.

5 Why Does the US Lack Strong, General Personal Data Protections Against Non-Governmental Entities?

Even though constitutional rights do not run against private individuals or entities, and despite the First Amendment making privacy regulation more difficult, it would still be possible for the national government to enact and enforce a more general privacy law than exists at present. The question thus arises: Why doesn't the US have broader protections of personal data that run against companies like Facebook, Google, and Twitter?

Many factors are doubtless at work, but the biggest issue relates to a general lack of concern about personal data protection within contemporary society in the US. US residents are, for the most part, rather indifferent to the collection

86 *Volkszählung [Census Act] Case*, 65 BVerfGE 1, reprinted and translated in part in Donald P Kommers and Russell A Miller, *The Constitutional Jurisprudence of the Federal Republic of Germany* (3rd edn, 2012) Duke University Press Books, 408–11 (recognizing a constitutional right of "informational self-determination" under Articles 1 and 2 of the Basic Law and requiring that the government's collection, storage, and use of an individual's personal data be strictly necessary and used only for self-evidently legitimate government purposes); see *Rasterfahndung [Data-mining] Case*, 115 BVerfGE 320, 349–57, 361–65 (holding unconstitutional so-called "dragnet" surveillance as a method of investigation); see generally Russell A Miller, 'Balancing Security and Liberty in Germany' (2010) 4 J Nat'l Sec L & Pol'y 369, 384–88 (discussing the Federal Constitutional Court's generally skeptical stance toward broad-based government data collection and mining practices).

87 Case C-131/12 *Google Spain v Agencia Española de Protecciόn de Datos* (CJEU, 13 May 2014).

and use of their personal data by private companies[88]—and are so to a degree that most Europeans would likely find shocking, dangerous, or perhaps a bit of both.[89] Moreover, some prominent legal academics in the US have argued that market forces, if allowed to operate freely and work themselves out, will adequately safeguard the individual's interest in data privacy.[90] In the US, many people—including ordinary citizens but also government officials and legal academics—are largely unconcerned about the threat to informational self-determination that social media companies, search engine providers, and other for-profit, private corporations that collect, store, and mine personal data present to privacy.

Part of the problem relates to the common law methodology as a means of addressing legal problems. Although the US, at both the federal and state levels, does rely heavily on statutory enactments, or "codes," a great deal of law reform in the US occurs at the state level on an interstitial basis. All but one US state uses a common law method of rule-making, meaning that the courts have principal responsibility for creating and enforcing civil law rules (meaning the law of contract, property, and tort).

The common law fashions new rules, or modifies existing rules, on a retrospective basis.[91] As litigation moves forward from the trial to the appellate courts, parties may argue that existing legal rules should be applied as they currently exist—or they can argue for the modification or wholesale repeal of existing common law rules. The common law methodology is backward looking, not forward looking.[92] It does not anticipate problems so much as it reacts to them—after they have arisen.[93]

88 Krotoszynski (n 1) 17–18, 22–25.

89 See James Q Whitman, 'Enforcing Civility and Respect: Three Societies' (2000) 109 Yale LJ 1279, 1285, 1344, 1358–59, 1384–87; see also James Q Whitman, 'The Western Cultures of Privacy: Dignity versus Liberty' (2004) 113 Yale LJ 1151, 1159–60 (observing that "Americans and continental Europeans perceive privacy differently" and positing that "when all is said and done, it is impossible to ignore the fact that Americans and Europeans are, as the Americans would put it, coming from different places").

90 See for example Fred H Cate, 'The Changing Face of Privacy Protection in the European Union and the United States' (1999) 33 Ind L Rev 173, 223–25, 231–32. Professor Cate argues that "U.S. government and business leaders should avoid imposing costly new privacy protection merely as a sop to European data protection officials." Ibid 231. Instead, US should continue to rely on "self-governance and open markets." Ibid 232.

91 PS Atiyah and Robert S Summers, *Form and Substance in Anglo-American Law: A Comparative Study of Legal Reasoning, Legal Theory, and Legal Institutions* (1987) Oxford University Press, 1–35, 96–114.

92 Ibid 1150–56; see also Jeffery A Pojanowski, 'Convergence and Divergence in Statutory Interpretation' in Marko Novakovic (ed), *Common Law and Civil Law Today: Convergence and Divergence* (2019) Vernon Press, 60 ("Classical common law reasoning was pragmatic, reactive, and contextual, not abstract, programmatic, and systematic.").

93 See Atiyah and Summers (n 91) 134–46.

The civil law tends to be more forward looking and to attempt to ward off problems before they manifest within society. The Code Napoléon (French Civil Code), the German Civil Code, and even the GDPR are very much forward looking and proactive, rather than backward looking and reactive. In the civil law tradition, legislators, judges, and legal academics work to update the law on an ongoing basis in a way that both anticipates and meets the needs of an evolving society.[94] The objective is not simply to remediate wrongs after they take place—ideally, the civil code will prevent and deter the harms from happening in the first place.

In some respects, the civil law method reflects greater confidence in the ability of government to study problems and reach the correct conclusions.[95] When a legal system adopts rules in advance of social, scientific, or technological change, there is a risk of getting things wrong.[96] A more conservative, interstitial approach should in theory avoid blown calls. On the other hand, however, such an approach comes at a price—sometimes new problems require big picture, systemic thinking—rather than merely tinkering around the edges.

As explained earlier, in the US, at the federal law, personal data protection consists of a series of unrelated statutes, adopted at various points in time, often in response to perceived shortcomings in the existing legal landscape. The US has never created a comprehensive data protection regime that addresses in a systematic and comprehensive way informational self-determination. Instead, as problems have appeared, Congress has taken discrete steps to address those problems—but only those problems.

In thinking about moving toward a regime of global digitality for personal data protection, this difference in forward-looking/backward-looking regulation will present particularly difficult problems. In general, the US approach prefers minimal, reactive regulation and reposes tremendous trust in private market participants to behave responsibly.[97] We know, from almost daily examples of failures to respect personal data privacy, that unregulated private markets in personal data

94 John Henry Merryman and Rogelio Pérez-Perdomo, *The Civil Law Tradition: An Introduction to the Legal Systems of Europe and Latin America* (3rd edn, 2007) Stanford University Press.

95 Ibid 27–31, 62–67 (discussing the process of codification and the role of legal science in the process of codification of the law).

96 Frederick Schauer, 'Giving Reasons' (1995) 47 Stan L Rev 633, 635, 654–58.

97 Cate (n 90) 223–32. As Cate states the proposition, "the United States has historically depended heavily on private industry, private property, and individual self-reliance" to secure privacy values. Ibid 223. He also posits that "[t]he preference for private action and individual responsibility is especially clear when information is involved." Ibid. This kind of heedless faith in private market orderings to safeguard personal data privacy might seem tremendously unwise—perhaps even shocking—to European eyes. Nevertheless, Cate's account of the US approach to information privacy is both fair and accurate.

will not effectively or reliably self-regulate. We also know that individual consumers, faced with monopoly service providers for social media platforms and search engines, lack any meaningful bargaining power with companies like Facebook, Google, Twitter, and YouTube. Despite these well-established facts, the US legal system tends to view very skeptically government interventions in private markets (including information markets). US residents tend to view government with mistrust and repose greater confidence, more reflexively, in private, for-profit corporations.[98]

These larger cultural differences will impede the ability of the US to reach broad agreement with Europe and the rest of the world on appropriate transnational standards regarding the protection of personal data. Quite frankly, it should not be at all surprising that the CJEU has ruled that the US personal data protection standards, reflected in the so-called "Privacy Shield" agreement, are not materially equivalent to European standards, and therefore insufficient to meet the requirements for a legally valid agreement that will permit US companies to collect, store, and trade in the personal data of EU residents.[99]

Like the Safe Harbor agreement that preceded it, the Privacy Shield did nothing to ensure that EU residents' personal data was safe from US government storage and snooping—a situation that the CJEU held to be fundamentally irreconcilable with Articles 7 and 8 of the European Charter.[100] As with an earlier CJEU decision (*Schrems I*) that found the US protections contained in the Safe Harbor agreement to be legally inadequate,[101] *Schrems II* reaffirms that the CJEU will not waive off the right of EU residents to informational self-determination when a company like Facebook or Instagram stores their data in the US (rather than the EU).

The ostensibly equivalent protection to the GDPR under the Privacy Shield agreement involved reliance on a low-level State Department functionary (the "ombudsperson"), who possessed no authority to actually search the relevant

98 See Krotoszynski (n 1) 11–12, 16–18, 22–25, 29 (noting that US citizens seem quite blasé about the risks that private companies present to privacy values but are more concerned about government snooping); see also Ronald J. Krotoszynski Jr, 'Questioning the Value of Dissent and Free Speech More Generally: American Skepticism of Government and the Protection of Free Speech' in Austin Sarat (ed), *Dissenting Voices in American Society* (2012) Cambridge University Press, 213, 215–29 (arguing that pervasive distrust and mistrust of the government helps to explain US free speech law and practice far more effectively than other, purposive theories of the freedom of speech).

99 C-311/18 *Maximilian Schrems v Data Protection Comm'r* (CJEU, 17 July 2020) [hereinafter "Schrems II"].

100 See ibid paras 168–201. Because the US federal government, under the Foreign Intelligence Surveillance Act, enjoys unfettered access to data and communications from persons located outside the United States without adequate procedural or substantive safeguards, the Privacy Shield agreement, which the EU Commission had deemed constitutionally acceptable, was held "incompatible with Article 45(1) of the GDPR, read in the light of art 7, 8 and 47 of the Charter, and is therefore invalid" ibid para 199.

101 Case C-362/14 *Maximilian Schrems v Data Protection Comm'r* (CJEU, 6 October 2015).

intelligence agency databases and no power to require the removal of personal data—or even the ability to restrict US national security agencies' access to it. To find that this mere pantomime of privacy to address violations of EU residents' data privacy in the US provided fully equivalent protection to the GDPR would have required a judicial act of astonishing willful blindness, an entirely implausible legal fiction, or perhaps a large dose of both.[102] The US government engages in broad-based, dragnet surveillance of electronic communications in ways that are completely non-transparent and lack any meaningful judicial oversight. We know this from the very disturbing, yet unaddressed, Edward Snowden revelations.[103]

The Privacy Shield did nothing meaningful to guarantee that personal data pertaining to EU residents would be equally secure in the US as it is within the territory of the EU under the GDPR. The CJEU was entirely correct to reach this conclusion in *Schrems II*. As future *Schrems*-type claims get brought and decided, the weakness and incomplete nature of US personal data protection provisions will become increasingly difficult to simply ignore. US companies seeking to do business in the EU will probably have to adopt protocols and procedures to avoid exporting such data to the US in order to avoid liability under both the GDPR and domestic privacy regimes.

6 Global Digitality, Personal Data Protection, and "The Law of the Horse"

Some years ago, Frank Easterbrook, a former University of Chicago law professor and currently a federal judge serving on the U.S. Court of Appeals for the Seventh Circuit, wrote a highly influential law review article about how technology can precipitate legal change. Titled "Cyberspace and the Law of the Horse,"[104] the article argues that the internet will not present any serious new legal problems or challenges. His principal claim is that any effort to create a specialized legal regime for the internet would, like a hypothetical "law of the horse," be "doomed to be shallow and miss unifying principles."[105] In his view, it would be far better to consider problems presented by cyberspace "in the context of broader rules" involving contract, property, and tort.[106] While the effects of a new technology on existing social, legal, and cultural relationships are working themselves out,

102 But cf Schrems II (n 99) para 197:

> Therefore, the ombudsperson mechanism to which the Privacy Shield Decision refers does not provide any cause of action before a body which offers the persons whose data is transferred to the United States guarantees essentially equivalent to those required by Article 47 of the Charter.

103 Krotoszynski (n 1) 11.

104 Frank H Easterbrook, 'Cyberspace and the Law of the Horse' (1996) U Chi Legal F 207.

105 Ibid.

106 Ibid.

it would be best to do "nothing" because "[i]f you don't know what's best, let people make their own arrangements."[107] In the alternative, Easterbrook argues that it usually will be most prudent simply to "keep doing what you have been doing."[108]

Almost a quarter century later, it's become reasonably clear that the internet in fact does create problems that require targeted legal responses. Today, information crosses national boundaries instantly—literally at the speed of light over fiberoptic cables—and the instant information transfers create serious social effects in places far removed from the source of the information.[109] To frame the problem in law and economics terms, transnational information flows create externalities that impose costs on persons in jurisdictions far removed from the servers that house stored information. And, when the dissemination of this information causes harms within a jurisdiction, regulators will seek to address those harms.[110] Just as problems like pollution and carbon emissions require a globalized approach, social harms caused by the collection and redistribution of personal data require a transnational approach in order to be effective.[111] There is a clear need for global digitality—even if the prospects for arriving at a common position on how to reconcile informational privacy and speech are highly uncertain.

The conflict of laws issues associated with informational privacy are profound and exponentially greater than the intellectual property law issues that motivated Judge Easterbrook to write his "Law of the Horse" essay. Even if differences in intellectual property rights exist across domestic legal systems, these are almost invariably differences of scope rather than kind. When a work of art or literature should enter the public domain is a matter about which reasonable minds can and will differ. But, the notion that an author should possess a protected property interest in her work is not something that almost any industrialized democracy would reject completely.

Control over personal information, however, is qualitatively different. In the US, the legal system rejects, almost categorically, the idea that the press should be prohibited from disseminating truthful but embarrassing information about

107 Ibid 210.

108 Ibid.

109 *Google Inc v Equustek Solutions Inc* [2017] 1 SCR 824, para 41 (observing that "[t]he Internet has no borders—its natural habitat is global" and, accordingly, effective enforcement of domestic rights requires the use of global injunctions that "apply where Google operates—globally").

110 See Ronald J. Krotoszynski Jr, 'Privacy, Remedies, and Comity: The Emerging Problem of Global Injunctions and Some Preliminary Thoughts on How Best to Address It' in András Koltay and Paul Wragg (eds), *Comparative Privacy and Defamation* (2020) Edward Elgar, 307–14, 323–27.

111 *Google Inc v Equustek Solutions Inc* (n 109); see also Krotoszynski (n 110) 307–12, 323–28 (discussing in some detail the serious problem that global injunctions will present if the EU or Member States attempt to enforce their domestic privacy regulations on an extraterritorial basis in the US).

public officials, public figures, and persons involved in matters of public concern. The commitment to unregulated information streams runs strong and deep.[112] What is more, the press may usually decide for itself whether particular information constitutes a "matter of public concern."[113] Unlike in Europe, neither legislatures nor courts possess much discretion to decide that truthful information about a public official or public figure is not relevant to public discourse.

Accordingly, something like the right to be forgotten (RTBF), which the CJEU first recognized in *Google Spain*[114] and which the GDPR now codifies,[115] is unknown in the US. And, as explained earlier,[116] the First Amendment would present an insurmountable obstacle against the government prohibiting the disclosure of truthful, but embarrassing, personal information if the subject is a public official, public figure, or if the information at issue relates to a matter of public concern.

Despite US resistance to joining the global data privacy bandwagon, it seems reasonably clear that a global consensus in favor of stricter limits on the collection and distribution of personal data is emerging. The GDPR enshrines not only the RTBF, but also establishes concrete limits on the collection and use of personal data more generally. Moreover, the CJEU has held that, in its current form, the GDPR does not have extraterritorial effect.[117] Some similar protections could be enacted in the United States—but would have to be very carefully drawn to avoid running into First Amendment difficulties.

For example, a more limited form of the RTBF already exists in the context of credit reporting personal data under the FCRA.[118] Even so, a generalized legal obligation on the part of a search engine provider to de-index embarrassing but

112 Krotoszynski (n 1) 27–30, 33–36, 146–48, 171–72.

113 *Snyder v Phelps* (n 12); see Robert C Post, 'The Constitutional Concept of Public Discourse: Outrageous Opinion, Democratic Deliberation, and Hustler Magazine v Falwell' (1990) 103 Harv L Rev 601, 668–80 (detailing the federal courts' aversion to defining "matter of public concern" and positing that democratic discourse arguably requires that the concept be defined by speakers rather than courts, legislatures, or civil law juries).

114 *Google Spain* (n 87) paras 89–94, 98–99.

115 GDPR, art 17 (codifying the right to erasure, or RTBF, by vesting the subject of data with "the right to obtain from the controller the erasure of personal data concerning him or her without undue delay").

116 See supra text and accompanying notes 44 to 63.

117 See Case C-507/17 *Google LLC v CNIL* [2019] ECLI:EU:C:2019:772, paras 57–58, 61–66. The Court of Justice was very clear, however, that the EU could enforce the RTBF on an extraterritorial basis if it wished to do so. See ibid paras 57–58.

118 15 USC § 1681i (2018), providing that

> if the completeness or accuracy of any item of information contained in a consumer's file at a consumer reporting agency is disputed by the consumer and the consumer notifies the agency directly, or indirectly through a reseller, of such dispute, the agency shall, free of charge, conduct a reasonable reinvestigation to determine whether the disputed information is inaccurate and record the current status of the disputed information, or delete the item from the file.

truthful personal information would likely be invalidated on free speech grounds in the US. The information at issue in *Google Spain*, for example, would clearly constitute a matter of public concern and the government could not constitutionally proscribe its publication.[119] Any sort of official legal proceeding, including the involuntary sale of personal property to satisfy a tax debt, would squarely count as a matter of public concern in the US.[120]

We are likely to see increasing pressure from the EU and other privacy-protective jurisdictions on the US to better secure rights of informational privacy. The RTBF provides a good example of why such a trend will almost certainly take hold. If information is available anywhere, it's arguably available everywhere.[121] A de-indexing order limited to sites using a particular geographic domain name, such as .fr, .de, or .es, means that the information will be readily available if someone searching for it simply uses a foreign version of Google or Bing (for example, google.com). It is true enough, of course, that in the Google case involving the French privacy regulatory agency (CNIL), the CJEU has held that the GDPR does not authorize the issuance of global injunctions requiring worldwide de-indexing of search engine results.[122] However, the CJEU decision was a narrow and technical one.[123]

Thus, as presently written, the GDPR does not have extraterritorial effect beyond the borders of the EU's Member States.[124] At the same time, however, the CJEU clearly held that if the EU wishes to authorize global injunctions to enforce the RTBF, it has the competence to adopt such a regulation.[125] Were the EU to amend the GDPR in the future to expressly authorize global de-indexing

119 Krotoszynski (n 1) 171 ("*Google Spain*, to U.S. eyes at least, represents a disturbing elevation of privacy rights over the ability of would-be listeners and viewers to obtain true, nonmisleading information"); Krotoszynski (n 110) 326 ("Recognition of a general RTBF in the US would be constitutionally dubious on First Amendment grounds, and likely legally impossible. Under existing First Amendment jurisprudence, the same is the case for recognising and enforcing foreign judgments enforcing the RTBF."). What is more, from a US perspective, "[t]he implications of this doctrine for speech related to democratic self-government are plainly bad." Krotoszynski (n 1) 171.

120 See, for example, *Florida Star v BJF*, 491 US 524, 532–40 (1989) (holding that, under the First Amendment, a newspaper may publish the name of a rape victim despite a Florida state law that prohibited publishing the names of victims of sexual crimes).

121 *Google v Equustek* (n 109) paras 41–42, 44–46; see Krotoszynski (n 110) 319–26 (discussing the *Equustek* decision and the need for global injunctions to fully protect and secure the RTBF but also noting the RTBF's fundamental incompatibility with US constitutional free speech principles).

122 *Google v NCIL* (n 117) paras 61–66.

123 Ibid paras 57–58, 72.

124 Ibid paras 58, 61–73; see Krotoszynski (n 110) 311–12:

> Instead of issuing a broad ruling, the CJEU issued a very narrow decision that holds that art 17 of the GDPR, which secures the RTBF, does not have extraterritorial effect. In consequence, a de-indexing order to secure the RTBF must be limited to the member states of the EU.

125 *Google v NCIL* (n 117) 57–58, 62–68, 71.

orders, the CJEU would almost certainly uphold the revised regulation as a proportionate and necessary means to secure personal data (as well as privacy and human dignity more generally).[126] At that point, the conflict between European data privacy law, on the one hand, and US free speech law, on the other, would become quite problematic. Any business seeking to do business in both the EU and the US would face a Hobson's choice: De-index materials that users in the US have a constitutional right to peruse (and risk losing those users to a US search engine that does not maintain a European presence) or limit de-indexing of search results to sites targeting EU users (and risk incurring huge fines and penalties for failing to implement a European privacy regulator's lawful order to scrub the result on a global, or worldwide, basis).

How can we possibly resolve this conflict? To be sure, the CJEU's *Google* decision, which disallowed the French privacy regulator's (CNIL) effort to require Google to implement a French RTBF de-indexing order on a global basis, has put off the day of reckoning until such time as the EU adopts a data protection regulation that expressly possesses extraterritorial effect. However, because search results available anywhere are effectively available everywhere, this conflict of laws problem will have to be addressed at some point in the future. The US has a strong interest in working on a constructive basis to create a global rule that protects the First Amendment interests of US residents—while also respecting the legal privacy interests of EU residents.

In this sense, global digitality is both possible and necessary. Even if agreement on the substantive rules governing personal data protection are not possible because of strongly conflicting constitutional priorities—privacy in Europe and free speech in the US—it might be possible to agree on when a sovereign state may legitimately and lawfully regulate the collection, storage, and use of data being maintained abroad. The US would certainly have an important stake in determining when US companies must make data available to foreign governments or businesses. The rules governing extraterritorial application of personal data privacy regulations could be negotiated on a global basis. To do so would also put everyone on fair notice of the rules regarding the behaviors and activities that would potentially trigger the applicability of a particular nation's privacy regulations. This approach would be vastly superior to a self-help regime—a kind of digital "Wild West" in which national governments enact competing, overlapping, and contradictory data privacy rules.

In fact, the problem may not come to a point of impasse based on European privacy regulations, but rather from content regulations adopted by a nation like China or Turkey. One could easily imagine China attempting to impose global de-indexing orders for content that the Communist Party of China deems inimical to its domestic political interests. Access to the Chinese market could be used as

126 See ibid para 71 ("EU law does not currently require that the de-referencing granted concern all versions of the search engine in question, it also does not prohibit such a practice.").

leverage for forcing US-based companies to censor search engine results not only in China, but in the US as well. It also bears noting that the CJEU and ECtHR have both made clear that information in which a legitimate public interest exists is not subject to de-indexing. The scope of a matter of public interest is, to be sure, more circumscribed in the jurisprudence of the CJEU and ECtHR than in the jurisprudence of the Supreme Court of the United States, but there is a shared human rights commitment to respecting freedom of speech in order to facilitate the process of collective deliberation that is essential to making democratic self-government work.[127] The difference relates to the degree to which the press may define for itself, as it wishes, the concept of publication in the public interest.[128]

By way of contrast, China's government has no similar commitment to an open and vibrant political marketplace of ideas. China will seek to censor content as a means of exerting comprehensive social control over its residents. In this sense, then, European governments should be careful what they wish for. It may be that if Brussels embraces global de-indexing orders on a unilateral basis that Beijing's autocratic government will be the primary beneficiary. Rather than protecting European citizens from the re-publication of embarrassing information on US websites, it might well be the case that both American and European citizens alike find it harder to access truthful information that clearly relates to matters of public interest.

7 Conclusion

From a US perspective, significant substantive differences in the scope of data protection law between the US approach and the European approach will make global digitality, or harmonization, a very difficult undertaking. Some of these substantive differences also reflect the relative priority placed on fundamental human rights—to be more precise, on personal honor, reputation, and dignity in Europe, and on the freedom of speech and press in the US. Significant differences in cultural attitudes and values explain these material differences in the objective order of human rights values. In the US, citizens tend to trust the private sector reflexively and mistrust the government; this has led to relatively weak national data privacy standards that secure informational self-determination only on a piecemeal, or patchwork, basis. In addition, this skepticism of the state's power and government interventions in private markets has enabled entities that collect, store, and commodify an individual's personal data to do so largely free and clear of significant legal impediments (save in very circumscribed contexts, such as student educational records or borrowers' records for audio-visual materials).

Because of these fundamental differences in the relative importance and priority of fundamental human rights, reaching a global consensus on the substance of personal data protection law will be a difficult, and perhaps impossible,

127 Krotoszynski (n 1) 156–60.
128 Ibid 271, n 169.

undertaking. On the other hand, however, it might be possible to arrive at agreements regarding the transnational application of domestic or regional privacy rules across national borders. The possibility of agreeing on which sovereign may exercise regulatory authority, rather than on the substance of the regulations themselves, might prove to be a more fruitful enterprise. In conclusion, globality on the ability to impose a regulatory regime could be achieved more readily than globality regarding the regulations themselves.

Part III

Consumer Contract Law

5 The Challenge of Globalized Online Commerce for U.S. Contract and Consumer Law

Christopher G. Bradley

1 Introduction

Online commerce has grown dramatically in the last decade, becoming the primary way that consumers buy goods. The Covid-19 pandemic of 2020–2021 only underscored and accelerated this new reality. Merchants and consumers may interact directly or as mediated through platforms such as eBay or Amazon.

Amazon plays several key roles in modern commerce, all of which have continually increased in importance over the last decade and which provide a useful illustration of the different aspects of modern technology-mediated commerce. In its most familiar role, Amazon acts as the retailer of goods to consumers who purchase from it directly; it also manufacturers some of these goods itself through "Amazon Marketplace," which is completely integrated with its direct sales function. Amazon serves as a platform on which goods are sold by others, with Amazon receiving a significant "cut" of sales—a business that perhaps surprisingly constitutes more than half of its total overall sales.[1] Thus, while Amazon continues to build and stock more warehouses to try to improve the speed and ease of product delivery, the manufacturers and many of the real sellers of goods are far away from the buyer. Finally, through its Amazon Web Services, it acts as host for many online businesses through its cloud services, essentially renting out the right to use its servers and software for customer interaction, data analysis, manufacturing and supply management, and so on. In other words, even online commerce that doesn't itself take place on Amazon's platform often relies on its technology.[2]

1 Marc Bain, 'Amazon's Unruly Third-Party Marketplace Now Sells More Stuff Than Amazon Itself' (*Quartz*, 19 April 2018) (quoting shareholder letter), <https://qz.com/1256651/amazon-marketplace-sold-more-stuff-than-amazon-itself-in-2017/> accessed 1 October 2020.

2 Amazon Web Services controls approximately a third of the market for such services. 'Fourth Quarter Growth in Cloud Services Tops off a Banner Year for Cloud Providers' (*Synergy Research Group*, 5 February 2019) <www.srgresearch.com/articles/fourth-quarter-growth-cloud-services-tops-banner-year-cloud-providers> accessed 1 October 2020. The $10.5 billion in revenues from its cloud operations in the first quarter of 2020 were more than 13% of Amazon's overall earnings. Amazon.com Announces First Quarter Results (*BusinessWire*, 30 April 2020) <www.businesswire.com/news/home/20200430005943/en/Amazon.com-Announces-First-Quarter-Results> accessed 1 October 2020.

DOI: 10.4324/9781003283881-9

Given its central role in so many aspects of ecommerce, it is unsurprising that the fortune of Jeff Bezos, Amazon's founder and CEO, has ballooned to more than $200 billion as his company's stock rose more than 85% through the first three quarters of 2020.[3] While some of the rise of online contracting during the pandemic will recede eventually, much of the increase is likely to endure. Reflecting this expectation, traditional retailers have filed for bankruptcy relief in great numbers, many of them liquidating rather than attempting reorganization.[4]

Online transactions differ from traditional dealings in numerous respects, some of which benefit consumers and others of which do not. Among other changes, consumer transactions now cross national borders more often than before, involve much greater degrees of speed and automation, and rely upon novel forms of market intermediation—and, often, manipulation. New transacting practices call for new forms of regulation, but the law has failed to keep up. Technologies have empowered merchants and platforms to outpace consumers and consumer protection law. Legal protections have become inadequate in light of the realities of common internet-based transacting practices. This is due to an inadequate body of law and a set of regulators who are hindered by stark political, legal, and institutional limitations.

This chapter diagnoses the current inadequacies of the regulation of consumer contracting in the United States, including across borders, and it assesses proposed technological and market solutions, which have been cast as far more promising than their reality supports. It calls for solutions—involving statutory, institutional, and technological change—commensurate with the scope of the actual problems presented by our globalized, digitized world of consumer commerce.

2 A Ragged Patchwork of Consumer Protection Laws, Regulations, and Institutions

Laws and legal institutions protect consumers in numerous ways in their transactions with merchants. Consumer transactions are thought to require special protections for a number of reasons. Merchants are specialized and repeat players, who can take advantage of their expertise to tilt the scales of the transacting process in their favor. They have every opportunity and incentive to develop deep, detailed knowledge of their products, their markets, and their consumers.

3 Michelle Toh, 'Jeff Bezos is Now Worth a Whopping $200 Billion' (*CNN*, 27 August 2020) <www.cnn.com/2020/08/27/tech/jeff-bezos-net-worth-200-billion-intl-hnk/index.html> accessed 1 October 2020.

4 Melissa Repko and Lauren Thomas, 'As Pandemic Stretches on, Retail Bankruptcies Approach Highest Number in a Decade' (*CNBC*, 3 August 2020) <www.cnbc.com/2020/08/03/with-pandemic-retail-bankruptcies-approach-highest-number-in-a-decade.html> accessed 1 October 2020. The transaction costs associated with starting a new retailer suggests that a significant portion of these losses of traditional, brick-and-mortar establishments may be permanent.

Both reputational and market constraints limit their exploitation of their superior position to some degree but do not completely make up for the imbalance.[5] A large body of research in behavioral psychology and economics has provided an increasingly thorough understanding of the distinctive aspects of consumer contracting. In addition, not all consumers are similarly situated. Vulnerable subsets of consumers require greater protection. This might include those with traditionally recognized vulnerabilities such as advanced age or lack of education but also those who lack access to technology, including payment technology.

Understanding the regulation of cross-border online consumer commerce in the United States requires traversing a thicket of different laws and authorities. Most obviously, cross-border consumer contracts are subject to longstanding common-law principles as developed by courts, as well as, in specific areas, statutes such as the Uniform Commercial Code and the Magnuson-Moss Warranty Act. But regulation of numerous aspects of consumer transactions remains subject to non-uniform state law of contract and of consumer protection.[6] Neither federal nor the various bodies of state law have been significantly revisited in light of the changing face of consumer transactions, particularly as mediated by new technologies, though many proposals have been made over the years.[7]

Lacking meaningful legislative guidance, courts have stretched these bodies of state doctrine to cover online transactions. Courts' efforts in this regard have been strained and controversial. For instance, courts have struggled with how to apply traditional notions of consent in the context of adhesion contracts, which often seek to shunt disputes to arbitration or impose restrictions on choice of venue, on class action or other aggregate litigation procedures, and on available remedies.[8] While these problems pre-date the turn to online commerce, it has made them much more pressing, as so many more transactions are governed by lengthy, bespoke terms and conditions imposed by merchants.[9] Traditional defenses such as unconscionability and consumer deception have unclear application when

5 Christopher G. Bradley, 'The Consumer Protection Ecosystem: Law, Norms, and Technology' (2019) 97 Denver L Rev 35.

6 On state laws prohibiting Unfair and Deceptive Acts and Practices (UDAP), see Dee Pridgen, 'The Dynamic Duo of Consumer Protection: State and Private Enforcement of Unfair and Deceptive Trade Practices Laws' (2017) 81 Antitrust L J 911, 912–19.

7 There is a vast and thoughtful literature on the changes that technology should bring to consumer law. Rory Van Loo is the most prolific and influential proponent of such changes. See, for example, 'Helping Buyers Beware: The Need for Supervision of Big Retail' (2015) 163 U Pa L Rev 1311.

8 Part 4 explores recent scholarly controversy over an attempt to "restate" this still evolving body of law. See Adam J Levitin and others, 'The Faulty Foundation of the Draft Restatement of Consumer Contracts' (2019) 36 Yale J Reg 447; Oren Bar-Gill, Omri Ben-Shahar and Florencia Marotta-Wurgler, 'The American Law Institute's Restatement of Consumer Contracts: Reporters' Introduction' (2019) 15 Eur Rev Contract L 91.

9 Dee Pridgen, 'ALI's Proposed Restatement of Consumer Contracts—Perpetuating a Legal Fiction?' (*Consumer Law & Policy Blog*, 8 June 2016) <https://pubcit.typepad.com/clpblog/2016/06/dee-pridgens-important-guest-post-update-on-the-alis-proposed-restatement-of-consumer-contracts-will.html> accessed 1 October 2020.

invoked by consumers who contest terms contained in adhesive, online contracts or in sets of online "policies" that may or may not form part of a contract—most importantly, so-called "privacy policies."[10]

Merchants have become more sophisticated in presenting customized sales interfaces based on particular consumer characteristics. Companies use artificial intelligence and "Big Data" analytics to identify customers who may be more susceptible to a given sales pitch or who may be willing to pay more than the price charged to other customers.[11] Companies even seek to deter certain undesirable customers or impose more restrictive dispute resolution agreements on customers whose profile suggests they may be more likely to file lawsuits, to diminish the likelihood of litigation—or stated differently, to reduce the possibility that there will be accountability for abusive practices.[12]

The pervasiveness of the disagreements over the orientation and the uncertainty of this area of law is exemplified by a remarkable showdown. In May 2019, a long-simmering proposed *Restatement of the Law, Consumer Contracts*, which was drafted, revised, and defended by three accomplished reporters, failed to obtain the approval of the American Law Institute. Part 4 of this chapter discusses this dispute, which aptly illustrates the challenges of consumer transactions at this conflicted moment. The proposed Restatement faced fierce opposition from both consumer advocates *and* advocates in the business community. The controversy centered on several provisions intended to clarify how contract law should apply to online consumer transactions. The reporters' attempts to propose a balanced approach fell short because advocates from both sides feel that an ultimate equilibrium might be more favorable to them; decades after commerce began to turn online, the law remains so unstable that hope for ultimate advantage springs on both sides.

A number of practical features of modern commerce interact with various bodies of law to deny consumers effective remedies for many types of harm.[13] The problem goes well beyond contract doctrine. Products liability law developed as part of U.S. tort law rather than contract, although of course it lies in the backdrop of every transaction. It provides an important set of protections for consumers injured by defects in mass-produced products. Yet it is weakened by the structure of a growing share of online commerce. Platform-based transactions have diminished liability for product defects that are not immediately obvious to a buyer or user of goods. Platforms like Amazon have sought to evade liability

10 Lauren E Willis, 'Why Not Privacy by Default?' (2014) 29 Berkeley Tech L J 61.

11 Van Loo (n 7); Ryan Calo, 'Digital Market Manipulation' (2014) 82 Geo Wash L Rev 995, 1015–16; Lauren E Willis, 'Performance-Based Consumer Law' (2015) 82 U Chi L Rev 1309, 1320–21.

12 Yonathan A Arbel and Ray Shapira, 'Theory of the Nudnik: The Future of Consumer Activism and What We Can Do to Stop It' (2020) 74 Vanderbilt L Rev 929, 959–73.

13 Amy J Schmitz, 'Remedy Realities in Business-to-Consumer Contracting' (2016) 58 Ariz L Rev 213.

for products they sell "merely" as a marketplace.[14] Yet the "true" sellers may be difficult to identify, difficult to sue across borders, or "judgment proof" (that is, lacking adequate resources to pay a judgment or easily able to discharge a judgment debt in bankruptcy), leaving injured customers without a remedy.[15] Both legal and reputational factors that protect consumers in more traditional retail interactions are often missing from online transactions. Corporate law, too, plays a role in this; it has made it easier to do business through shell entities with little accountability for ultimate owners or operators. In online transactions, consumers often lack familiarity with a given seller and are less likely to have anything more than one-off contact. Producers and sellers of inferior products may eventually face an accounting, whether being kicked off of platforms or losing business from negative reviews, but these processes take time, and in the gap period, consumers are left very exposed. And of course, a new "storefront" entity can be easily created, potentially starting the whole process over again.[16] That manufacturers and sellers are increasingly on the other side of national borders from consumers brings additional practical and legal restrictions that make it harder for consumers to obtain redress. These practical factors undermine legal protections—the law-in-the-books fails in light of lived realities.

Procedural rules also serve as crucial aspects of consumer protection, and they have increasingly turned against consumers. In addition to the procedural aspects of the laws already mentioned, there are further limits that have become important. Disputes are often shunted to arbitration, where any potential relief will rarely be worth pursuing. Collective remedies such as class actions have become more difficult due to doctrinal changes and the prevalence of anti-class action clauses in adhesion contracts.[17]

Privacy has taken on increasing importance as well. As is now well-known, consumer information is a major component of the consideration received by merchants, and the right to gather and commercially exploit consumer information is a primary non-monetary way in which platforms receive compensation for their

14 Edward J Janger and Aaron D Twerski, 'The Heavy Hand of Amazon: A Seller Not a Neutral Platform' (2020) 14 Brooklyn J Corp Fin & Comm L 259 (noting that most courts have favored Amazon's claim to be a mere marketplace and not a "seller" under tort law; providing a useful overview and powerful critique of these case).

15 Shantal Riley, 'Who's Responsible for Defective Products Sold on Amazon?' (*PBS Frontline*, 11 March 2020) (describing a product liability suit against Amazon in which both the plaintiff "and Amazon were unable to locate the third-party seller to seek damages after the accident" and compiling other similar examples), <www.pbs.org/wgbh/frontline/article/whos-liable-for-defective-products-sold-on-amazon/> accessed 1 October 2020.

16 Eben Novy-Williams and Spencer Soper, 'Nike Pulling Its Products From Amazon in E-Commerce Pivot' (*Bloomberg News*, 12 Nov 2019) ("Nike reportedly struggled to control the Amazon marketplace. Third-party sellers whose listings were removed simply popped up under a different name.") <www.bloomberg.com/news/articles/2019-11-13/nike-will-end-its-pilot-project-selling-products-on-amazon-site> accessed 1 October 2020.

17 Samuel Issacharoff and Florencia Marotta-Wurgler, 'The Hollowed-Out Common Law' (2020) 67 UCLA L Rev 600, 632–35 (discussing "anti-aggregation" law).

role as intermediary.[18] Businesses exploit private consumer information relentlessly.[19] Despite increased attention in recent years, privacy law remains seriously undeveloped in the United States.[20] The absence of consumer-protective privacy law permits merchants aggressively and covertly to extract and use valuable consumer data, imposing largely unrecognized costs on consumers engaging in online commercial activities. Not only are substantive protections lacking, but in addition, courts have imposed limits on standing for consumers whose private information has been compromised.[21] These limits raise litigation costs and risks and prevent consumers from obtaining redress.

These and other bodies of law impact the balance of power between merchants and consumers. Even this picture remains far from complete. There are state and federal consumer protection laws and regulations, often known as UDAP laws, that broadly prohibit unfair or deceptive acts or practices vis-à-vis consumers.[22] Some UDAP-type laws permit private causes of action, but others charge regulators with exclusive power to investigate potential violations and enforce these regulations. Consumers' rights of action are subject to some of the practical and procedural limits discussed earlier; while some UDAP laws provide statutory damages and fee-shifting provisions that facilitate consumers' claims, most do not.

State regulators are generally under-funded and under-staffed.[23] In addition, they remain subject to political pressures and their activities differ dramatically across states.[24] The importance of politics to regulators may make them beholden to businesses within their borders and less responsive to cross-border actors or regulators. In addition, although regulators regularly collaborate across borders, they may in some cases lack the capacity or legal authority to do so effectively.

This Part has painted a picture of the legal landscape for online consumer contracts. The picture is bleak, and it is evident that the problems go far beyond contract and commercial law. However, there is reason for hope as well: Each area surveyed earlier represents not only an area of current weakness but a potential policy lever for consumer advocates, a potential avenue for influence and change. Progress may come in many forms and from many actors—at the global, national, state, or local levels, and from the judicial, executive, and legislative branches.

18 Christopher G. Bradley, 'FinTech's Double Edges' (2018) 93 Chicago-Kent L Rev 61, 63–70 (exploring the example of consumer loan comparison-shopping platform Lending Tree).

19 Willis (n 10).

20 Margot Kaminski, 'A Recent Renaissance in Privacy Law' Comm ACM (September 2020) 24; Ronald J. Krotoszynski, in this volume.

21 For example, in Re Supervalu, Inc, Customer Data Security Breach Litigation, 870 F 3d 763 (8th Cir 2017) (denying standing to customers whose data was stolen but had not actually yet been subjected to fraudulent charges or identity theft).

22 See Pridgen, 'Dynamic Duo' (n 6).

23 Pridgen, 'Dynamic Duo' (n 6) 932 ("State attorney general offices are by nature limited in their resources. They do not and cannot provide access to justice for all consumers who need it.").

24 Prentiss Cox, Amy Widman and Mark Totten, 'Strategies of Public UDAP Enforcement' (2018) 55 Harv J Legis 37.

3 The Limits of Technological Approaches to Consumer Protection

If technological development played a significant role in harming consumer interests, does it also play a role in helping them? Obviously, technology has already brought a degree of aid to consumers: While the perils of online contracting remain underrated, online consumer contracting does present consumers with numerous advantages over traditional purchasing contexts.

Shopping from home is more convenient, private, and relaxed than heading to a brick-and-mortar location and interacting with a live salesperson. In addition, ecommerce can permit easier comparison shopping across a much wider variety of goods, with information including user reviews easy to access. Cost savings may emerge from merchants' not having to maintain physical footprints or hire sales floor staff as well as from the increased competition among providers of goods beyond any specific geographical area. Finally, too, it can broaden access to commerce for those who face location-, transportation-, or health-related limitations. The online world was a boon, for instance, to my late mother, who enjoyed contributing to the family's wellbeing through shopping, and yet who, as a result of primary progressive Multiple Sclerosis, spent more than twenty years with profoundly limited mobility, making it both difficult and uncomfortable to visit physical stores.

In addition, technology has been adapted to address some of the evident inadequacies of consumer law. Some of the largest actors in online commerce have erected their own protections for customers, as they seek to build consumer confidence in new marketplaces, payment systems, and transactional forms. For example, online platforms work to prevent fraud and often provide compensation to defrauded consumers. At considerable expense, they have put infrastructure in place to provide consumers with reliable mechanisms for making payments, which is particularly important given the inadequacies of the antiquated global payments systems. Some of these protections may become entrenched as pro-consumer norms expected of online marketplaces in the future.

Online dispute resolution services are one of the most interesting and promising "products" arising at the intersection of online commerce and consumer protection. Platforms and marketplaces have invested significantly in providing cheap and relatively reliable means of resolving basic disputes between sellers and buyers. Online dispute resolution (ODR) efforts of platforms such as eBay hold promise at resolving a range of disputes, particularly in small-scale consumer transactions, at a price and convenience that makes consumer participation realistic.[25] These tools are simple programs that seek to facilitate resolution by requiring speedy online submission of evidence and explanations by each side and providing a largely automated analysis of many run-of-the-mill disputes,

25 See generally Amy J Schmitz and Colin Rule, *The New Handshake: Online Dispute Resolution and the Future of Consumer Protection* (2017) Amer Bar Assoc; Schmitz (n 13).

such as disputes over conditions of products upon arrival. The programs can also facilitate mediation or arbitration of disputes, although often the determination isn't binding: Parties who choose to bring formal legal action can still do so, although the amounts in controversy rarely support such a step. Dispute resolution services may become an expected part of the service package provided by platforms.

All of these undeniable benefits and promising developments should be duly acknowledged, but it is also true that the shift to online commerce has added costs for consumers and for markets. Many of these relate to aggregation and network effects. Most online commerce is facilitated by a small number of platforms that have provided the reliability and trust that I just sketched out. While online platforms and marketplaces facilitate competition among providers of goods, they exploit their oligopolistic position and reap remarkable profits. Many platform providers impose shockingly high fees on merchants using their platforms, yet their market power permits them to maintain these fee structures.[26] Merchants, particularly small merchants, feel they have no choice. In addition, platform providers' services come with hidden costs. For example, Amazon has been accused of failing to police against counterfeit or stolen goods; it has been accused of using its privileged position to make and sell its own knockoff products and undercut the original sellers of unique goods.[27] Yet many sellers believe they cannot forgo selling products on Amazon. Even a manufacturer with the heft of Nike was unable to convince Amazon to provide sufficient protection from "knock-off" products; ultimately Nike withdrew from making direct sales through Amazon: "Nike reportedly struggled to control the Amazon marketplace. Third-party sellers whose listings were removed simply popped up under a different name. Plus, the official Nike products had fewer reviews, and therefore received worse positioning on the site."[28]

For consumers, too, the funneling of so much commerce through a few crucial providers has significant costs, some obvious and some hidden. For example, marketplaces use customized consumer data in order to push products on them and to price discriminate.[29] They also monetize consumers' private information and data about consumer behavior in numerous ways that are, at a minimum, not well recognized by consumers and might be resisted by many consumers if they understood what was happening and had sufficient opportunity to resist. Internet

26 Karen Weise, 'Prime Power: How Amazon Squeezes the Businesses Behind Its Store' (*NY Times*, 19 December 2019) (describing the numerous financial and other demands Amazon makes of businesses using its platform to sell goods) <www.nytimes.com/2019/12/19/technology/amazon-sellers.html> accessed 1 October 2020.

27 Daisuke Wakabayashi, 'Prime Leverage: How Amazon Wields Power in the Technology World' (*NY Times*, 15 December 2019) <www.nytimes.com/2019/12/15/technology/amazon-aws-cloud-competition.html> accessed 1 October 2020.

28 Novy-Williams and Soper (n 16). "Few other brands possess the kind of muscle Nike has, so it may be harder for them to leave." Ibid.

29 Willis (n 11) 1317–21.

commerce providers emphasize price and convenience but while these may be the most salient points for most consumers, the easily ignored, hidden costs of ecommerce may mean that the deal for consumers isn't so good after all.

As for online dispute resolution (ODR), it provides an important layer of protection but, in its current form, has significant limitations. Existing ODR portals are largely limited to shipping, payment, and initial condition of products. They resolve disputes within their ambit successfully but suffer from sharp limits. Platforms balk when confronted with claims for personal injury or large-escale property injury, such as a residence destroyed by an electrical fire caused by a product defect. An overly narrow focus on contracting and payment should not distract from broader deficiencies of protection with respect to, for instance, products liability, abusive commercial practices, and unlawful financing schemes. What is more, ODR tools permit the central, privileged providers to aggregate more market power. This raises concerns over pricing, lack of consumer access to technology, and ever-increasing concentration of information on consumer behavior in the hands of a few.

Yet more concerning, for-profit use of ODR tools risks creating a privileged class of consumers and disputes for which resolution technologies are readily available, while those without access, or those whose disputes are not resolvable on the platform, are left out. Access to technology increasingly governs access to markets, and some groups remain limited in their ability to access technology.[30] ODR works best, from the perspective of merchants and platforms, with respect to standard disputes that can be quickly resolved, whether on an automated basis or with very little human involvement or management consideration. For-profit providers have little incentive to invest in ODR procedures to resolve disputes that require more customized consideration or decision-making. Disputes not meeting the criteria established by the ODR provider will be left for the courts or for arbitration, and in reality, many such claims will never be brought, no matter what their importance as a matter of public policy.[31] Businesses will invest in sufficient procedures to build confidence in their platform among the main body of consumers, but their priorities will not include the distributive and fairness concerns that might matter to society as a whole.

The message of this chapter is certainly not tech utopianism, but nor is it tech pessimism. Call it tech realism. Market and technological approaches to the new consumer protection problems of online commerce hold some promise, but their promise should not be overstated.

Technology will have to be harnessed by lawmakers, regulators, and consumer advocates in order to help consumers with the endemic problems of consumer protection in the digital age. Along these lines, there is promising work seeking to find better ways for consumers to organize themselves to pressure merchants

30 On the digital divide, see Bradley, 'FinTech's Double Edges' (n 18) 92–94.

31 Rory Van Loo, 'The Corporations as Courthouse' (2016) 33 Yale J Reg 547; Schmitz (n 13).

and marshal the power of reputation in the case of consumer protection.[32] These efforts remain quite limited in scope but are promising areas for further research and experimentation.

Part 4 illustrates some key legal and political battles in modern consumer protection by focusing on the remarkable recent mêlée over the *Restatement of the Law, Consumer Contracts*. This work tried to reshape contract law to fit the realities of modern practices, to bring clarity for merchants and consumers. However, it drew fierce oppositions from both sides of this divide and shows how deeply divided and unsettled the relationship between consumers and merchants in the age of ecommerce remains. In light of the ultimate failure of this project, Part 5 of this chapter returns to what can be done to remedy the problems with online consumer transactions.

4 Not Ready to Restate: A Rejected Consumer Contracting "Bargain"

In 2019, in the fiercest consumer law controversy in recent memory, the American Law Institute declined to approve a proposed *Restatement of the Law, Consumer Contracts*. The Restatement's reporters were well-respected academics, all of whom have done important, groundbreaking work focused on modern commercial practices and consumer protection.[33] The project went through several revisions in response to criticisms. Nonetheless, after a bitter fight, the project was tabled by the full ALI membership.[34] Its failure—indeed, the fact that it drew such fierce opposition—surprised many, and perhaps the reporters themselves.

The Restatement was an attempted middle ground, an attempt to clarify and consolidate contract law in the age of streamlined and especially online consumer commerce.[35] A "Grand Bargain" lay at its heart: The Restatement provided that consumers' assent to contracting terms written by the business either prior to or mid-way through the contractual relationship could be largely assumed, provided the terms met rudimentary standards of notice, and that "privacy policies" would generally be included as terms in consumer contracts, all of which was considered to be favorable to business interests. But the Restatement also emphasized,

32 Yonathan A Arbel, 'Reputation Failure: The Limits of Market Discipline in Consumer Markets' (2020) 54 Wake Forest L Rev 1239.

33 For example, Oren Bar-Gill, *Seduction by Contract: Law, Economics and Psychology in Consumer Markets* (2012) Oxford; Florencia Marotta-Wurgler, 'Competition and the Quality of Standard Form Contracts: The Case of Software License Agreements' (2008) 5 J Empirical Legal Studs 447; Omri Ben-Shahar, 'Fixing Unfair Contracts' (2011) 63 Stanford L Rev 869.

34 Amer L Inst, 'Restatement of the Law, Consumer Contracts, Status' (only Section 1 (of 9) approved by membership) <www.ali.org/projects/show/consumer-contracts/> accessed 1 October 2020.

35 Bar-Gill and others, 'Reporters' Introduction' (n 8) (reproducing draft of the proposed Restatement at 99–102).

and arguably enhanced, consumer access to various defenses and challenges to the enforcement of contract terms. It sought to revise unconscionability and deception doctrines, to make it more difficult for companies to disavow precontractual representations, to impose unusual or surprising contract terms, or to use the "parol evidence rule" to deny consumers the benefit of representations made prior to the moment of contracting by the merchant's representatives.[36]

The Restatement purported to be based on a careful, quantitative analysis of a substantial body of relevant case law.[37] As it turned out, the empirical analysis that provided the basis of the project's core findings served as a wedge issue for its opponents. The sharpest challenges to the Restatement were positioned as methodological in nature and centered on the Restatement's analysis of the existing body of contract cases.[38] The methodological emphasis was necessary in part because the reporters had trumpeted their innovative, quantitative empirical approach as providing a distinctively sound foundation to their conclusions. Opponents challenged the underlying evidence, arguing among other things that few courts had actually based their rulings on the principles presented in the Restatement and that there was considerable precedent supporting different or even opposite conclusions. They argued both that there was too little case law to form a consensus and that the sparse case law was itself equivocal in its support for the principles announced in the Restatement.

The Restatement was opposed by a most remarkable coalition: Representatives of business interests and advocates for consumers both fought it bitterly. The alliance in opposition doesn't indicate an alliance in reasoning, however. Business interests were most concerned by the Restatement's introduction of concepts and terms from the academic literature but not known in the case law, such as the concept of saliency; they feared the prospect of courts led down primrose paths by creative consumer advocates, unsettling what they consider a generally favorable status quo.[39]

36 Whether the Restatement actually expands all of the specified defenses is a matter of some controversy. Letitia James and others, 'Letter to Members of the American Law Institute from Twenty-Three State Attorneys General, Restatement of the Law, Consumer Contracts' (14 May 2019) <www.consumerfinancemonitor.com/wp-content/uploads/sites/14/2019/05/letter_to_ali_members2.pdf> accessed 1 October 2020 (objecting that the unconscionability defense has not been expanded or clarified).

37 Oren Bar-Gill, Omri Ben-Shahar and Florencia Marotta-Wurgler, 'Searching for the Common Law: The Quantitative Approach of the Restatement of Consumer Contracts' (2017) 84 U Chi L Rev 7.

38 Levitin and others (n 8); Gregory Klass, 'Empiricism and Privacy Policies in the Restatement of Consumer Contract Law' (2019) 36 Yale J Reg 45.

39 Fred H Miller, 'A Restatement That Is Not a Restatement' (18 April 2019) 22 *Consumer Financial Servs. Law Report* 1; Alan S Kaplinksy, 'ALI's Restatement of the Law, Consumer Contracts: An Ill-Conceived and Poorly Implemented Project' (*Consumer Finance Monitor*, 16 May 2019) <www.consumerfinancemonitor.com/2019/05/16/alis-restatement-of-the-law-consumer-contracts-an-ill-conceived-and-poorly-implemented-project/> accessed 1 October 2020.

By contrast, consumer advocates mostly expressed frustration with the portrayal of a firm legal consensus on the issue of contract formation and assent. To some of them, the absence of controlling case law was itself meaningful, suggesting that the area of law remained unclear, or perhaps even that merchants were intentionally making sure that "bad" cases were kept out of the courts. Undoubtedly, many would-be cases are shunted into arbitration, are settled before a ruling, do not yield a written opinion,[40] or are dealt with by regulators rather than in the judicial process. Or the injuries are simply "lumped" by consumers.[41]

With these critiques of the project's ambitious methodological claims in hand, opponents recast the project as not a "restatement" of the law as already applied by courts but an effort to shape and clarify what remains still inchoate and unsettled. Cannily, by making much of the empirical faults of the Restatement and attacking the empirical work that had been presented as the project's primary basis, opponents weakened the project considerably. Opponents were able to shift the debate, forcing American Law Institute members considering their vote on the matter not to ratify a course already blessed by a clear majority of courts but to take a stand on the normative desirability of the balance struck by the Restatement.

Practically speaking, the empirical debate, while important, would have been of primarily academic interest and would not have doomed the project had the objectors—or perhaps even one of the two primary camps—considered the substantive outcome of the project to be desirable. Although the Restatement had its supporters,[42] the objections were widely publicized and opposition at ALI meetings was organized in advance; the against-the-odds effort to derail the Restatement was successful. This effort reflects not just an attempt to protect the integrity of empirical legal scholarship, important though that goal may be to many of the objectors; the elaborate strategic effort reflects staunch opposition to the substance of the "Grand Bargain." So it is worth considering the substantive reasons that advocates were opposed to the Restatement and how the debate speaks to the broader outlook for the law of consumer contracts in today's environment.

As mentioned, the Restatement was opposed vehemently from prominent advocates on both the merchant and the consumer side—a puzzling coalition. Business interests opposed the "Grand Bargain" because it risked expanding the

40 Matters may be resolved by trial-level state courts that have no call for reasoned, written opinions. Many debt collection lawsuits yield only default judgments.

41 See, for example, Issacharoff and Marotta-Wurgler (n 17).

42 See, for example, Steven O Weise, 'The Draft Restatement of the Law, Consumer Contracts Follows the Law' (*The ALI Advisor*, 5 April 2019) <https://thealiadviser.org/consumer-contracts/the-draft-restatement-of-the-law-consumer-contracts-follows-the-law/> accessed 1 October 2020.

availability of consumer defenses. They seemed to believe that whether in arbitrations or in courts, they could prevail on contract formation and assent and defeat any of the standard common-law defenses. In other words, they believed that disputes are currently governed by a relatively certain and business-friendly version of contract law, better for them than the Restatement, particularly with its potentially risky attempted expansion of unconscionability and deception defenses.

Businesses had, and have, reason for optimism. Courts generally appear to believe that judges must adapt traditional common law to the imperative of stimulating easy, mass commerce but that public policy or distributional concerns should be left for the legislative branch. Courts often base their rulings on naïve assumptions about economics and use this simplistic and empirically unsupported economic reasoning to support their "adaptations" of the common law to modern business practices. The notorious ruling of the United States Supreme Court in *Carnival Cruise Lines v. Shute* provides an easy example.[43] In the decision, a majority of the Court enforced a forum selection clause in favor of the cruise line, against consumers who were seriously injured on a cruise but could not afford to bring an action in the cruise line's preferred forum.[44] The clause at issue was listed among much other small print terms on the cruise ticket received only after the transaction had been completed. The customers apparently "agreed" to the term by not cancelling the cruise upon receipt of the ticket.[45]

In justifying its decision, the *Carnival* Court stated that

> it stands to reason that passengers who purchase tickets containing a forum clause like that at issue in this case benefit in the form of reduced fares reflecting the savings that the cruise line enjoys by limiting the fora in which it may be sued.[46]

Of course, it's not at all clear that any cost savings for Carnival outweighed the increased costs (in the form of risk) imposed on all customers; or that any surplus generated would go to consumers in the form of lower costs rather than to shareholders as additional profits, given the actual characteristics of the market for

43 499 U S 585 (1991). Numerous negative assessments followed on the heels of the case. For example, Patrick J Borchers, 'Forum Selection Agreements in the Federal Courts After Carnival Cruise: A Proposal for Congressional Reform' (1992) 67 Wash L Rev 55, 59; Lee Goldman, 'My Way and the Highway: The Law and Economics of Choice of Forum Clauses in Consumer Form Contracts' (1992) 86 Nw U L Rev 700.

44 The appeals court opinion states they could not afford the cross-country litigation; the Supreme Court majority claims this statement lacked evidentiary support.

45 Because the consumers did not directly challenge their receipt of notice of the terms, the Court stated that they "presumably retained the option of rejecting the contract with impunity." *Carnival Cruise Lines* (n 43) 595.

46 *Carnival Cruise Lines* (n 43) 594.

cruises, rather than the idealized world of perfectly competitive and information-rich markets the Supreme Court seems to have based its ruling on.[47] The Court also failed to acknowledge the distributive concerns presented: Should customers as a whole reap cost savings at the expense of those without the resources to litigate in far-flung venues?

The *Carnival Cruise Line* decision is hardly alone in indulging in pro-business assumptions and armchair-economics in order to enforce contract terms. Businesses generally, although by no means universally, count on this type of approach from U.S. courts. Thus, opening consumer challenges to the knee-jerk enforcement of contract terms represented too great a risk, even if it permitted merchants to consolidate their perceived progress on other fronts. Apparently, merchants feared a blitz of unconscionability or deceptive practices arguments emanating from consumers who might otherwise be bound by disadvantageous standard terms in merchants' adhesion contracts. Merchants preferred the current state of the law because it generally presumes their preferred standard terms are in place and gives consumers only narrow opportunities to urge defenses. As mentioned, because merchants can use arbitration or confidential settlements to "bury" cases in which such defenses might otherwise be successful, the availability of pro-consumer precedent is more lacking than it perhaps should be. In the view of merchants, the Restatement risked giving consumers too many ways to make mischief—providing some clarity as to defenses that have otherwise largely remained in the shadows.[48]

By contrast, consumer advocates argued that the proposed principles placed too little emphasis on ensuring that consumers actually understood and agreed to the terms. Consumer advocates resisted the notion that consumers should bear the burden of urging a defense to contract terms. Rather than permitting a judge to deny that terms were ever agreed upon—which, all concede, is the likely reality in many consumer contracts—the Restatement would force judges to overturn terms that were presumed valid. Consumer advocates were skeptical that courts would accept such defenses with any regularity, even where merited. Although their views are diverse, consumer advocates generally take the view that the burden of establishing the enforceability of contractual terms should be shifted to merchants. They argue that in order to enforce particular terms, merchants should be required to demonstrate that the terms are not abusive or unfair and that the contracting process was not deceptive as to the consumer in question.[49] Most also believe that numerous unfair terms should be prohibited explicitly and

47 For instance, with a few large cruise operators dominating the market, they might easily be able to collect and charge above-market prices; in addition, venue clauses and similar terms are buried in practically illegible terms and conditions, and this might hinder efficient pricing of them in this market.

48 This is not to say that the defenses are unsuccessful; merely that successful invocations are not well-known. Jacob Hale Russell, 'Unconscionability's Greatly Exaggerated Death' (2019) 53 U Cal Davis L Rev 965.

49 Pridgen 'Proposed Restatement' (n 9).

altogether, not just by consumer protection law but on the basis of contract law itself. Arbitration provisions, and particularly those that bar class actions, are good examples of such bêtes noires.

Consumer advocates prioritize the preservation of access to courts, and to both common-law and modern statutory consumer-protective doctrines. They have numerous strong arguments. For one, traditional doctrine presents a more robust notion of consent than has become the norm in online contracting. Again, while debates over adhesion contracts are hardly unique to the ecommerce context, they bear greater importance when such contracts seek to control the vast majority of purchases of goods and services. Consumer advocates argue that courts should be more skeptical of merchants' attempts to hit all consumers with blunderbuss "terms of service" regardless of consumers' actual understanding or agreement.

Consumer advocates also have a powerful argument based on actual merchant practices (although this argument does not seem to have arisen in the Restatement debates). As numerous remarkable studies have shown, businesses increasingly use artificial intelligence and large troves of data to target individual consumers and particularize price and other aspects of their offers to consumers—often precisely in order to maximize likelihood of purchase while minimizing actual comprehension of undesirable terms of agreements.[50] It is at best cynical and hypocritical, consumer advocates argue, for businesses tailoring the customer experience to their advantage to then protest that they shouldn't be forced to give a second thought to consumers' reasonable expectations or consent to contractual terms. Because merchants can and do customize their interactions with customers in numerous ways, often taking advantage of informational advantages about individual consumers, they cannot be permitted to disavow knowledge of individuals or the ability to customize interactions in order to ensure that contracting practices actually attain something like the contractual ideal of agreements made by informed parties for mutual benefit.

In the end, consumer advocates judged that anything that consumers got out of the Restatement was not worth consolidating their losses in terms of assent/formation.[51] Consumers' advocates may have felt that in the days of a Republican administration showing little concern for consumer issues, they had nowhere to go but up. Consumer advocates may have also thought that the wind was changing; and indeed, public attitudes on technology have been changing. For example, public attention has been drawn of late to consumer privacy issues and to the dangers of centralization of power and money in the hands of a few massive corporations. As views change, political resistance to contract law favoring these

50 Lauren E Willis, 'Deception by Design' (2020) 34 Harv J L & Tech 115.

51 Adam Levitin, 'Podcast on ALI Consumer Contracts Restatement' (*Credit Slips Blog*, 16 May 2019) ("[The Restatement] creates more litigation problems for businesses without creating meaningful consumer protections") <www.creditslips.org/creditslips/2019/05/podcast-on-ali-consumer-contracts-restatement.html> accessed 1 October 2020.

parties may well rise. Courts and legislators alike may be more amenable to consumer protection through contract law as well as through other bodies of dedicated consumer-oriented law and regulation, although this remains to be seen.

The penultimate Part of this chapter further assesses the prospects for change, suggesting some legal and regulatory reforms that consumer advocates may welcome, although of course they do not speak with one voice.

5 Marshaling Doctrinal, Regulatory, and Technological Protections for Consumers in the Digital Age

A revolution in consumer commerce calls for a revolution in consumer protection. The first revolution has come; the other has not. Whether political forces will align to permit legal change remains unclear, but the need is clear. This Part of the chapter looks to the prospects for change and the forms it might take.

Change to governing laws could make a clear and significant difference. This includes both substantive rules regarding how and on what terms contracts are formed—see the Restatement debate discussed previously—as well as the procedural means through which harm is redressed. Perhaps the most well-known aspect of consumer law is that the harm of a wrongful business practice may be, on a per-consumer level, too small to make it worth pursuit of a claim. Despite this fact being widely—universally?—acknowledged, its effect on actual laws is limited.[52] Access to collective remedies has narrowed in recent years, in fact; at the same time, due to strongly pro-arbitration federal law, consumers in the United States have often been forced out of courts and into arbitration fora in which their claims for the most part quickly and quietly die.

So far, courts have limited consumers' avenues to legal redress. Ensuring that consumers can band together and seek relief through class actions and other forms of collective action would be one promising avenue for reform, as would be providing for statutory damages and attorneys' fees where actions are otherwise uneconomical to bring. In addition to legislative and regulatory change, shifts in social attitudes may cause judges to become more receptive to the adaptation of common-law remedies.

Legal change might be especially crucial in the realm of consumer privacy. Over time, several conclusions about consumers' private data have become increasingly clear, not just to the experts who might have known them from the start, but to many in the broader public. First, the stakes of this issue are high for consumers, because the misuse of their private information can disrupt every area of their existence in our internet-saturated society, disrupting personal security, social life, and access to employment, housing, credit, and commerce. Second, companies will not sufficiently police themselves and market dynamics cannot be trusted to protect data. Ultimately, protection of consumers' data will require legislative intervention, at least some of which will require national and even international

52 See Bradley, 'FinTech's Double Edges' (n 18) 83; ibid, n 78 (collecting sources).

coordination to be successful. Some jurisdictions have passed laws that represent worthwhile first steps in this regard, but most remain sluggish, having not even started down what will no doubt be a long road toward appropriate substantive and procedural regulation of this important and challenging dimension of modern life and commerce.

Fostering regulatory institutions is also crucial to consumer protection in the digital age. Regulatory institutions play a crucial, multifaceted role in consumer protection. First, regulatory institutions are a vital link between law-in-the-books and law-in-action. Consumers and their advocates can only rarely bring legal actions cost-effectively, particularly in the current landscape, which is hostile to forms of collective remedy. Regulators can investigate and bring actions that would not be feasible for anyone else, due for instance to a high degree of complexity or to the fact that the harm for each individual consumer is relatively small. Second, regulators can often pass new regulations and issue guidance, responding to emerging challenges more nimbly than legislators. Third, regulators play a role in research, by information gathering and aggregation and by providing analysis of industry practices and trends. By providing guidance concerning emerging issues, by gathering and promulgating information and analysis, and by providing a focal point for advocacy, regulators can help facilitate consumer organization and activism.

Yet as surveyed in Part 2, regulators are limited in various ways. Many lack statutory authority to bring certain claims, promulgate certain regulations, or take other actions that would serve the public interest. Others lack funding. The cross-border nature of much digital commerce adds more difficulties. Because there is no effective transnational consumer regulator or means for regular regulatory cooperation, regulators may lack authority to address them, or even motivation—injured consumers outside of a given jurisdiction may be unable to bring sufficient pressure to bear on authorities designated to regulate well-connected businesses within that jurisdiction.

It is easy to see that regulators could be helped by increased funding; by statutory authorization to regulate and enforce, including across borders and in greater collaboration with other authorities; and by efforts to foster research and development of novel tools and approaches. Again, while such steps might seem pie-in-the-sky, changes in political attitudes can bring speedy change.[53] It is important to keep in mind as well that within the United States, individual states retain the power to pursue many of these steps on their own; California, New

53 Witness the transformation of antitrust from sleepy legal backwater to prominent populist rallying-cry against the most powerful companies in the world. Whether the new notions of antitrust will have effect remains to be seen, but the change of political support for "breaking up" large tech companies is a striking fact. See David Streitfeld, 'To Take Down Big Tech, They First Need to Reinvent the Law' (*NY Times*, 20 June 2019) <www.nytimes.com/2019/06/20/technology/tech-giants-antitrust-law.html> accessed 1 October 2020.

York, and others have passed laws and strengthened institutions for consumer protection in the last several years.[54]

Regulation may itself take novel forms, for instance, as a combination of technological and legal tools. Professor Lauren Willis has proposed a combination of legal and technical protections in the form of what she calls "performance-based regulation."[55] As applied to consumer contracts, her model would require companies to show that their customers know what they have agreed to for a consumer contract term to be binding. Her proposal sounds outlandish from a traditional regulatory perspective, but it emerges from a deeply observed account of how merchants actually engage in online commerce. It takes into account new marketing and sales strategies and may well be not only the most effective but also the cheapest form of effective regulation.

Online dispute resolution may provide real consumer relief as well. While the most advanced ODR efforts remain those developed by private actors, the limits of which are described in Part 3, ODR holds considerable promise. With public oversight to ensure that concerns of fairness and access are much more to the fore, ODR could substantially lower the costs of dispute resolution and thus increase the remediability of numerous forms of consumer harm that consumers currently "lump."[56] Again, technology is no panacea; it's not a matter of simply implementing an off-the-rack ODR system to resolve all consumer disputes. But given the many failures of our existing dispute resolution system for consumers, ODR is an important avenue for potential change and improvement to the status quo.

6 Conclusion

Consumer protection is vital, both because consumer impact on the economy is substantial, and thus protecting and facilitating the healthy functioning of consumer markets is valuable, but also because there is independent value in consumer protection, particularly of vulnerable individuals. To permit producers and sellers to take advantage of consumers belies fundamental societal commitments to equality and opportunity.

54 Alex Roha, 'California Expands Oversight of Consumer Protection Watchdog' (*Housing Wire*, 28 September 2020) (discussing laws in California, New York, and Pennsylvania), <www.housingwire.com/articles/california-expands-oversight-of-consumer-protection-watchdog/> accessed 1 October 2020; Jill Cowan and Natasha Singer, 'How California's New Privacy Law Affects You' (*NY Times*, 3 January 2020) (describing California privacy law), <www.nytimes.com/2020/01/03/us/ccpa-california-privacy-law.html> accessed 1 October 2020.

55 Willis (n 11).

56 Emily S Taylor Poppe, 'Why Consumer Defendants Lump It' (2019) 14 Nw J L & Soc Pol'y 149 (quoting Katherine Porter, *Modern Consumer Law* (2016) Wolters Kluwer, 518 ("Underenforcement via private lawsuit is perhaps the most vexing problem in consumer law")).

This chapter has argued that consumer contracting in the digital age presents a real and present challenge for which our current legal, regulatory, technological, and social structures are inadequate. Business practices have changed rapidly, transforming consumer markets. But regulatory vigilance has been lacking. Legal tools lag behind, and public support for regulatory institutions has been inadequate.

The work of consumer protection is never done. The law and regulation needed to ensure consumer access to the necessities of life has to evolve as the ways in which consumers interact with markets and products evolve.[57] Adequately addressing the challenges of consumer protection today will require the involvement of technology, but we cannot expect actual progress by relying passively on technology alone. Instead, developing the new technological and legal forms of consumer protection we need will require a renewed commitment to research, political organization, public interest lawyering, and other forms of social involvement.

57 Bradley (n 5).

6 Paradigms of EU Consumer Law in the Digital Age

Felix Maultzsch

1 Introduction

Consumer contracts and their legal regulation constitute one of the core areas of EU law and the Union's concept of a European single market. Article 114(1)(2) of the Treaty on the Functioning of the European Union (TFEU)[1] allows for harmonisation of provisions that "have as their object the establishment and functioning of the internal market", which includes issues of consumer law.[2] In addition, Art. 38 of the Charter of Fundamental Rights of the European Union (CFR)[3] guarantees a high level of consumer protection as a fundamental right. At the same time, digitalisation is advancing inexorably, constantly challenging the law and demanding a reaction from it. Against this background, it seems promising to shed some light on how the rapid process of digitalisation influences the field of consumer contracts from a European perspective. In doing so, the following considerations will focus on the example of business-to-consumer (B2C) contracts for the sale of "conventional" goods in an increasingly digital environment, especially in the form of online sales. One might wonder whether, in tracing the relationship between consumer contracts and a possible emerging law of global digitality, it would not be more rewarding to analyse contractual contents that are themselves "digitalised". Such an approach could focus, for example, on contracts for the supply of digital content that have undergone a process of harmonisation in the EU recently.[4]

1 Consolidated version of the Treaty on the Functioning of the European Union [2012] OJ C326/47.

2 See Stephen Weatherill, Stefan Vogenauer and Petra Weingerl, 'Private Autonomy and Protection of the Weaker Party' in S Vogenauer and S Weatherill (eds), *General Principles of Law: European and Comparative Perspectives* (2017) Hart Publishing, 255, 257ff.

3 Charter of Fundamental Rights of the European Union [2012] OJ C326/391.

4 Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services [2019] OJ L136/1. For an analysis of this Directive see Karin Sein and Gerald Spindler, 'The New Directive on Contracts for the Supply of Digital Content and Digital Services—Scope of Application and Trader's Obligation to Supply—Part 1' (2019) 15 ERCL 257 and Karin Sein and Gerald Spindler, 'The New Directive on Contracts for Supply of Digital Content and Digital Services—Conformity Criteria, Remedies and Modifications—Part 2' (2019) 15 ERCL 365.

DOI: 10.4324/9781003283881-10

However, to observe possible emerging patterns of a "digital code" of consumer law, it might be even more conclusive to focus on a traditional type of contract, such as the sale of goods, that comes from the offline world and to ask whether and to what extent it is influenced by new patterns of digitality.

The main argument of this chapter will be that, although there is no comprehensive, separate body of law for cross-border online sales in the European context, sales law in general is heavily influenced by the new paradigm of digital sales. In this paradigm, the primary aim of contract law is no longer to protect the individual autonomy of the parties and to balance their interests but more and more to protect and facilitate markets as such. In that scenario, a party-centred perspective on contract law is replaced by a market-centred perspective. The shift to this market paradigm is not limited to substantive contract law but extends to regulatory techniques in private international law, law enforcement and developments in private contractual practice.

The following analysis will proceed in several steps: After a closer look at the concept of a market-centred approach to contract law (Section 2), its leading role for consumer sales will be traced across different sub-areas. These include international jurisdiction and conflict of laws (Section 3), the related issue of the extra-territorial application of EU consumer law (Section 4), important trends in substantive EU sales law (Section 5), alternative means of dispute resolution and enforcement of consumer rights (Section 6) and private governance by contract and technology (Section 7). Some conclusions will complete the considerations (Section 8).

2 The Market-Centred Approach to Contract Law

With the increasing importance of online sales in digital markets, we can witness a new paradigm of consumer law, namely the shift from a party-centred perspective to a market-centred perspective on consumer contract law.[5]

To understand this shift, it is useful to shed some light on the classical paradigm of contract law as it is embedded in the Continental European tradition, especially in the German Civil Code (*Bürgerliches Gesetzbuch*). The German Civil Code follows a normative concept which might be called a "personal" account of contract law.[6] This concept classifies a contract, first and foremost, as an autonomous act of the parties and it aims at ensuring an adequate balancing of interests between them. The benchmark for contractual justice is determined by the idea of private autonomy. The parties make use of a contract as a means to independently arrange for their living conditions and to pursue ends which are

5 Cf for different accounts of contract law in the recent process of European harmonisation on a general level Martijn W Hesselink, 'Five Political Ideas of European Contract Law' (2011) 7 ERCL 295. See, for the following, also Felix Maultzsch, 'Einführung: Steht das BGB vor seiner Ablösung?' in J-U Hahn (ed), *Gemeinsames Europäisches Kaufrecht: Moderner Ansatz oder praxisferne Vision?* (2012) C.H.Beck, 9, 14ff.

6 See Jörg Neuner, *Allgemeiner Teil des Bürgerlichen Rechts* (12th edn, 2020) C.H.Beck, § 10 para 2ff.

not questioned or channelled by contract law.[7] This results, by and large, in a formal legal framework which is not meant to serve economic policy aims but to order personal legal relations. Logically consistent, this legal framework is a general civil law which applies regardless of whether the parties to a contract are members of a certain market group such as traders or consumers.[8] The focus is on the legal subject as such and not on its being part of the market.

In contrast, the consumer law of the EU in its digitalised version has its primary focus less on the protection of individual autonomy and on levelling parties' interests but more and more on the protection and facilitation of markets. In this context, we can find a strong link to the policy aim of fostering the European single market, especially by strengthening cross-border consumption.[9] This overarching goal leads to the micro-perspective of a personal contractual relation being superseded by the macro-perspective of the market. Consequently, the normative focus shifts from the contractual parties as individual legal subjects to a broader thinking in market groups such as traders and consumers. EU contract law, therefore, does not come as a general civil law but rather as a new type of commercial law with a focus on B2C contracts.[10]

Having sketched the dichotomy between a party-centred perspective and a market-centred perspective on contract law, two caveats seem to be important.

Firstly, one might rightfully argue that the focus on market facilitation found in EU contract law is not a novelty of the age of digitalisation but has always been at the heart of the idea of a European single market.[11] In particular, the

7 Werner Flume, *Allgemeiner Teil des Bürgerlichen Rechts, Band II: Das Rechtsgeschäft* (4th edn, 1992) Springer, § 1; cf also Franz Wieacker, *Privatrechtsgeschichte der Neuzeit* (3rd edn, 2016) Vandenhoeck and Ruprecht, 481ff and, on the importance of personal responsibility in a traditional sense, Michael Martinek, 'Das Prinzip der Selbstverantwortung im Vertrags- und Verbraucherrecht' in K Riesenhuber (ed), *Das Prinzip der Selbstverantwortung: Grundlagen und Bedeutung im heutigen Privatrecht* (2011) Mohr Siebeck, 247, 254ff.

8 Cf, with criticism of the differing approach of EU law, Thomas Pfeiffer, 'Anwendungsbereich: Vertragsparteien und Vertragsgegenstand' in O Remien, S Herrler and P Limmer (eds), *Gemeinsames Europäisches Kaufrecht für die EU?—Analyse des Vorschlags der Europäischen Kommission für ein optionales Europäisches Vertragsrecht vom 11. Oktober 2011* (2012) C.H.Beck, 35, 39ff.

9 Simon Whittaker, 'The Optional Instrument of European Contract Law and Freedom of Contract' (2011) 7 ERCL 371, 381ff. For an in-depth account of the instrumental focus of EU private law, see Christoph U Schmid, *Die Instrumentalisierung des Privatrechts durch die Europäische Union—Privatrecht und Privatrechtskonzeptionen in der Entwicklung der Europäischen Integrationsverfassung* (2010) Nomos.

10 Peter-Christian Müller-Graff, 'Ein fakultatives europäisches Kaufrecht als Instrument der Marktordnung?' in H Schulte-Nölke, F Zoll, N Jansen and R Schulze (eds), *Der Entwurf für ein optionales europäisches Kaufrecht* (2012) Sellier European Law Publishers, 21, 30ff and Peter-Christian Müller-Graff, 'Der Introitus des optionalen Europäischen Kaufrechts: Das erste Kapitel im Kontext von Kodifikationskonzept und Primärrecht' in M Schmidt-Kessel (ed), *Ein einheitliches europäisches Kaufrecht?—Eine Analyse des Vorschlags der Kommission* (2012) Sellier European Law Publishers, 51, 68ff.

11 Cf Weatherill, Vogenauer and Weingerl (n 2) 257ff.

EU concept of consumer protection was never limited to the aim of creating a legal environment in which consumers possess the means to make substantial autonomous decisions in the sense of a classical party-centred perspective on contract law. In contrast, the EU approach has, even before the advent of digitalisation, put a strong emphasis on fostering consumer confidence in the context of cross-border relations and on boosting consumption.[12] However, cross-border consumption by consumers was severely limited on a practical level before the emergence of digitalised online sales. Of course, it was possible for traders to physically transfer their goods across borders to offer them to consumers all over Europe on the spot, and the EU has long done its best to support this process. But it is only with the opportunity of consumers to "reach out" by means of digital orders that a market-centred approach of consumer contracts was able to achieve full momentum. It, therefore, does not come as a surprise that the EU itself proclaims a new paradigm with its agenda to transform the European single market into a "digital single market".[13]

Secondly, it would be a mistake to assume a pure contradiction between a market-centred and a party-centred approach of contract law. The market is the very means by which legal persons can enter into an autonomous contractual relationship as free and equal subjects.[14] Against that background, the law of the European single market can be perceived as an institutional framework allowing for individual freedom (*Freiheitsermöglichungsrecht*).[15] Vice versa, traditional contract law is not limited to being a background for mere individual legal relations but also has the character of an institutional arrangement which orders economic transactions as such.[16] However and despite all transitions and interconnections between the two paradigms, one can still draw a distinction as to what the *Leitmotiv* of contract law is.[17]

The traditional notion which is embodied in the classical account of the German Civil Code has its focus on freedom of contract.[18] This principle is supplemented by default rules fulfilling a service function for the parties by

12 See Bettina Heiderhoff, *Europäisches Privatrecht* (5th edn, 2020) C.F. Müller, para 192ff and Hannes Rösler, *Europäisches Konsumentenvertragsrecht: Grundkonzeption, Prinzipien und Fortentwicklung* (2004) C.H.Beck, 188ff.

13 See the EU Commission's agenda 'Shaping the Digital Single Market' <https://ec.europa.eu/digital-single-market/en/policies/shaping-digital-single-market> accessed 10 May 2021.

14 Müller-Graff, 'Der Introitus des optionalen Europäischen Kaufrechts' (n 10) Sellier European Law Publishers, 53ff.

15 Martin Schmidt-Kessel, 'Der Vorschlag der Kommission für ein Optionales Instrument—Einleitung' in M Schmidt-Kessel (ed), *Ein einheitliches europäisches Kaufrecht?—Eine Analyse des Vorschlags der Kommission* (2012) Sellier European Law Publishers, 1, 2ff.

16 For the interconnection between private autonomy and market mechanisms see Flume (n 7) § 1/7 and Fritz Rittner, 'Der privatautonome Vertrag als rechtliche Regelung des Soziallebens' (2011) 66 JZ 269.

17 Cf Maultzsch (n 5) 16ff and Whittaker (n 9) 386ff.

18 Flume (n 7) § 1/8.

relieving pressure from the process of contractual negotiations and by making gaps in contracts controllable.[19] Finally, mandatory law—besides its possible protective function for third parties and public interests—is basically meant to protect "weak" parties in situations where the preconditions for a substantive autonomous decision are not fulfilled (e.g. consumer protection law in a narrow sense).[20]

In contrast, the new market-centred approach increasingly replaces the idea of freedom of contract by a standardisation of possible contractual contents. In particular, we find mandatory law for B2C transactions in EU law not only as a means to protect "weak" parties[21] but even where a specific need of protecting consumers' autonomy is difficult to discern.[22] In that context, we encounter a phenomenon of what might be called "bonus rules" for consumers. This refers to very consumer-friendly and typically mandatory rules which are not meant to protect legitimate expectations but to boost consumption incentives. Finally, the market paradigm of contract law is focussed on equality of competition for traders in cross-border transactions.[23] All of these properties are quite coherent for a set of law which is not so much meant to guarantee an adequate levelling of parties' interests in personalised legal relations but to ensure smooth commerce and consumption across borders.[24]

3 International Jurisdiction and Conflict of Laws: Connecting Factors

A market-centred approach can, first of all, be recognised in the connecting factors chosen by European private international law for international jurisdiction and conflict of laws. The relevant rules can be found in Art. 17(1)(c) of the Brussels Ibis Regulation[25] (international jurisdiction) and Art. 6 of the Rome I Regulation[26] (conflict of laws). If a seller "directs" its business to the state in

19 Hein Kötz, *Vertragsrecht* (2nd edn, 2012) Mohr Siebeck, para 58; For an in-depth analysis, see Johannes Cziupka, *Dispositives Vertragsrecht: Funktionsweise und Qualitätsmerkmale gesetzlicher Regelungsmuster* (2010) Mohr Siebeck, 44ff.

20 See Neuner (n 6) § 3 para 12ff and, on a more general level, also Claus-Wilhelm Canaris, 'Wandlungen des Schuldvertragsrechts—Tendenzen zu seiner "Materialisierung"' (2000) 200 AcP 273.

21 Although this protective approach is often invoked as the core of EU consumer law, see Norbert Reich, *General Principles of EU Civil Law* (2014) Intersentia 37ff.

22 For more details, see infra Section 5.

23 See, with respect to the targeting criterion in international jurisdiction and conflict of laws, infra Section 3, and, with respect to the principle of full harmonisation, infra Section 5.

24 Cf Heiderhoff (n 12) para 237ff.

25 Regulation (EU) 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgements in civil and commercial matters (recast) [2012] OJ L351/1.

26 Regulation (EC) 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I) [2008] OJ L177/6.

which the consumer has its habitual residence and if the contract "falls within the scope" of the directed activities, then

1. the consumer's place of habitual residence will be the place of jurisdiction and the substantive law of this place will be applicable to the contract, furthermore
2. the parties to the contract cannot deviate from these rules to the detriment of the consumer by a choice-of-court or choice-of-law agreement.

According to the case law of the Court of Justice of the European Union (CJEU), the question whether a seller has directed its business to the market where the consumer has its habitual residence must be determined by taking into account all circumstances.[27] The mere facts that a seller's website is retrievable in the consumer's country and does use the language of that country do not suffice in that respect. But the content of the website (adjustable language, possible choice of delivery destination), its appearance (country-specific top-level domains) as well as the provision of international customer care (international dialling codes, etc.) have to be taken into account. By submitting a trader to the legal standards of the targeted market, EU law not only privileges consumers but also facilitates competitive standardisation regardless of the place of business of the acting traders. This is because the enforcement of the target market standards treats all suppliers equally which direct their business to a certain geographical area.

It should also be noted that the CJEU has given Art. 17(1)(c) of the Brussels Ibis Regulation and Art. 6 of the Rome I Regulation a very broad reading, extending far beyond the core area of cross-border online sales. In the *Mühlleitner* case, it has held that Art. 17(1)(c) of the Brussels Ibis Regulation not only applies to distance selling but also to cases where a consumer has only acquired pre-contractual information on a website directed to its home country and has then chosen to enter into the contract abroad at the seller's place of business.[28] This decision was not unavoidable since a joint declaration of the European Council and the EU Commission on ex-Art. 15 Brussels I Regulation[29] (Art. 17 Brussels Ibis Regulation), which is also referred to by the Rome I Regulation,[30] had stated that the rule should be limited to cases of distance selling.[31] Furthermore, the CJEU decided in the *Emrek* case that if a seller directs its business towards a foreign market via the internet, consumers domiciled in this market who later enter into a local transaction at the seller's place of business abroad can take advantage of Art. 17(1)(c) of the Brussels

27 Joint Cases C-585/08 and C-144/09 *Pammer and Hotel Alpenhof* [2010] ECR I-12527, para 80ff.

28 Case C-190/11 *Mühlleitner* (CJEU, 6 September 2012) para 32ff.

29 Council Regulation (EC) 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgements in civil and commercial matters [2001] OJ L12/1.

30 See recital 24 of the Rome I Regulation.

31 See Rat der EU, 'Erklärungen zur Brüssel I-Verordnung' (2001) IPRax 259, 261.

Ibis Regulation even if the seller's online targeting had no causal influence on the contract.[32] For example, if a tourist from Germany buys a good in a department store in Paris, she may later on sue the seller in Germany (Art. 17(1)(c) of the Brussels Ibis Regulation) and may have German consumer protection law applied (Art. 6 of the Rome I Regulation) if the department store has promoted the respective goods in Germany online, even if the German consumer was unaware of this targeting activity prior to entering into the contract in Paris. This rule of the *Emrek* decision has been criticised as overly consumer-protective.[33] However, given the preceding *Mühlleitner* decision, it seems as a rather plausible next step. If the rules in Art. 17(1)(c) of the Brussels Ibis Regulation and Art. 6 of the Rome I Regulation are no longer limited to distance selling but also extended to local transactions, it would compromise legal certainty to further ask whether the preceding online activity had some causal influence on the contract at hand. In any case, the line of decisions from *Mühlleitner* to *Emrek* is a vivid example of the hypothesis that paradigms of cross-border online sales increasingly influence traditional consumer sales, too.[34]

4 Extra-Territorial Application of EU Consumer Law

Turning to the issue of extra-territorial application of EU consumer law in a digitalised environment, one should notice the interconnection of this issue with the principle of market orientation under Art. 17(1)(c) of the Brussels Ibis Regulation and Art. 6 of the Rome I Regulation discussed already. The lower the requirements for directing business to an EU consumer target market by a non-EU seller, the more the extra-territorial application of EU consumer law will occur just by application of the rules outlined earlier. Indeed, the CJEU follows a kind of long-arm approach in that respect by relaxing the requirements for directing business to a target market under the doctrine of the *Pammer and Hotel Alpenhof* case law: for example the supply of international customer care and adjustable language and delivery options on a website may suffice for the targeting criterion.[35]

In cases that do not fulfil the requirement of directing business to a certain consumer market, one might still ask whether EU consumer law or the consumer law of a specific EU Member State may nonetheless be applied as so-called

32 Case C-218/12 *Emrek* (CJEU, 17 October 2013) para 20ff.

33 See Giesela Rühl, 'The Consumer's Jurisdictional Privilege: On (Missing) Legislative and (Misguided) Judicial Action' in F Ferrari and F Ragno (eds), *Cross-Border Litigation in Europe: The Brussels I Recast Regulation as a Panacea?* (2015) Wolters Kluwer, 67, 90ff.

34 Cf Peter Mankowski and Peter Nielsen, 'Article 17' in U Magnus and P Mankowski (eds), *European Commentaries on Private International Law, Vol I: Brussels Ibis Regulation* (2016) Otto Schmidt, para 68: "The legal development followed the development in marketing techniques, but that must not be equated with letting the grip on traditional marketing techniques slip".

35 *Pammer and Hotel Alpenhof* (n 27) para 83ff.

overriding mandatory provisions (*Eingriffsnormen*) under Art. 9 of the Rome I Regulation.[36] Such rules are defined as

> provisions the respect for which is regarded as crucial by a country for safeguarding its public interests, such as its political, social or economic organisation, to such an extent that they are applicable to any situation falling within their scope, irrespective of the law otherwise applicable to the contract.
>
> (Art. 9(1) of the Rome I Regulation)

While this concept is traditionally focussed on genuine sovereign regulatory law such as, for example, foreign trade legislation, the CJEU has also shown general sympathy for classifying private law as overriding mandatory provisions if its rationale is not only to protect "weak" parties but also to structure markets and to protect social peace. This position should be seen in the light of the fact that the allocation of competences between the EU and the Member States typically mandates the Union to enact private law legislation rather than classical public regulatory law. Consequently, the inclusion of private law into the concept of overriding mandatory provisions strengthens the Union's ability to enact internationally mandatory rules.[37]

This idea was initially developed in the famous *Ingmar* decision for the field of self-employed commercial agents.[38] Here, the Court decided that the mandatory EU law guarantees for commercial agents may also apply in cases where the contract for agency is concluded with a non-EU principal and governed by non-EU law but where the activities of the commercial agent are carried out within the EU. An important rationale for this decision has been that the EU Commercial Agents Directive is not only meant to protect individual agents but also to create a level playing field for all commercial agency activities within the EU.[39] Here, we again find a clear focus on a market-centred approach.

The approach of the *Ingmar* decision has been extended by the *Unamar* case to protective guarantees that go beyond EU standards and are based on Member States' private law.[40] According to the CJEU, such rules may qualify as overriding mandatory provisions in the sense of Art. 9 of the Rome I Regulation if they are not only meant to protect individuals but also structure markets. This approach

36 For further analysis on this point see, with a critical account, Felix Maultzsch, 'Artikel 9 Rom I-VO' in B Gsell, W Krüger, S Lorenz and J Mayer (eds), *beck-online.GROSSKOMMENTAR* (1 February 2021) C.H.Beck, para 27ff.

37 Cf Andrea Bonomi, 'Overriding Mandatory Provisions in the Rome I Regulation on the Law Applicable to Contracts' (2008) 10 YbPIL 285, 294. However, for a strong criticism in this respect see Gunther Kühne, 'Die Parteiautonomie zwischen kollisionsrechtlicher und materiellrechtlicher Gerechtigkeit' in H Krüger and H-P Mansel (eds), *Liber amicorum Gerhard Kegel* (2002) C.H.Beck, 65, 82.

38 Case C-381/98 *Ingmar* [2000] ECR I-9305.

39 Ibid para 23ff.

40 Case C-184/12 *Unamar* (CJEU, 17 October 2013).

may further pave the way for a possible extra-territorial application of consumer law. However, the final decision on this matter remains on the side of the respective EU Member States that have enacted rules which may qualify as having an overriding mandatory nature.[41] One can observe somewhat contradictory approaches in national case law in that respect. For example, French courts are rather open-minded towards an extra-territorial application of French consumer law, especially for consumer loans,[42] while the German courts have so far followed a more restrictive approach.[43] In any case, the option of classifying consumer law as being overriding mandatory provides another example of the shift from a party-centred to a market-centred approach.

5 Trends in Substantive EU Sales Law

The most relevant recent legislation concerning EU sales law is the Consumer Rights Directive (2011)[44] and the new Sale of Goods Directive (2019).[45] While the former has an emphasis on duties to inform and rights of withdrawal (*inter alia*, in distance selling contracts), the latter has a focus on the standards for conformity of the goods and consumer rights in cases of non-conformity. The original proposal of the new Sale of Goods Directive was drafted only for consumer distance sales as a genuine part of the agenda for a digital single market.[46] However, the scope of the final version was extended to all consumer sales since different sets of EU law for online and offline contracts would have caused an undue fragmentation of the law. Nonetheless, the needs of cross-border online markets dominate the content of the new Sale of Goods Directive, thereby reinforcing the observation that paradigms of the digital world tend to "spill over" to traditional consumer sales. In particular, many of the rules in the new Sale

41 See Maultzsch (n 36) para 56.

42 Cass civ (1) 23 May 2006 (2007) 96 Rev crit dr int pr 85.

43 BGH NJW 2006, 762.

44 Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council [2011] OJ L304/64. This directive has been updated, first of all with respect to contracts for the supply of digital content, by art 4 of the Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules [2019] OJ L328/7.

45 Directive (EU) 2019/771 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the sale of goods, amending Regulation (EU) 2017/2394 and Directive 2009/22/EC, and repealing Directive 1999/44/EC [2019] OJ L136/28.

46 For a background and criticism of the former proposal Felix Maultzsch, 'Der Entwurf für eine EU-Richtlinie über den Online-Warenhandel und andere Formen des Fernabsatzes von Waren' (2016) 71 JZ 236, 238.

of Goods Directive mirror parallel rules and standards of the new Directive on the Supply of Digital Content.[47] This approach should manage the increasingly blurred transitions between contracts for the sale of goods and for the supply of digital content, for instance in cases of physical products with extensive digital components (cross-linked cars, smartphones, wearables, etc.).

Focussing on the substance of the digital market paradigms that can be found in recent EU sales law, one should notice two key aspects.

Firstly, we find a shift from the principle of minimum harmonisation which dominated earlier EU consumer law (e.g. the 1999 Sale of Goods Directive),[48] to the principle of full harmonisation embedded both in the Consumer Rights Directive (Art. 4) and the new Sale of Goods Directive (Art. 4). The principle of minimum harmonisation entails EU protective standards as a kind of "floor" that can be exceeded by the national law of the Member States in favour of consumers. In contrast, the principle of full harmonisation not only defines the minimum but also the maximum level of consumer protection that can be required by the Member States as a kind of "ceiling". This regulatory shift has been widely discussed and also criticised in recent years.[49] Amongst other aspects, criticism has focussed on the fact that full harmonisation does not take into account specific interests of certain Member States that might call for even higher protective standards in some fields and does not allow for a regulatory competition between different solutions based on a common minimum of consumer protection. While this criticism certainly has its merits, the major argument of the EU legislator in favour of the shift towards full harmonisation is the perceived need for equality of competition between all businesses in European-wide online markets as a means to boost cross-border supply and consumption.[50] Such a level playing field can only be ensured in a system of full harmonisation. Once more, this regulatory background gives evidence of the fact that current legislative strategies are strongly influenced by a market-centred perspective even at the expense of other advantages that might be connected with alternative strategies such as a principle of minimum harmonisation.

Secondly, one comes across a phenomenon in the new EU instruments that might be called "bonus rules" for consumers. These are rules which cannot fully be explained by legitimate protective needs of consumers but which are rather

47 Supra (n 4).

48 Directive 1999/44/EC of the European Parliament and of the Council of 25 May 1999 on certain aspects of the sale of consumer goods and associated guarantees [1999] OJ L171/12.

49 See Stefan Grundmann, 'Die EU-Verbraucherrechte-Richtlinie Optimierung, Alternative oder Sackgasse?' (2013) 68 JZ 53, 63ff; Carsten Herresthal, 'Die Vorzugswürdigkeit einer europäischen Vertragsrechtsharmonisierung durch optionale Instrumente' in J-U Hahn (ed), *Gemeinsames Europäisches Kaufrecht: Moderner Ansatz oder praxisferne Vision?* (2012) C.H.Beck, 83, 94ff; Maultzsch (n 46) 238.

50 See the Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the online and other distance sales of goods, COM(2015) 635 final, 2ff and 9ff.

aimed at generating a positive general attitude towards (online) consumption and, thereby, at boosting markets.[51] I would like to focus on two examples of such rules.

The first example is the mandatory 14-day right of withdrawal for consumers in distance sale contracts, especially online sales, under Art. 9 of the Consumer Rights Directive. While the parallel right of withdrawal in off-premises contracts is largely undisputed due to the psychological overload typically faced by consumers in such situations, a comparable need of protection is quite often questioned for distance sale contracts.[52] It may well be argued that the alternative of a right to choose between a contract with or without a withdrawal right (at different price levels) would already cover the legitimate interests of consumers in distance sales.[53] By instead implementing a general mandatory right of withdrawal, the European legislator has opted for a special "bonus" for consumers engaging in online consumption.

The second example is the mandatory one-year shift of burden of proof regarding quality defects in favour of consumers according to Art. 11 of the new Sale of Goods Directive. Under this rule,

> [a]ny lack of conformity which becomes apparent within one year of the time when the goods were delivered shall be presumed to have existed at the time when the goods were delivered, unless proved otherwise or unless this presumption is incompatible with the nature of the goods or with the nature of the lack of conformity.

This amounts to a considerable expansion of consumer protection in comparison with Art. 5(3) of the 1999 Sale of Goods Directive, under which the shift of burden of proof was limited to six months, albeit on the principle of minimum harmonisation. On a practical level, the new rule may in many cases be tantamount to a mandatory one-year guarantee for quality and durability.[54] Although this solution might fit into broader aims of sustainability, it deviates from a genuine contractual balancing of interests which would allow for more nuanced options regarding the seller's responsibility as to durability, especially with respect to goods at different price levels.

In summary, there is evidence that EU consumer sales law is indeed shifting away from the idea of consumer law as a means to protect "weak" parties and is

51 Cf Maultzsch (n 5) 17ff; Müller-Graff, 'Ein fakultatives europäisches Kaufrecht als Instrument der Marktordnung?' (n 10) Sellier European Law Publishers, 33ff.

52 Horst Eidenmüller, 'Why Withdrawal Rights?' (2011) 7 ERCL 1; Gerhard Wagner, 'Zwingendes Vertragsrecht' in H Eidenmüller and others (eds), *Revision des Verbraucher-acquis* (2011) Mohr Siebeck, 1, 27ff.

53 However, critical of such an approach Michael Höhne, *Das Widerrufsrecht bei Kaufverträgen im Spannungsverhältnis von Opportunismus und Effektivität* (2016) Mohr Siebeck, 81ff.

54 Cf Maultzsch (n 46) 242.

increasingly focussed on facilitating and boosting (online) markets by creating a kind of carefree consumption environment.[55]

6 Alternative Means of Dispute Resolution and Enforcement of Consumer Rights

While EU consumer law has long focussed on improving the substantive rights of consumers, the Union has more recently taken significant steps to strengthen the practical enforcement of those rights, too. This ties-in with the well-known aversion of consumers to enforce their rights in traditional court procedures which are often complicated, expensive and lengthy. These problems are specifically pertinent in the case of cross-border transactions and affect, in particular, international online contracts. Therefore, the development of efficient, low-threshold and fast means of consumer rights enforcement ranks high in the recent EU consumer law agenda and the latest project of a "New Deal for Consumers".[56]

As a kind of pioneer work, the 2008 Mediation Directive requires EU Member States to facilitate mediation in civil cases.[57] It starts from the premise that mediation is a time- and cost-saving procedure which strengthens the acceptance of conflict resolution by citizens and thereby enhances access to justice for them.[58] While the practical impacts of the mediation instrument have been limited so far, the EU has subsequently started a comprehensive initiative to promote alternative means of dispute resolution (ADR) in consumer disputes. The most important results of this initiative date from 2013 and are the Directive on Consumer ADR (ADR Directive)[59] and the Regulation on Online Dispute Resolution for Consumer Disputes (ODR Regulation)[60] which have to be seen as coordinated measures.[61] The ADR Directive requires EU Member States to establish sufficient institutions for alternative resolution of consumer disputes. In doing so, the Member States can resort to private ADR entities but have to ensure that these

55 Of course, such a development does not come without a price for consumers since it functions like a kind of "compulsory insurance" which will influence the price level of goods and services. For a general account on this mechanism, see Tobias Tröger, 'Inhalt und Grenzen der Nacherfüllung' (2012) 212 AcP 296, 305.

56 For this initiative see <https://ec.europa.eu/info/law/law-topic/consumers/review-eu-consumer-law-new-deal-consumers_en> accessed 10 May 2021.

57 Directive 2008/52/EC of the European Parliament and of the Council of 21 May 2008 on certain aspects of mediation in civil and commercial matters [2008] OJ L136/3.

58 Cf recitals 2ff of the Mediation Directive.

59 Directive 2013/11/EU of the European Parliament and of the Council of 21 May 2013 on alternative dispute resolution for consumer disputes [2013] OJ L165/63.

60 Regulation (EU) 524/2013 of the European Parliament and of the Council of 21 May 2013 on online dispute resolution for consumer disputes [2013] OJ L165/1.

61 For an instructive overview on the content of the two instruments, see Caroline Meller-Hannich, Armin Höland and Elisabeth Krausbeck, '"ADR" und "ODR": Kreationen der europäischen Rechtspolitik. Eine kritische Würdigung' (2013) 22 ZEuP 2014, 8, 17ff and Herbert Roth, 'Bedeutungsverluste der Zivilgerichtsbarkeit durch Verbrauchermediation' (2013) 68 JZ 637, 639ff.

entities meet certain standards of efficiency and quality.[62] The ODR Regulation does not introduce a separate mechanism for online-ADR but merely creates a platform enabling consumers to identify the suitable national ADR institution that is competent for disputes stemming from online sales or service contracts (Art. 2(1) of the ODR Regulation). For this purpose, a European ODR platform that lists all national ADR entities has been established by the EU Commission under Art. 5 of the ODR Regulation.[63] Furthermore, EU law is also tackling the issue of effective redress in cases of dispersed loss. In a recommendation from June 2013, the EU Commission still proposed that all EU Member States should introduce opt-in class actions for monetary relief in mass harm situations.[64] However, the recent developments have moved somewhat away from class actions and towards a solution by representative actions, which is more in sync with the Continental European tradition of law enforcement. Therefore, the EU has recently introduced a Directive on representative actions for the protection of the collective interests of consumers.[65] Finally, a new Directive on better enforcement and modernisation of consumer protection rules puts an emphasis on monetary penalties for businesses which do not comply with the pertinent rules.[66]

All of these new means of dispute resolution and enforcement of consumer rights have been subject to an intensive debate which can only be touched upon briefly at this point. For example, major objections against the consumer ADR initiatives are that the EU Member States will be required to develop and monitor a complex ADR system which is not suitable to enforce mandatory consumer rights and which, as a partial privatisation of the justice system, may impair legal protection by public courts in this area.[67] Therefore, several

62 Among these standards are the requisite qualification and impartiality of the persons handling the complaints (art 6 of the ADR Directive), the transparency of the ADR services offered by the respective entities (art 7 of the ADR Directive), as well as the effectiveness and the fairness of the proceedings (arts 8, 9 of the ADR Directive). In case the outcome of the ADR procedure is binding on the consumer, which is only possible by a respective agreement made between the consumer and the trader after the occurrence of the dispute (art 10 of the ADR Directive), the Member States need to guarantee that the mandatory rights of the consumer are not compromised by the solution (art 11 of the ADR Directive).

63 See <https://ec.europa.eu/info/live-work-travel-eu/consumers/resolve-your-consumer-complaint_en> accessed 10 May 2021.

64 Commission Recommendation 2013/396/EU of 11 June 2013 on common principles for injunctive and compensatory collective redress mechanisms in the Member States concerning violations of rights granted under Union Law [2013] OJ L201/60, 64ff.

65 Directive (EU) 2020/1828 of the European Parliament and of the Council of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC [2020] OJ L409/1.

66 Directive (EU) 2019/2161 (n 44).

67 Horst Eidenmüller and Martin Engel, 'Against False Settlement: Designing Efficient Consumer Rights Enforcement Systems in Europe' (2014) 29 Ohio St J Disp Res 261; Meller-Hannich, Höland and Krausbeck (n 61) 30ff; Roth (n 61) 640ff; Gerhard Wagner, 'Private Law Enforcement through ADR: Wonder Drug or Snake Oil?' (2014) 51 CML Rev 165.

alternatives for efficient enforcement of consumer rights have been suggested. These suggestions range from the introduction of streamlined small-stakes proceedings at local courts[68] to the introduction of consumer class actions.[69] In any case, it seems clear that the newly introduced mechanisms are not, at least not primarily, aimed at enforcing consumer rights in a "legal" fashion but their focus is rather on quick, cheap and standardised solutions that flank the reliability and operability of consumer markets as such. In the case of ADR administered by private bodies and possibly by online tools, this can lead to a kind of "rough justice" that may nonetheless be welcomed as opposed to the danger of a complete failure of consumer rights enforcement in State court systems.[70] In contrast, the approach of the most recent "New Deal for Consumers" with its focus on representative actions and monetary penalties may be analysed as a type of semi-public market surveillance somewhat shifting away from thinking in individual private legal relations.[71]

Notwithstanding the respective advantages and perils of the new instruments, the developments in the field of dispute resolution and enforcement affirm the tendency towards a focus on market protection and facilitation rather than on a thinking in individual private legal relations *stricto sensu*.

7 Private Governance by Contract and Technology

With respect to the phenomenon of private governance[72] by contract and technology for consumer contracts, the rising importance of online intermediary platforms seems to be the most salient development. While many of these platforms, at the same time, also operate as suppliers of goods and services to consumers, their most important function is to act as "market guards" or "market makers".[73] This issue has an impact on different levels of legal relevance.

Firstly, online platforms function as gatekeepers in making decisions as to which suppliers and consumers will be admitted to a respective platform market. In particular, algorithmic models employed by the platform operators may often lead to a subtle shaping of preferences or even to a full or partial denial of

68 Eidenmüller and Engel (n 67).

69 Wagner (n 67).

70 See Gerhard Wagner, 'Die Richtlinie über Alternative Streitbeilegung—Law Enforcement statt mediative Konfliktlösung' (2013) 16 ZKM 104.

71 For further analysis on pitfalls of the approach taken by the proposal, see Tanja Domej, 'Die geplante EU-Verbandsklagenrichtlinie—Sisyphos vor dem Gipfelsieg?' (2019) 27 ZEuP 446.

72 This concept is defined as a type of social ordering which is based on rules and procedures that are set by private actors but are intended to affect the broader public; see Catherine E Rudder, 'Private Governance as Public Policy: A Paradigmatic Shift' (2008) 70 JOP 899.

73 Cf Marco Cian, 'Online Platforms as Gatekeepers to the Digital World—A Preliminary Issue on Business Freedom, Competition and the Need for a Special Market Regulation' (2018) EuCML 209.

consumer access to the platform and its offerings.[74] From a contractual point of view, the acceptable standards of such gatekeeping are only fragmentarily regulated on the EU level.[75] If a certain limitation of access by consumers[76] is based on suspicious criteria, the Directives against discriminatory behaviour in contractual relations[77] may apply. On a cross-border level, the Geo-Blocking Regulation[78] prohibits impairment of access to online interfaces, such as professional websites, on the basis of nationality or place of residence (Art. 3) and also puts a ban on making the general conditions of access to goods or services dependent on these criteria (Art. 4). However, these rules do not amount to a duty to deal with specific customers or to deliver goods to certain states,[79] nor does the compliance with the Geo-Blocking Regulation, in itself, amount to a targeting of certain markets in the sense of Art. 17(1)(c) of the Brussels Ibis Regulation and Art. 6 of the Rome I Regulation.[80] This leads to a rather limited contribution of the Geo-Blocking Regulation to a consumer's right of access to platforms on a practical level.[81] However, there might be some supplementary approaches in national law to tackle the problem of platform access by consumers. For example, the German Federal Constitutional Court has decided that private actors may not exclude individuals without good cause and due process from activities which are (generally) open to the public and the access to which is important for participating in

74 For further discussion on this see Gerhard Wagner and Horst Eidenmüller, 'Down by Algorithms? Siphoning Rents, Exploiting Biases, and Shaping Preferences: Regulating the Dark Side of Personalized Transactions' (2019) 86 U Chi L Rev 581.

75 From the perspective of competition law, see the recent Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act), COM(2020) 842 final.

76 Regarding access of businesses to platforms, the so-called P2B Regulation sets further standards which focus mainly on transparency issues: Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services [2019] OJ L186/57.

77 Council Directive 2000/43/EC of 29 June 2000 implementing the principle of equal treatment between persons irrespective of racial or ethnic origin [2000] OJ L180/22 and Council Directive 2004/113/EC of 13 December 2004 implementing the principle of equal treatment between men and women in the access to and supply of goods and services [2004] OJ L373/37.

78 Regulation (EU) 2018/302 of the European Parliament and of the Council of 28 February 2018 on addressing unjustified geo-blocking and other forms of discrimination based on customers' nationality, place of residence or place of establishment within the internal market and amending Regulations (EC) 2006/2004 and (EU) 2017/2394 and Directive 2009/22/EC [2018] OJ L60 I/1 (Geo-Blocking Regulation).

79 Cf recitals 18(3) and 27 of the Geo-Blocking Regulation.

80 See art 1(6) of the Geo-Blocking Regulation and supra III on the role of directing business on the level of international jurisdiction and conflict of laws. For further analysis on this see Dieter Martiny, 'Private International Law Aspects of Geo-blocking and Portability' in C Benicke and S Huber (eds), *National, International, Transnational: Harmonischer Dreiklang im Recht. Festschrift für Herbert Kronke* (2020) Ernst und Werner Gieseking, 351, 356ff.

81 For further discussion of this problem see Marc Dietrich, *Die situative Anwendung von Art 17 Brüssel Ia-VO und Art 6 Rom I-VO* (2020) Mohr Siebeck 137ff.

social life.[82] Although the case at hand was from the offline world and concerned the access to soccer stadiums, it may well be argued that some online platforms nowadays are at least as important for social life as sporting events. Along that line, the decision of the Federal Constitutional Court could be the starting point of a stricter legal scrutiny on online platform operators' decisions as to admission to the platform.

Secondly, the phenomenon of online platforms fosters thinking in overall customer relations at the expense of the traditional legal thinking about the specific rights and duties in individual (sales) contracts. This is because many platform operators extract considerable economic value from the long-term acquisition of consumer data in the course of platform activities. One might even argue that, in some cases, the entering into contracts involving specific goods or services with consumers is no longer an end in itself for businesses, but rather a mere means to create more important surplus in a data-driven market structure.[83] It is on par with this assumption that many of the leading platforms are often more generous with respect to the handling of specific contracts than the standards of EU consumer law would require them to be (e.g. with respect to the terms of withdrawal rights). All of this puts pressure on the declining relevance of legal rights and obligations in specific contracts to the benefit of an overall market management.

Thirdly, private rulemaking by online intermediary platforms for the transactions carried out via the platforms poses important issues of how to classify these rules (terms of use, payment systems, feedback systems, dispute resolution clauses, etc.) from a legal point of view. The traditional account, which is, amongst others, still followed by the German courts, classifies such provisions set by the platform operator as standard terms even if this operator is not a party to the sales contracts entered into by suppliers and consumers via the platform.[84] Consequently, the provisions are, in principle, subject to a review under the EU Unfair Contract Terms Directive.[85] However, an emerging opposing view analyses these terms not from a contractual perspective but considers them as a means of market organisation by a third-party actor.[86] According to this view, the terms of use provided for by platform operators should not be subject to a legal review on a contractual level but merely under the rules of competition law if the respective platform operator gains a dominant position in the market.[87] If

82 BVerfG NJW 2018, 1667—*Stadionverbot*.

83 Critical of this development and in favour of a general "right to anonymity" for consumers in the digital world Wagner and Eidenmüller (n 74) 607ff.

84 Cf BGH NJW 2011, 2421 para 21 and OLG Hamm MMR 2015, 25, 27.

85 Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts [1993] OJ L95/29.

86 See Heike Schweitzer, 'Digitale Plattformen als private Gesetzgeber: Ein Perspektivwechsel für die europäische "Plattform-Regulierung"' (2019) 27 ZEuP 1, 7ff.

87 See, in that context, the recent amendment of German competition law in GWB (*Gesetz gegen Wettbewerbsbeschränkungen*) sec 19a that deals with actors of "outstanding cross-market significance for the competition".

this view were to prevail, contractual thinking would once more step behind the perspective of overall market structures.

Finally, an intensive debate has emerged on how to cope with the phenomenon that, via online intermediary platforms, consumers often no longer enter into contracts with large professional suppliers, but rather with small- and medium-sized enterprises or even with consumers on the supplier side, too.[88] This development could compromise the effectiveness of EU consumer law, since these rules require a B2C transaction and do not apply to C2C contracts. Against that background, a recent amendment to the Consumer Rights Directive requires platform operators to ensure strict transparency as to who the consumer's partner is in contracts entered into via the platform.[89] Going even further, the problem of intertwined legal relations in the platform business has led to policy proposals according to which platform operators should themselves be liable for any breaches of contracts entered into via the platform. This liability would apply even though the platform operator has made clear that it will function only as an intermediary and not as a contractual partner to the platform transactions. Most notably, the Model Rules on Online Intermediary Platforms, adopted by the European Law Institute (ELI) in 2020,[90] suggest such a liability on the part of platform operators if the operator has a "predominant influence" over the suppliers offering goods or services on the platform (Art. 20 of the ELI Model Rules).[91] However, it has been criticised that such an approach would unduly compromise established contractual principles, in particular the idea of privity of contract (*Relativität der Schuldverhältnisse*).[92] The question whether a platform operator, in addition to its role as an intermediary, is liable in cases of a breach of the contracts entered into via the platform should, in principle, be left to a free contractual solution (e.g. by the means of guarantees extended to consumers by the platform operator). If, in contrast, the view of the ELI Model Rules were to prevail, this would once more mark a triumph of market ordering over classical contractual thinking in the field of digitalised consumer contracts.[93]

88 For an in-depth analysis of this problem, see Caroline Meller-Hannich, *Wandel der Verbraucherrollen: Das Recht der Verbraucher und Prosumer in der Sharing Economy* (2019) Duncker und Humblot; see also Christoph Busch and others, 'The Rise of the Platform Economy: A New Challenge for EU Consumer Law?' (2016) EuCML 3.

89 See Directive (EU) 2019/2161 (n 44) art 4(5)(1).

90 European Law Institute, 'Report of the European Law Institute: Model Rules on Online Platforms' (2019) <www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Model_Rules_on_Online_Platforms.pdf> accessed 10 May 2021.

91 For a further explanation of this rule see Christoph Busch and others 'The ELI Model Rules on Online Platforms' (2020) EuCML 61, 65 and Hans Schulte-Nölke, 'Plattformverträge und Vertrauensschutz' in U Blaurock and F Maultzsch (eds), *Vertrauensschutz im digitalen Zeitalter* (2020) Nomos, 167, 211ff.

92 Felix Maultzsch, 'Contractual Liability of Online Platform Operators: European Proposals and established Principles' (2018) 14 ERCL 209, 227ff; see also Andreas Engert, 'Digitale Plattformen' (2018) 218 AcP 304, 315ff.

93 Cf for the link between a platform operator's liability by virtue of a "predominant influence" and schemes of public law regulation Maultzsch (n 92) 224ff.

8 Conclusions

The preceding analysis has shown that the process of digitalisation fosters a shift of paradigms in EU consumer contract law. The classical party-centred view with its focus on adequately levelling the parties' interests and protecting "weak" parties to secure their autonomous decision-making has been increasingly replaced by a market-centred approach with a focus on protecting and facilitating (online) markets by the means of contract law.[94] On the level of international jurisdiction and conflict of laws, this shift is typified by an orientation of the relevant connecting factors on market activities and by the tendency to an extended geographical scope of application.[95] With respect to substantive sales law, one can witness a shift to standardisation of contractual relations by the means of full harmonisation in EU law and by the phenomenon of "bonus rules" for consumers that abandon the idea of mere consumer protection in favour of facilitating and boosting consumption in online markets.[96] This process is flanked on a procedural level by an enhancement of ADR procedures and collective representative actions which favour fast and standardised solutions instead of an enforcement of individual rights *stricto sensu*.[97] In the field of online intermediary platforms, a thinking in terms of separated contracts is increasingly replaced by a digitalised management of consumer relations by the platform operators. This, in turn, induces policy proposals to compromise established contractual principles such as the idea of privity of contract for the sake of intensifying platform operators' liability towards consumers.[98] Finally, the market-focussed perspective of digitalised sales contracts also has a strong influence on the development of EU law applicable to traditional offline sales contracts. This has resulted in an increasing domination of digital paradigms over consumer sales law in general.

94 See supra Section 2.
95 See supra Sections 3 and 4.
96 See supra Section 5.
97 See supra Section 6.
98 See supra Section 7.

Part IV
Media Law

7 Law of Digitality

Media Law—U.S. Perspectives

Ellen P. Goodman

1 Digital Platform Disclosure Obligations for Political and Commercial Advertising

One of the first U.S. attempts to translate analog transparency regimes to the digital world was the Honest Ads Act, introduced for a second time in March 2019.[1] Seeking to uphold the principle that "the electorate bears the right to be fully informed," the Act would close the digital loophole for online campaign ads. Platforms would have to reveal the identities of political ad purchasers.[2] While the Honest Ads Act is stalled in Congress, several states have moved forward to adopt similar legislation, including California, Maryland, Washington, and New York.

California's Social Media DISCLOSE Act of 2018[3] requires political adverting sponsorship disclosures. New York's Democracy Protection Act of 2018[4] requires paid political ads to display disclaimers stating whether the ad was authorized by a candidate as well as who actually paid for the ad. Washington state has altered its campaign finance laws to require disclosure of the names and addresses of political

1 HR 2529, 116th Cong 2019–2020; s 1356, 116th Cong 2019–2020; The For the People Act 2019 (HR 1) incorporated the Honest Ads Act in sections 4026 and 4028.

2 See Mark Warner's bill summary <www.warner.senate.gov/public/index.cfm/the-honest-ads-act?page=1> accessed 2 October 2020; see also Sen Mark Warner, 'Potential Policy Proposals for Regulation of Social Media and Technology Firms' White Paper (draft) 2018 <https://regmedia.co.uk/2018/07/30/warner_social_media_proposal.pdf> accessed 2 October 2020; for a more far-reaching proposal see Abby K Wood and Ann M Ravel, 'Fool Me Once: Regulating "Fake News" and Other Online Advertising' (2018) 91 S Cal L Rev 1227 (proposing disclosures also for unpaid ads among other communications).

3 Social Media DISCLOSE Act, AB 2188, Gen Assemb 92nd Sess (Cal 2018), AB 864 (Cal 2019) <https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB2188> accessed 2 October 2020.

4 Democracy Protection Act, AB 09930, Gen Assemb (NY 2018) (amending definition of "political communication" in NY 17 CL §14–106 and adding section(a) to §14–106; §14–107(b)2–3 requiring digital records of online platform independent expenditures).

DOI: 10.4324/9781003283881-12

ad sponsors and the cost of advertising.[5] Canada has passed a law requiring that platforms publish the verified real names of ad purchasers.[6]

Disclosures intended for intermediaries can also be found in all of the proposed and adopted campaign ad transparency legislation. The Honest Ads Act would require platforms to maintain a public ad repository of all political advertisers that have spent more than $500 on ads or sponsored posts. Canada's political advertising law also mandates an ad repository. California's DISCLOSE Act requires political campaign advertisers to list their top three contributors and platforms to maintain a database of political ads run in the state.[7] New York's Democracy Protection Act mandates that political ads be collected in an online archive maintained by the State Board of Elections.[8] Washington state requires disclosure of "the geographic locations and audiences targeted, and total number of impressions generated by the advertisement or communication."[9]

Maryland's law,[10] currently enjoined by a federal judge who found First Amendment violations,[11] goes further than New York's or California's by man-

5 HB 2938, 65th Leg, Reg Sess (Wash 2018).

6 Election Modernization Act SC 2018, c 31 (Can); akin to the situation in Washington state, Google pulled or blocked all ads that fell within C-76's purview ahead of federal elections in March 2019: Tom Cardoso, 'Google to Ban Political Ads Ahead of Federal Election, Citing New Transparency Rules' (Globe and Mail, 4. March 2019) <www.theglobeandmail.com/politics/article-google-to-ban-political-ads-ahead-of-federal-election-citing-new/> accessed 2 October 2020.

7 Social Media DISCLOSE Act, AB 2188, Gen Assemb, 92nd Sess (Cal 2018), AB 864 (Cal 2019), which passed the California Senate Elections Committee and was before the Appropriations Committee as of July 2, 2019, proposes amendments to AB 2188 to further define "online platform disclosed advertisements" and offer additional definitional clarity. AB 2188 defines "online platforms" as websites and digital applications that sell advertising directly to advertisers. It does not, however, apply to websites or apps that *only* display advertisements sold via another platform. The Social Media DISCLOSURE Act works in tandem, so to speak, with the California Consumer Privacy Act 2018, which gives residents the right to know what data businesses collect about them as well as the ability to request that they delete the information, and is expected to take effect in 2020.

8 Democracy Protection Act, AB 09930, Gen Assemb (NY 2018) (amending definition of "political communication" in NY 17 CL §14–106 and adding section(a) to §14–106; §14–107(b)2–3 requiring digital records of online platform independent expenditures).

9 Political Advertising, 390 WAC §18–050 (2018); in response to the new Washington law, Google pulled all covered ads. Jim Brunner and Christine Clarridge, 'Why Google Won't Run Political Ads in Washington State for Now' (*Seattle Times*, 7 June 2018) <www.seattletimes.com/seattle-news/google-halts-political-ads-in-washington-state-as-disclosure-law-goes-into-effect/> accessed 2 October 2020.

10 Online Electioneering Transparency and Accountability Act, SB 875/HB 981, Gen Assemb, Reg Sess (Md 2018), Md Code Ann, Elec Law § 13–405; see also Michael Dresser, 'Google No Longer Accepting State, Local Election Ads in Maryland as Result of New Law' (*Baltimore Sun*, 29 June 2018) <www.baltimoresun.com/politics/bs-md-google-political-ads-20180629-story.html> accessed 2 October 2020.

11 *Wash Post et al v McManus et al* 355 F Supp 3d 272 (D Md 2019) (holding that the law was overbroad among other infirmities); see also Letter from Lawrence J Hogan, Governor of Md, to Thomas V Mike Miller, Jr, President of the S of Md, and Michael E Busch, Speaker of the H of Md (25 May 2018) <https://governor.maryland.gov/wp-content/uploads/2018/05/EWS-HB981-SB875-Online-Electioneering.pdf> accessed 8 October 2020 (voicing support for the core goals of the new law but declining to sign the bill on constitutional grounds, and thereby allowing the law to pass without his signature).

dating more extensive disclosure of ad reach—beyond total ad impressions—under the state inspection requirement power given to the Board of Elections.[12] Several other states, including Wyoming[13] and Vermont,[14] have simply extended preexisting campaign finance laws to digital advertisers. Without comprehensive federal legislation, political advertising regulation will remain balkanized.[15]

By all accounts, the impetus for the post-2016 wave of disclosure laws pertaining to digital ads was the revelation of foreign election interference by Russia. The new laws are therefore obviously geared toward mitigating against similar future manipulation efforts and to that extent have implications for non-U.S. network platform advertisers. However, as already mentioned, new public laws have no juridical bearing on digital advertising outside of the U.S. At the same time, the platforms like to make their approaches as globally uniform as possible. Facebook first tested its new self-imposed disclosure practices in Canada before rolling them out in the U.S.[16] In response to Washington State's ad disclosure requirements, Facebook decided to ban political advertisements altogether in that state, and this became an approach that Twitter took up nationally; it's possible that the platforms will move in this direction globally.

2 Digital Platform Disclosure Obligations for Deep Fakes and Bots

Bots have enabled massive messaging campaigns that disguise authorship, and in this way increase the perceived value or strength of an opinion.[17] A substantial number of tweeted links are bots and fake accounts designed to flood the information space with an opinion expressed so frequently, people believe it.[18] Deep

12 The Maryland law, like New York's and California's, builds on existing campaign finance law. It includes general reporting and disclaimer requirements including the identity of the ad purchaser(s), a digital copy of the ad, and the issue or candidate on behalf of which it was run. Md Code Ann, Elec Law §13–405.1. Within 48 hours' notice, sites hosting online ads must disclose "an approximate description of the geographic locations where the [ad] was disseminated," "an approximate description of the audience that received or was targeted to receive the [ad]," and "the total number of impressions generated by the [ad]"; Md Code Ann, Elec Law, §13–405(c)(1)-(2).

13 Act No 3, SF0018, 65th Leg, Gen Sess (Wyo 2019).

14 Act No 129, H283, Gen Assemb (Vt 2018).

15 In 2018, the Federal Election Commission accepted public comment on whether it should apply broadcast television and radio disclosure obligations on online audio and video political advertising. Public hearings on the same question followed. See Internet Communication Disclaimers and Definition of "Public Communication," 83 Fed Reg 58, 12864 (26 Mar 2018). However, the FEC has not had a quorum of commissioners and is essentially not functioning.

16 Casey Newton, 'Facebook Announces New Advertising Disclosures Days before Congressional Hearings' (*The Verge*, 27 October 2017) <www.theverge.com/2017/10/27/16560792/|facebook-ad-disclosures-political-advertising-russia> accessed 8 October 2020.

17 Renee DiResta, 'Computational Propaganda: If You Make It Trend, You Make It True' (2018) 106 The Yale Rev 4, 12–29.

18 Stefan Wojcik and others, 'Bots in the Twittersphere' (*Pew Res Ctr*, 9 April 2018) <www.pewinternet.org/2018/04/09/bots-in-the-twittersphere/(finding two-thirds of tweeted links were bots)> accessed 8 October 2020; see also Madeline Lamo and M Ryan Calo, 'Regulating Bot Speech' (2019) 66 UCLA L Rev 988.

fakes create fraudulent impressions of authorship through ventriloquy, using AI to fake what has been said or done.[19] Proposed and adopted laws to address deep fakes and bot-generated speech seek to ensure that people are informed about who is speaking to them (in the case of bots) and whether what they are sensing is real (in the case of deep fakes).

California SB 1001 makes it illegal for a bot to communicate with someone with "the intention of misleading and without clearly and conspicuously disclosing that the bot is not a natural person," and requires removal of offending accounts.[20] It requires that any "automated online ['bot'] account" identify itself as such if it is being used to engage a person in California in order to influence them to either make a purchase or vote. Notably, the law makes clear that it "does not impose a duty on service providers of online platforms."

At the federal level, Senator Feinstein has introduced the Bot Disclosure and Accountability Act to clamp down on the use of social media bots by political candidates. The bill would prevent candidates, their campaigns, and any other political group, from using bots as a type of political advertising. The FTC would be given power to direct the network platforms to develop policies requiring the disclosure of bots by their creators/users.[21] Hewing to the California example, Sen. Mark Warner has proposed to require platforms to identify inauthentic accounts and determine the origin of posts and/or accounts.[22]

These bills, if enacted, would be limited to communications within the jurisdiction of the United States. As with all internet governance interventions, there is the potential that the platforms would conform their behavior globally to the most demanding standards for the sake of simplicity and uniformity.[23] Indeed, when Mark Zuckerberg has spoken publicly about "new rules for the internet," he has referenced proposals such as the French content review standards as if they would apply everywhere. In a recent op-ed, he called for countries to adopt a GDPR-like regulation so as to introduce a "common framework" across borders.

19 Council on Foreign Relations, 'Deep Fakes and the Next Generation of Influence Operations' (14 November 2018) <www.cfr.org/event/deep-fakes-and-next-generation-influence-operations> accessed 8 October 2020.

20 Bolstering Online Transparency Act (BOT), SB 1001, Gen Assemb (Cal 2018).

21 Bot Disclosure and Accountability Act 2018, S 3127, 115th Cong; A similar bill was introduced in the California Assembly by Marc Levine (D-San Rafael), AB 1950, Gen Assemb (Cal 2018).

22 Warner (n 2).

23 Mark Zuckerberg, 'The Internet Needs New Rules. Let's Start in These Four Areas' (*Wash Post*, 30 March 2019) <www.washingtonpost.com/opinions/mark-zuckerberg-the-internet-needs-new-rules-lets-start-in-these-four-areas/2019/03/29/9e6f0504-521a-11e9-a3f7-78b7525a8d5f_story.html> accessed 8 October 2020. Zuckerberg's op-ed was also published in Ireland. Mark Zuckerberg, 'Yes, We Need Regulation—But We Can't do It on Our Own' (*Indep*, 30 March 2019) <www.independent.ie/business/technology/mark-zuckerberg-yes-we-need-regulation-but-we-cant-do-it-on-our-own-37967115.html> accessed 8 October 2020.

3 Government Access Obligations Under the First Amendment's Public Forum Doctrine

In *Knight First Amendment Inst. at Columbia Univ. v. Trump*, 302 F. Supp. 3d 541 (S.D.N.Y. May 23, 2018), a group of seven citizens sued President Trump for blocking them on Twitter. The claim was that the President, qua government, engaged in viewpoint discrimination in a "public forum" in violation of the First Amendment. The court ruled that President Trump's Twitter feed, which is used consistently for government business, constitutes a "designated public forum" much like a public park where people congregate to express their views.[24] The court distinguished the "interactive space" of the feed, where a user can interact with the President's tweets by responding, retweeting, etc., from Trump's original tweets, which are government speech and not subject to a First Amendment claim.

On appeal in the Second Circuit, a unanimous three-judge panel upheld the district court, determining that "the First Amendment does not permit a public official who utilizes a social media account for all manner of official purposes to exclude persons from an otherwise-open online dialogue because they expressed views with which the official disagrees."[25] The court declared that "once the President has chosen a platform and opened up its interactive space to millions of users and participants, he may not selectively exclude those whose views he disagrees with." The court was quick to add that "not every social media account operated by a public official is a government account," and that "in most instances [similar cases will] be a fact-specific inquiry," depending on how the official describes and uses the account, what features are made available, and how others regard and treat the account. The Second Circuit ruling, as a First Amendment case, has no foreseeable extraterritorial effect.

4 Digital Platforms' Exposure to Liability as Publishers and Distributors

Section 230 of the Communications Decency Act 1996 (CDA)[26] protects online intermediaries like social media platforms from liability for transmitting third-party

24 See *Packingham v North Carolina* 582 US (2017) (Kennedy J, describing social media as "the modern public square" and a "protected space").

25 *Knight First Amendment Institute v Trump*, No 18–1691 (2d Cir 2019). The government petitioned for rehearing en banc on August 23, 2019. Shortly after the Second Circuit ruling upholding the District Court, former state assemblyman Dov Hikind (D) and New York congressional candidate Joseph Saladino separately sued Rep. Alexandria Ocasio-Cortez (D-NY) over being blocked from her personal Twitter account. Josh Bowden, 'Ocasio-Cortez Sued Over Twitter Blocks' (*The Hill*, 9 July 2019) <https://thehill.com/homenews/house/452327-ocasio-cortez-sued-over-twitter-blocks> accessed 8 October 2020; see, for example, Compl, *Hikind v Ocasio-Cortez*, No 1:19-cv-03956 (EDNY 9 July 2019).

26 The key portion of the provision reads, "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." 47 USC § 230(c)(1).

content. The clear legislative intent behind Section 230 was to encourage content moderation while allowing intermediaries the leeway to experiment with moderation strategies.[27] At a time when internet technologies were young and marginal to the circulation of speech, Section 230 was crafted to give pioneers of early internet technologies the room to innovate.[28]

Senator Ron Wyden—one of the authors of Section 230—likened the immunity to both a shield and a sword.[29] It protects internet platforms from liability for the third-party content they host, while at the same time empowering the platforms to moderate and curate content freely.[30] In either case, whether moderating or failing to moderate, the platform is not treated as the publisher and therefore is not subject to typical publisher responsibilities.[31] Section 230 is the most robust safe harbor provision of its kind in terms of the activities it covers and the scope of immunity it offers.

There are exceptions to Section 230 immunity.[32] There is no immunity from liability associated with federal criminal law, intellectual property (which is governed by statutes like the Digital Millennium Copyright Act), and certain digital communications laws. Courts too have made clear that Section 230 protections

27 See Danielle Keats Citron and Benjamin Wittes, 'The Internet Will Not Break: Denying Bad Samaritans § 230 Immunity' (2017) 86 Fordham L Rev 401, 404; Ellen P. Goodman and Ryan Whittington, 'Section 230 of the Communications Decency Act and the Future of Online Speech' (Policy Paper No 20, The German Marshall Fund of the United States, August 2019) 5–6 <www.gmfus.org/sites/default/files/publications/pdf/Goodman%20%20Whittington%20-%20Section%20230%20paper%20-%209%20Aug.pdf> accessed 8 October 2020.

28 See Goodman and Whittington (n 27) 3–4 ("Combatting the Moderators' Dilemma").

29 For more background on Section 230 see Danielle Keats Citron and Benjamin Wittes, 'The Problem Isn't Just Backpage: Revising Section 230 Immunity' (2018) 2 Geo L Tech Rev 453; Goodman and Whittington (n 27).

30 Courts have consistently affirmed that viewpoint neutrality in curation and moderation is not a prerequisite for Section 230 immunity. See, for example, *Prager University v Google LLC*, 19-cv-340667 (Cal Superior Ct 2019) (holding that YouTube's placing of certain Prager University's videos in "restricted mode," and demonizing others, on the alleged basis of an anti-conservative bias "is expressly covered by section 230"); *Force v Facebook Inc*, No 18–397 (2d Cir 2019) ("We do not mean that Section 230 requires algorithms to treat all types of content the same. To the contrary, Section 230 would plainly allow Facebook's algorithms to, for example, de-promote or block content it deemed objectionable.").

31

> No provider or user of an interactive computer service shall be held liable on account of—any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable.
>
> 47 USC § 230(c)(2)(A)

32 See 47 USC § 230(e).

do not apply to platforms that participate in the development, creation, or proactive facilitation of unlawful content.[33]

Once internet platforms became so dominant in controlling speech flows, it was inevitable that Section 230 would come under pressure. The first major contraction of Section 230 came with the 2018 law Allow States and Victims to Fight Online Sex Trafficking Act (FOSTA). FOSTA, along with the Stop Enabling Sex Trafficking Act (SESTA), expanded federal criminal liability for sex trafficking. FOSTA/SESTA allows for civil actions and state criminal prosecutions to go forward against internet services for violating federal sex trafficking laws.[34] In short, the laws make intermediaries liable for "knowingly assisting, supporting or facilitating a sex trafficking violation." FOSTA/SESTA applies to U.S. citizens who engage in human trafficking wherever they are.

4.1 Judicial Interpretations of Section 230

Section 230 continues to be interpreted broadly.[35] Two cases from 2019 are illustrative.

33 *Fair Hous Council v Roommates*, 521 F 3d 1157 (9th Cir 2008) (holding that platforms that engage in the creation or development of unlawful material will not get Section 230); *FTC v Accusearch*, 570 F3d 1187 (10th Cir 2009) (holding that a "service provider is 'responsible' for the development of offensive content if it specifically encourages development of what is offensive about the content"); *Oberdorf v Amazon.com Inc*, 930 F3d 136 (3d Cir 2019) (holding that Amazon is a legally responsible for a third party vendor's sale of a defective product via Amazon Marketplace under the Pennsylvania products liability statute, and that plaintiff's claims were not barred by Section 230); *Jane Doe No 14 v Internet Brands, Inc, DBA Modelmayhem.com*, No 12–56638 (9th Cir 2016) (holding that Section 230 did not bar plaintiff's failure-to-warn claim against Model Mayhem for not notifying users that rapists were finding victims on the site because said claim does not treat Model Mayhem as a "publisher or speaker"); *Force v Facebook* (n 30):

> Plaintiffs seek to hold Facebook liable for "giving Hamas a forum with which to communicate and for actively bringing Hamas' message to interested parties." But that alleged conduct by Facebook falls within the heartland of what it means to be the "publisher" of information under Section 230(c)(1). So, too, does Facebook's alleged failure to delete content from Hamas members' Facebook pages.

34 47 USC § 230(e)(5). In addition, it created at Section 230 exemption for state law criminal sex-trafficking prosecution charges.

35 See, for example, *FTC v LeadClick LLC*, 838 F3d 173–175 (2d Cir 2016); *Marshall's Locksmith v Google*, LLC, 925 F3d 1263, 1267 (DC Cir 2019); *Doe v Backpage.com, LLC*, 817 F 3d 12, 18 (1st Cir 2016); *Jones v Dirty World Entm't Recordings, LLC*, 755 F3d 398, 408 (6th Cir 2014); *Doe v MySpace*, 528 F3d 413, 418 (5th Cir 2008); *Almeida v Amazon*, 456 F3d 1316, 1321 (11th Cir 2006); *Carafano v Metrospace*, 339 F3d 1119, 1123 (9th Cir 2003); *Zeran v AOL*, 129 F3d 327, 330 (4th Cir 1997); *Daniel v Armslist, LLC*, 2019 WI 47 (Wis Sup Ct 2019).

4.1.1 Herrick v. Grindr LLC

Herrick v. Grindr, involved an "e-personation" attack—what has been called "malicious catfishing"—on Mr. Herrick via a fraudulent Grindr post from an ex-boyfriend.[36] The social networking and dating app failed to respond to Herrick's multiple requests for relief from the thousands of unsolicited online inquiries. He sued Grindr under a theory of product liability in an attempt to avoid a Section 230-based defense. He claimed that he was not suing Grindr for its role as a publisher of third-party content but rather for its poor "management of its users." He took aim at Grindr's design and operation of the app (i.e. inadequate safety measures). The district court ruled in favor of Grindr twice on Section 230 grounds[37] and the Court of Appeals for the Second Circuit affirmed.[38]

The Second Circuit confirmed that "interactive computer services" covered by Section 230 include "social networking sites . . . and online matching services . . . which, like Grindr, provide subscribers with access to a common server." Rejecting Herrick's attempt to circumvent the Section 230 issue, the court said that the perpetrator's "online speech is precisely the basis of his claims that Grindr is defective and dangerous. Those claims are based on information provided by another information content provider and therefore satisfy the second element of § 230 immunity." The court also refused to entertain the plaintiff's innovative theory that Grindr's publication of geolocation information constituted content creation. The court noted that such information was produced by a user-generated, real-time, automated process. Finally, the plaintiff's arguments premised on Grindr's alleged defects of design and operation failed. The court held that "the manufacturing and design defect claims seek to hold Grindr liable for its failure to combat or remove offensive third-party content, and are barred by § 230."

4.1.2 Force v. Facebook, Inc.

Even more forceful in its affirmation of Section 230's scope is the recent *Force v. Facebook*, also coming out of the Second Circuit.[39] The case is one of several involving lawsuits alleging material support for terrorism on the part of network

36 *Herrick v Grindr, LLC*, 17-cv-932 (SDNY 2017). For a detailed account of the facts by the plaintiff's attorney, see Carrie Goldberg, 'Herrick v. Grindr: Why Section 230 of the Communications Decency Act Must Be Fixed' (*Lawfare*, 14 August 2019) <www.lawfareblog.com/herrick-v-grindr-why-section-230-communications-decency-act-must-be-fixed> accessed 15 October 2020.

37 *Herrick v Grindr LLC*, 17-cv-932-VEC (SDNY 2018).

38 *Herrick v Grindr LLC*, No 18–396 (2d Cir 2019).

39 *Force v Facebook* (n 30). For background leading up to the Second Circuit de novo review, see Sarah Grant, 'Second Circuit Hears Argument on Facebook's Liability for Hamas Attacks' (*Lawfare*, 6 March 2019) <www.lawfareblog.com/second-circuit-hears-argument-facebooks-liability-hamas-attacks> accessed 15 October 2020.

platforms.[40] In *Force*, the Second Circuit became the first federal appellate court to rule that Section 230 bars civil terrorism claims against social media companies.[41] Perhaps more importantly, Force confirms that Section 230 immunity applies to platforms even when their moderation processes are faulty.

Here, families of the victims of a Hamas terror attack in Israel sought to hold Facebook liable under the federal Anti-Terrorism Act (ATA) for providing Hamas with a forum to communicate. The plaintiffs asserted various federal anti-terrorism claims against Facebook, alleging, *inter alia*, that Facebook's provision of a forum for Hamas to communicate purportedly enabled the attacks. In 2017 the lower court dismissed the suit, ruling that "Facebook's choices as to who may use its platform are inherently bound up in its decisions as to what may be said on its platform," meaning that the alleged misconduct (i.e. failure to remove objectionable material and bad actors) necessarily involves "publishing" activity protected under Section 230.[42]

The appeals court held that "a defendant will not be considered to have developed third-party content unless the defendant directly and 'materially' contributed to what made the content itself 'unlawful.'" Since Facebook did not edit or suggest edits for Hamas' content, it was not a developer. Furthermore, its algorithms did not vitiate immunity. Making content available is central to the "publisher" function and does not amount to "developing" content. The court rejected the plaintiff's contention that use of algorithmic processes made Facebook a non-publisher and thus outside the scope of Section 230. In sum, the Force court determined that Facebook's conduct sat squarely within the "publisher" definition of Section 230. Facebook was not a developer of Hamas content, its use of algorithmic processes did not jeopardize its publisher status, and finally, adequacy in content moderation is not a prerequisite for Section 230 immunity.

The dissenting/concurring opinion by Chief Judge Katzmann in *Force v. Facebook* has also received significant attention.[43] Katzmann suggests that by connecting terrorists through algorithmic friend suggestions, Facebook had exceeded what Section 230 was meant to cover. He argued, *inter alia*, that "connecting" is not "publishing," and furthermore, that "publisher" and "platform" are distinct, the latter being the provider of "connections" rather than content. To support his argument, the dissent drew an analogy to a telephone conversation,

40 See, for example, *Taamneh v Twitter, Inc*, No 17-cv-04107-EMC (ND Cal 2018); *Cain v Twitter Inc.*, No 17-cv-02506-JD (ND Cal 2018); *Crosby v Twitter, Inc.*, 303 F Supp 3d 564 (ED Mich 2018); *Pennie v Twitter, Inc*, 281 F Supp 3d 874 (ND Cal 2017).

41 In both *Fields v Twitter*, No 16–17165 (9th Cir 2018) and *Crosby v Twitter* (n 40) the courts merely held that the plaintiffs in those cases—victims of an ISIS attack in Jordan and the Pulse nightclub shooting in Florida, respectively—did not demonstrate a sufficient causal link between the social media companies and the harm suffered by the plaintiffs.

42 *Force v Facebook*, 16-cv-5158-NGG-LB (EDNY 2017).

43 *Force v Facebook* (n 30) (Katzman, CJ dissenting from Parts I and II).

stating that it doesn't make sense to characterize the conversationalists involved as "publishers" as opposed to a more active and involved function.[44]

Suppose that you are a published author. One day, an acquaintance calls. "I've been reading over everything you've ever published," he informs you. "I've also been looking at everything you've ever said on the Internet. I've done the same for this other author. You two have very similar interests; I think you'd get along." The acquaintance then gives you the other author's contact information and photo, along with a link to all her published works. He calls back three more times over the next week with more names of writers you should get to know.[45]

While failing to prevail in this case, the dissent could gain traction in revisions to Section 230 being considered in Congress.

4.2 Territorial Question

When the Eastern District of New York first dismissed the *Force* case,[46] the *Force* plaintiffs attempted to argue that Facebook was "improperly attempting to apply Section 230(c)(1) extraterritorially." The statute lacks explicit indicia of extraterritorial application, so the court looked to the statute's "focus." The plain text of 230(c)(1) does not "cabin" the immunity provisions "based on either the location of the content provider or the user or provider of the interactive computer service." The court reasoned that location was, in fact, irrelevant to the application of Section 230 and that, "[g]iven the statutory focus on limiting liability, the location of the relevant 'territorial events' or 'relationships' cannot be the place in which the claims arise but instead must be where redress is sought and immunity is needed." In this case, the relevant location was not where the harmful conduct took place (Israel) but the location of the litigation. Therefore, no extraterritorial application was necessary.

5 Intermediary Liability Reform Proposals

The dissenting judge in *Force v. Facebook* strongly suggested that Congress amend Section 230 and it looks quite likely to do so. There are a number of reform

44 Cf Eric Goldman, 'Second Circuit Issues Powerful Section 230 Win to Facebook in "Material Support for Terrorists" Case—Force v. Facebook' (*Tech and Marketing Law Blog*, 31 July 2019) <https://blog.ericgoldman.org/archives/2019/07/second-circuit-issues-powerful-section-230-win-to-facebook-in-material-support-for-terrorists-case-force-v-facebook.htm> accessed 21 October 2020:

> [T]he capacious definition of "publish" in common law defamation does, in fact, apply to phone calls. More importantly, as the majority points out, telephone calls aren't covered by Section 230 because they aren't on the Internet. So, by invoking an offline analogy, I assume the dissenting judge is normatively resisting Section 230's exceptionalism.

45 *Force v Facebook* (n 30) (Katzman, CJ dissenting).

46 *Force v Facebook* (n 42) 17–18, 23–27.

proposals being considered against the risks that reducing the scope of intermediary immunity will (1) push platforms to be overly censorious and thereby chill free expression; (2) make government too present in content moderation decisions in violation of the First Amendment; and (3) disadvantage small intermediaries unable to manage the risks of litigation. Next are some of the major reform proposals.

5.1 Ex Post Duty of Care

One approach to modifying intermediary liability posits applying a duty of care standard to intermediaries. Applying this standard to network platforms would focus on content management standards and operations as a whole rather than individual instances of curation and/or removal. Under a duty of care model, a platform would be exposed to liability, but would not be found liable if it had exercised a duty of care with respect to content moderation. This approach has been suggested by Danielle Citron and Benjamin Wittes, among others.[47] Arguably, a duty of care approach encourages transparency on content moderation practices (combatting the so-called "logic of opacity")[48] and presents a "preventative" or "compliance" approach (contrasted by a punitive approach). Such a change would take a more negligence-centered approach to intermediary liability. This would empower courts to determine whether a platform's actions regarding specific content was reasonable by considering the context of the content and the platform's efforts to combat such content.

Citron and Wittes cite Dirty.com, a website "devoted to spreading gossip, often about college students," as an example of an internet firm that is afforded undue protection from Section 230.[49] Dirty.com was designed specifically to traffic in objectionable and often defamatory gossip, but through a combination of blanket immunity and anonymous online conduct, plaintiffs have been effectively robbed of recourse in the face of defamation or invasion of privacy. Creating a reasonable care standard could give plaintiffs a way to go after bad actors that have taken insufficient action against unlawful content.

While the Citron-Wittes proposal would expand the legal options available to those who have suffered tortious harm, it would also open the door to extensive and potentially frivolous litigation. One of the benefits of Section 230's protections is that it provides firms, including nascent startups and small-scale forums, with legal certainty. According to Engine, an organization that advocates on

47 Citron and Wittes (n 29); see also Karen Kornbluh and Ellen P. Goodman, 'Bringing Truth to the Internet' (2010) 53 Democracy <https://democracyjournal.org/magazine/53/bringing-truth-to-the-internet/> accessed 21 October 2020 (suggesting the involvement of an expert regulatory agency within the duty of care model).

48 Sarah T Roberts, 'Digital Detritus: "Error" and the Logic of Opacity in Social Media Content Moderation' (2018) 23 First Monday 3 <https://firstmonday.org/ojs/index.php/fm/article/view/8283/6649> accessed 21 October 2020.

49 Ibid.

behalf of smaller firms, the cost of defending a Section 230 case through the entire discovery process can range from $100,000 to more than $500,000.[50] Stripping blanket immunity from platforms in exchange for a negligence standard would enable plaintiffs to engage in extensive litigation aimed at determining whether a platform's conduct was, indeed, reasonable.

5.2 Creating Genre-Based Statutory Limitations

Some commentators have suggested that Section 230 be scaled back to strip "safe harbor" protections for certain categories of communication. Recent proposals take this approach, for example, with respect to deep fakes (sophisticated machine-learning technology that can fabricate realistic audio and video depictions) and platform-hosted advertising.

In a 2018 white paper on information platform regulation, Senator Mark Warner claimed that the development of deep fakes will "usher in an unprecedented wave of false and defamatory content."[51] The white paper posits that platforms "represent 'least-cost avoiders' of these harms" and that they "are in the best place to identify and prevent this kind of content from being propagated on their platforms."[52] Senator Warner proposes to revise Section 230 to make platforms liable "for state-law torts . . . for failure to take down deep fake or other manipulated audio/video content."[53] His proposal would create a notice and takedown system, in which the victim of a tortious deep fake can request that a platform remove unlawful (usually defamatory) content. If issued a takedown notice, platforms would be liable in instances "where they did not prevent the content in question from being re-uploaded in the future."

While notice and takedown regimes, like those embedded in the Digital Millennium Copyright Act, are often abused,[54] Senator Warner's proposal would, he argues, mitigate the risk of frivolous takedown requests by requiring victims to successfully prove in court that the synthetic content is tortious in nature prior to issuing a takedown request. John Bergmayer of the tech policy non-profit Public Knowledge has suggested exempting an entire class of communications from Section 230 protections, arguing that it may be beneficial to impose greater liability on platforms for "ads they run, even when those ads are provided by a third party."[55]

50 Engine, Section 230: Cost Report.

51 David McCabe, 'Scoop: 20 Ways Democrats Could Crack Down on Big Tech' (Axios, 2018) <www.axios.com/mark-warner-google-facebook-regulation-policy-paper-023d4a52-2b25-4e44-a87c-945e73c637fa.html> accessed 21 October 2020.

52 Ibid.

53 Ibid.

54 Daphne Keller, 'Empirical Evidence of "Over-Removal" By Internet Companies Under Intermediary Liability Laws' (*Stanford Center for Internet & Soc'y*, 12 October 2015) <http://cyberlaw.stanford.edu/blog/2015/10/empirical-evidence-over-removal-internet-companies-under-intermediary-liability-laws> accessed 21 October 2020.

55 John Bergmayer, 'How to Go Beyond Section 230 Without Crashing the Internet' (*Public Knowledge*, 21 May 2019) <www.publicknowledge.org/blog/how-to-go-beyond-section-230-without-crashing-the-internet/> accessed 21 October 2020.

The advertising marketplace is so confusing and complicated that internet firms often have no way of knowing what types of advertisements their users see. Additionally, many online advertisements fed to users are "fraudulent, misleading, or even vectors for malware."[56] The existing structure of advertising markets fails to meaningfully align incentives in a way that promotes quality advertisements. For Bergmayer, exposing platforms to greater liability for the advertisements they run could potentially reorient the marketplace in a way that improves advertising quality. Internet firms could "force the ad tech and online publishing industries to adopt technologies that give them more control and oversight of the ads they run."[57]

What the Warner and Bergmayer proposals have in common is that they identify potentially risky classes of content to exempt from Section 230 protections in order to realign platform incentives to reduce the amplification of harmful content.

5.3 Creating Narrow Content-Based Carve-Outs

A related effort is closer to the FOSTA approach and consists of targeting specific messages. In a Senate Intelligence Committee hearing on foreign influence on tech platforms, Senator Joe Manchin floated a proposal to carve out drug trafficking content from Section 230 protections.[58] Other carve-outs might involve lifting immunity for online harassment, conspiracy to incite violence, cyber-stalking, or consumer fraud.[59]

FOSTA-like efforts have the benefit of targeting narrow classes of content, but they risk re-creating the moderator's dilemma and chilling platform speech. FOSTA made it unlawful to knowingly assist, facilitate, or support sex trafficking. As one commentator puts it, if liability is created on the basis of what platforms "know" about user-generated content, they may "rationally choose to do less policing work as a way of reducing liability-creating knowledge."[60]

5.4 Expanding the Definition of Content "Development"

While Section 230 insulates platforms from liability associated with user-generated content, it does not protect platforms from liability associated with the "creation or development" of unlawful content.

56 Ibid.

57 Ibid.

58 Samantha Cole, 'Senator Suggests the Internet Needs a FOSTA/SESTA for Drug Trafficking' (*Motherboard*, 5 September 2018) <www.vice.com/en_us/article/8xbwvp/joe-manchin-fosta-sesta-law-for-drug-trafficking-senate-intelligence-committee-hearing> accessed 21 October 2020.

59 Kornbluh and Goodman (n 47).

60 Eric Goldman, 'New House Bill (Substitute FOSTA) Has More Promising Approach to Regulating Online Sex Trafficking' (*Tech & Marketing Law Blog*, 11 December 2017), <https://blog.ericgoldman.org/archives/2017/12/new-house-bill-substitute-fosta-has-more-promising-approach-to-regulating-online-sex-trafficking.htm> accessed 21 October 2020.

Courts have generally interpreted "development" very narrowly. Though platforms take actions to promote or curate content, courts have held that these practices do not constitute content "development." In many cases, platforms pay users to create content. This is a common arrangement on the likes of YouTube, where the platform enters into revenue sharing arrangements with content creators. Courts have declined to abrogate Section 230 protections for this level of involvement. In the 1998 case of *Blumenthal v. Drudge*, a federal court held that AOL, which paid money to promote a defamatory article published by the Drudge Report, was insulated from liability under Section 230 even though the company financially contributed to the promotion of defamatory content.[61] This was because AOL had played no direct role in creating the defamatory statements.

Platforms could be subjected to distributor liability where the platform financially incentivizes the creation and distribution of content.[62] In other words, if a company like YouTube enters into a revenue sharing arrangement with a content creator producing unlawful content, it could be made liable for aiding in the content's creation. The idea behind a Section 230 reform aimed at creating broader liability for developing and propagating unlawful content is to encourage platforms to "figure out just who it is doing business with."[63]

While this change might encourage platforms to scrutinize more heavily their financial relationships with content creators, it would not touch a lot of the most harmful content simply because there is no underlying liability in the absence of Section 230. This is true, for example, of disturbing content aimed at children. Because such content is not necessarily unlawful, making a platform liable for monetized content might not result in any additional liability and therefore no additional legal incentive to combat such content.

5.5 "Political Neutrality" Mandates

In 2019, Senator Josh Hawley (R-MO) introduced the Ending Support for Internet Censorship Act, which would treat Section 230 protections as a privilege rather than a right.[64] The act would require internet firms above a certain size to apply for an "immunity certification" from the Federal Trade Commission (FTC). To receive such a certification, a firm would be required to show, to the satisfaction of at least four commissioners, that the "company does not moderate information provided by other information content providers in a manner that is biased against a political party, political candidate, or political viewpoint."[65] Commentators have been highly critical of Hawley's proposal, claiming that the bill is poorly drafted, imprecise, and fatally vague. Legal scholar Blake Reid

61 *Blumenthal v Drudge*, 992 F Supp 44 (DDC 1998).
62 Bergmayer (n 55).
63 Ibid.
64 Ending Support for Internet Censorship Act, S.___, 116th Cong (2019).
65 Ibid.

criticized its lack of clarity in defining what exactly constitutes "politically biased moderation."[66] Legal scholar Daphne Keller finds the bill flawed at a fundamental level because "it assumes there is a such a thing as political neutrality and that the FTC can define and enforce what that is."[67] A requirement of political neutrality, even if it survived a vagueness challenge, would dramatically curtail the speech rights of online intermediaries.

Senator Hawley's proposal currently has no co-sponsors in the Senate and is unlikely to move forward. However, it may foreshadow efforts to curtail the abilities of internet firms to meaningfully police their platforms for all manner of potentially harmful content.

5.6 Section 230 as Regulatory Leverage

According to legal scholar Rebecca Tushnet, Section 230 protections ultimately amount to a grant of "power without responsibility."[68] While some have quibbled with the idea that Section 230 acts as a subsidy or a "gift,"[69] others have argued that the law asks for little in return from the internet firms that reap benefits from it.[70] In the future, lawmakers could use Section 230 as leverage to encourage platforms to adopt a broader set of responsibilities.[71] Proposals to make its protections contingent upon satisfying a set of pre-conditions can be classified as "quid pro quo" amendments.

One of the appeals of reforming Section 230 through quid pro quo amendments is that it effectively makes regulation optional. It provides lawmakers with the ability to "regulate" technology firms consistent with the First Amendment. A quid pro quo structure for Section 230 protections would present platforms with a choice: Do they want to adopt an additional and transparent set of duties and responsibilities regarding content moderation or are they willing to forego some of the protections afforded by Section 230? Quid pro quo amendments could take many forms. For example, to qualify for immunity, platforms could be required to publish data on their curation practices and moderation procedures.

Another possibility is that platforms above a certain size could be required to pay a portion of their gross revenue into a fund dedicated to support the

66 @blakereid (*Twitter*, 19 June 2019) <https://twitter.com/blakereid/status/1141391542319345665> accessed 21 October 2020.

67 @daphnek (*Twitter*, 19 June 2019) <https://twitter.com/daphnehk/status/1141395273895174144> accessed 21 October 2020.

68 Rebecca Tushnet, 'Power Without Responsibility: Intermediaries and the First Amendment' (2008) 76 Geo Wash L Rev 101.

69 Mike Masnick, 'Section 230 Is Not Exceptional, It Is Not Unique, It Is Not a Gift: It's the Codification of Common Law Liability Principles' (*TechDirt*, 16 July 2019) <www.techdirt.com/articles/20190714/18000542585/section-230-is-not-exceptional-it-is-not-unique-it-is-not-gift-codification-common-law-liability-principles.shtml> accessed 21 October 2020.

70 Stigler Center Media Subcommittee, *Protecting Journalism in the Age of Democracy* (2019).

71 Ibid 53.

accountability journalism necessary for a healthy information ecosystem. Karen Kornbluh and I have proposed making Section 230's safe harbor conditional upon the adoption of greater platform responsibility. The idea is to require large platforms to develop "detailed, transparent, appealable practices specifically for disrupting coordinated campaigns" that engage in activities that "threaten or intentionally incite physical violence, . . . that clearly constitute online harassment, or that constitute commercial fraud."[72] While treating Section 230 protections as a privilege would be a substantial change, such proposals do not discriminate on the basis of viewpoint and require adjudication on an ex post basis. They encourage platforms to be more responsible and accountable while also enabling them to operate with a meaningful degree of certainty and self-determination.

5.7 Requiring User-Identification Procedures

Legal scholar Gus Hurwitz has floated a process-oriented reform to Section 230. He has suggested making its "immunity for platforms proportional to their ability to reasonably identify speakers that use the platform to engage in harmful speech or conduct."[73] This proposal came on the heels of a recent decision by the Third Circuit Court of Appeals in the case of *Oberdorf v. Amazon.com*, in which the court held that Amazon could be held liable for the actions of a third-party user on the Amazon Marketplace under a products liability theory.[74] The Third Circuit concluded that, because it had sufficient involvement in facilitating the sale of a defective product whose seller was unknown, Amazon could be treated as the "seller" of the product, and therefore would not be protected under Section 230.

Hurwitz's approach deals with the common problem of anonymity in online spaces. Platforms that safeguard speaker anonymity can functionally pass Section 230 protections onto "masked" speakers who create unlawful content. If the identity of a content creator is unknown and the platform is indemnified, victims of tortious or criminal conduct will often be left without meaningful legal recourse. Though Hurwitz recognizes that anonymous speech is often a critical tool, his proposal would have platforms take reasonable care in ensuring that users engaging in potentially unlawful speech can be identified. In other words, this approach would go after "platforms that use Section 230 as a shield to protect those engaging in [unlawful] speech or conduct from litigation."[75]

72 Kornbluh and Goodman (n 47).

73 Gus Hurwitz, 'The Third Circuit's Oberdorf v. Amazon Opinion Offers a Good Approach to Reining in the Worst Abuses of Section 230' (*Truth on the Market*, 15 July 2019) <https://truthonthemarket.com/2019/07/15/the-third-circuits-oberdorf-v-amazon-opinion-offers-a-good-approach-to-reining-in-the-worst-abuses-of-section-230/> accessed 21 October 2020.

74 *Oberdorf v Amazon.com Inc* (n 33).

75 Ibid.

5.8 Knowledge-Based Standard

The framework established by E.U.'s E-Commerce Directive inserts a knowledge element into intermediary liability, making platforms liable for hosting or transmitting illegal content once they have actual or constructive knowledge of said content. Although this has not been a popular approach in the U.S., similar standards exist in copyright and criminal law.[76] The concerns with such an approach are that increased editorial control would be used as proof of "knowledge," thereby deterring platforms from doing the very kind of moderation that is being called for.

6 U.S. Initiatives to Counter Disinformation

A final set of legislative enactments and proposals that deserve mention are those that seek to counter disinformation using soft-law approaches of anti-propaganda and media education. The Countering Disinformation and Propaganda Act, which was included in the fiscal year 2017 National Defense Authorization Act (NDAA), established the Global Engagement Center within the State Department. The Center is an interagency body that coordinates government counter-propaganda efforts and provides grants to civil groups focused on similar issues. The fiscal year 2018 appropriations bill also included a new Countering Russian Influence and Aggression Fund. The fund amount was increased in 2019 from $250 million to $275 million.

State-level initiatives to counter disinformation have generally focused on media literacy. At least 24 states have introduced bills to that effect, most of which are directed at changes to primary school-level curriculum.[77] In 2018, California directed the Department of Education (DOE) to supply schools with online resources for new evaluation.[78] Connecticut has created a digital citizenship, internet safety, and media literacy council within their DOE.[79] Massachusetts lawmakers passed a bill in early 2018 that mandates civic education with an emphasis on media literacy.[80] Federally, Senator Amy Klobuchar (D-MN) recently introduced the Digital Citizenship and Media Literacy Act.[81] There have also been new efforts to update the 1938 Foreign Agents Registration Act (FARA) in order to increase transparency surrounding foreign funded media outlets.[82]

76 18 USC §§ 2252, 2258A, 2258B (knowledge-based liability and obligations for intermediaries regarding child sexual abuse material); 17 USC § 512 (intermediaries lose DMCA immunity based on actual or "red flag" knowledge).

77 See 'Putting Media Literacy on the Public Politic Agenda' (*Media Literacy Now*, updated 20 January 2020) <https://medialiteracynow.org/your-state-legislation/> accessed 21 October 2020.

78 SB 830, Reg Sess (Cal 2018).

79 SB 949, Pub Act 17–67, Gen Assemb, Reg Sess (Conn 2019).

80 S 2631, Gen Ct, 190th Sess (Mass 2018).

81 S 2240, 116th Cong, 1st Sess (2019).

82 See generally Nick Robinson, 'The Foreign Agents Registration Act Is Broken' (*Foreign Pol'y*, 22 July 2019) <https://foreignpolicy.com/2019/07/22/the-foreign-agents-registration-act-is-broken/> accessed 21 October 2020.

8 European Media Law in Times of Digitality

Stephan Dreyer, Matthias C. Kettemann, Wolfgang Schulz and Theresa Josephine Seipp

1 Introduction

Media law has been strongly influenced by digitality, especially in light of the intricate interaction between traditional print media (newspapers) and the wider media in all its communicative forms. These two dimensions are distinct, but connected. In Jürgen Habermas' terms an important evolution of our time was that of the composition of the legal medium (*Rechtsmedium*)[1] and, following Thomas Vesting, of the media of law (*Medien des Rechts*).[2] The practices of pervasive computing—*digitality* in the context of this research—are deeply connected to both Vesting's "media of law"[3] and the "figures" of media law. We are currently observing a reconfiguration of the field of democracy-relevant communication processes and actors. Institutions that were created for a pre-digital age of public television and other less established media are being reinvented for digital communication dynamics. New media, more content and differentiated audiences[4] all pose challenges for the law. Even if, on closer inspection, many phenomena of online communication were not really structural changes having only accelerated developments that had already begun, the communication processes on social media platforms were fundamentally new and are still not fully understood. This

1 Jürgen Habermas, 'Im Sog der Technokratie' in Jürgen Habermas (ed), *Im Sog der Technokratie: Kleine politische Schriften XII* (2013) Suhrkamp, 7: "Heute zeigen sich auch auf internationaler Ebene Anzeichen für eine Rationalisierung der staatlichen Herrschaftsausübung, welche einer Veränderung in der Komposition des Rechtsmediums entspricht".

2 The titular notion of Vesting's tetralogy is "Die Medien des Rechts"; see Thomas Vesting, *Die Medien des Rechts: Sprache* (2011) Velbrück; Thomas Vesting, *Die Medien des Rechts: Schrift* (2011) Velbrück; Thomas Vesting, *Die Medien des Rechts: Buchdruck* (2013) Velbrück and Thomas Vesting, *Die Medien des Rechts: Computernetzwerke* (2015) Velbrück. See, in particular, Vesting (2015), passim and 83–84.

3 For an English version, see Thomas Vesting, *Legal Theory and the Media of Law* (2018) Edward Elgar.

4 Matthias C. Kettemann and Anna Sophia Tiedeke, 'Online Order in the Age of Many Publics' (2021) 50 Kybernetes 1004–14 <https://doi.org/10.1108/K-07-2020-0423> accessed 5 July 2021.

DOI: 10.4324/9781003283881-13

is true for the emergence of new types of publics, but also for the optimal design of rules in complex sociotechnical normative ecosystems.

The rules that private platforms set for their users' communication represent a form of private order (and are the result of private order formation). While it has long been recognised that the law applies on the internet, we find that a large proportion of legally relevant online communications and transactions take place in these private spaces. And these private spaces are primarily subject to the private rules, general terms and conditions, and community standards of individual internet companies. They determine what we can say online, what we can buy, what private legal protection we can claim. On a larger scale, these private norms structure publicly relevant actions and influence transaction and communication processes that are essential for the formation of the public sphere and the negotiation of matters of public interest—and thus enter into a demanding interrelationship with the domains of public law. This, too, is part of the new order surrounding media law.

The effective enforcement of state-set law in digital communication spaces requires the involvement of the private companies that operate these spaces. Their position of power and the social impact associated with it are significant. This was demonstrated in January 2021 when Facebook Inc and Twitter Inc responded to statements made by the then incumbent US President Trump before and in connection with the storming of the Capitol in Washington, DC by blocking his accounts.[5]

These companies have developed their own differentiated rules and, in a functional sense, normative orders. These are incorporated into the contracts between users and companies under private law and are enforced with different technical and institutional designs.[6] The interaction of these private and public orders is complex,[7] and a differentiated dogmatic has yet to be developed.[8] In the balancing of power and law in the increasingly technically mediatised constellations of relationships of the present, law and its scholarship are only just beginning to work out normative dogmatics of entaglement and interaction between private and public law of the internet in light of the necessity of hybrid speech governance.

How does the European media order deal with this complexity and has it developed sufficiently under the conditions of digitality to be called a "media law of digitality"? This contribution will answer these vexing questions by presenting elements of the current EU media order (Section 2), before going on to address

5 Martin Fertmann and Keno C Potthast, 'Digital Time-outs for Trump: The Beginning of the End of Privileged Treatment of Incumbents by Social Networks?' (JuWissBlog No 5/2021, 18 January 2021) <www.juwiss.de/05-2021> accessed 5 July 2021.

6 Matthias C. Kettemann and Wolfgang Schulz, 'Setting Rules for 2.7 Billion: A (First) Look into Facebook's Norm-Making System: Results of a Pilot Study' (2020) <www.ssoar.info/ssoar/bitstream/handle/document/71724/ssoar-2020-kettemann_et_al-Setting_Rules_for_27_Billion.pdf> accessed 5 July 2021.

7 Matthias C. Kettemann and Anna Sophia Tiedeke, 'Back Up: Can Users Sue Platforms to Reinstate Deleted Content?' (2020) 9 (2) Internet Policy Rev.

8 Ibid.

attempts at reform (Section 3). Finally, we conclude that, yes, a European media law of digitality is emerging (Section 4).

2 The European Communication Order in Digitality[9]

2.1 Media-Specific Legal Instruments

The scope and content of the EU legal instruments in the media sector are characterised by the legislative competencies of the European organs, as deriving from European primary law (i.e. the European Treaties). The guarantee of a free internal market for services—including audiovisual media services—is the starting point of all media policy measures. EU legislators also regularly make reference to the protection of human rights relating to information and communications in Art. 10(1) ECHR, and the limited possibilities for their statutory restriction in Art. 10(2) ECHR, as grounds for harmonising legal instruments in this area. Since media services are also cultural assets—for which the EU has only limited supporting competences—[10] the focus at the heart of European media policy is on guaranteeing an EU-wide internal market for audiovisual media and their providers. This focus aims to create a market for the production and distribution of services and content based on a homogenous legal framework and where fair competition prevails.

The cornerstone of the media law framework at EU level is the Audiovisual Media Services Directive (AVMSD),[11] which primarily sets out specifications in relation to audiovisual (i.e., video) media content. The purposes pursued in it concern harmonisation of specifications in qualitative and quantitative advertising law, the protection of human dignity and minors, accessibility, short news reports of public events, the promotion of European works and the independence of regulatory bodies. The specifications in the Directive are usually[12] not directly

9 This section is drawn from the co-authors' work in Stephan Dreyer and others, *The European Communication (Dis)Order: Mapping the Media-relevant European Legislative Acts and Identification of Dependencies, Interface areas and Conflicts* (Working Papers of the HBI No 522020) <https://doi.org/10.21241/ssoar.71719> accessed 5 July 2021; this study was conducted in the framework of, and financed by, the German government during its EU Presidency and was used in a number of conferences on changes to the European media order.

10 TFEU, art 167; previously TEU, art 151.

11 Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) [2010] OJ L 95/1, as amended by Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities, OJ L 303/69.

12 Exceptionally, individual provisions of the Directive may be directly applicable if they safeguard the legal position of legal entities and have not been transposed or not fully transposed in a Member State; see Case C-152/84 *Marshall v Southampton and South-West Hampshire Area Health Authority (Teaching)* [1986] ECR 723 et seq—"Marshall".

applicable, but require transposition into national law by the individual Member States. To clarify which national law a provider is subject to, the Directive contains provisions for determining jurisdiction. These are based on the country-of-origin principle, which assumes that the respective national law of the Member State in which a provider is established generally applies. The Directive makes provision for the establishment of a European Regulators Group for Audiovisual Media Services (ERGA) to promote better agreement and cooperation between the Member States in enforcing the implemented AVMSD specifications. The AVMSD does not contain direct specifications for ensuring media diversity, but the recitals include basic pronouncements on the value of media pluralism in the audiovisual internal market.

Alongside the structuring framework of the AVMSD sit individual legislative acts containing *legal provisions regarding specific media content*, for instance in the area of the depiction of child sexual abuse.[13] The Terrorist Content Online Regulation (TERREG)[14] is also part of these content-related specific rules providing special requirements for dealing with unlawful content.

Further media-specific legal instruments are primarily those establishing funding programmes for European media productions (particularly the Creative Europe MEDIA Sub-Programme)[15] and media-specific exemptions, notably in the area of state aid rules.[16] However, these do not constitute direct media content-specific rules for media providers.

2.2 Sector-Specific Legal Framework

The EU has closely accompanied the technological, economic and social development of forms of electronic information and communication on the regulatory side at the latest since the start of the 1990s, including via the continuous further development of the corresponding legal regulatory frameworks. Corresponding offerings are continually appearing as forms of services, which are particularly supported by the European Treaties. Given this background, sets of rules have come about which have as their subject the provision of electronically provided

13 Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse, sexual exploitation of children and child pornography and replacing Council Framework Decision 2004/68/JHA [2011] OJ L 335/1 corrected by [2012] OJ L 18/7.

14 Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online OJ L 172/79.

15 Regulation (EU) 2021/818 of the European Parliament and of the Council of 20 May 2021 establishing the Creative Europe Programme (2021 to 2027) and repealing Regulation (EU) No 1295/2013 OJ L 189/34.

16 Treaty of Amsterdam amending the Treaty on European Union, the Treaties establishing the European Communities and certain related acts—Protocols—Protocol annexed to the Treaty establishing the European Community—Protocol on the system of public broadcasting in the Member States [1997] OJ C 340/109, as last amended by Protocol No 1 to the Treaty of Lisbon of 13.12.07, art 1(4)(b) H, para. 28, OJ C 306/163.

or disseminated services, with the e-Commerce Directive at the heart of these. The ICT-specific legal frameworks in contract law, intellectual property law and consumer law also belong to this category. However, electronically disseminated communications content is reliant on the technical infrastructure which transmits the information in the form of electric oscillations or bitstreams. Accordingly, the overall legal framework notably also includes the legislation in telecommunications law, as a primarily sector-specific competition law. Beyond this the EU regulatory framework contains content specifications operating partly across different services, notably in the area of illegal depictions and expressions.

2.2.1 E-Commerce and Electronic Services Law

One of the directives which remains of key relevance in the ICT sector is the e-Commerce Directive, which contains fundamental rules for the provision of electronic services. When adopting this Directive, too, the EU legislators were primarily concerned to create a harmonised area of law through which a minimum standard for the free provision of—in this case—commercial electronic services in the digital internal market could be ensured. The recitals also make reference to the protection of basic rights relating to information and communications from Art. 10 ECHR, and to the limits on those freedoms. Areas which the e-Commerce Directive harmonises are the principle excluding prior authorisation and the possibility of concluding legally valid contracts in distance selling; provider-related information and transparency obligations for commercial communications and for contracting; issues relating to resolving disputes and to legal protection; and liability privileges in relation to user-provided content in the case of technical intermediary services. The Directive also provides clarification of applicable national laws, again starting from the country-of-origin principle.

The Directive, which was adopted in 2000, has come under pressure in recent years in respect of more recently developed forms of services, particularly with regard to the question of the suitability for the current requirements of the liability privileges for intermediaries and platforms. Against this background, the European Commission has developed a comprehensive update of the e-Commerce Directive as part of the Digital Services Act (DSA).

Tax law, too, is facing new challenges in view of cross-border digital services. Classical corporation tax law always assumes established corporations whose profits are taxed in the place where the value is created, and consequently company earnings can be assigned to a particular country. With non-physical services offered EU-wide and with providers from outside the EU, traditional approaches to taxation are coming up against their limits. The Proposal for a Digital Services Tax Directive (DST Directive)[17] was an attempt to create a chargeable event for revenues from the provision of digital services, at a rate of 3%. After consultations

17 Commission, 'Proposal for a Council Directive on the Common System of Digital Taxation on Revenues Resulting from the Provision of Certain Digital Services' COM/2018/0148 final—2018/073.

with US representatives the approach was abandoned, however, in favour of a global approach within the framework of the OECD.

2.2.2 Telecommunications Law

The European Electronic Communications Code (EECC) to be implemented by 20 December 2020,[18] replaces the package of Directives last amended in 2009 in EU telecommunications law[19]—with the exception of the e-Privacy

18 Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast) [2018] OJ L 321/36, corrected by [2019] OJ L 334/164.

19 Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) [2002] OJ L 108/33; Directive 2002/19/EC of the European Parliament and of the Council of 7 March 2002 on access to, and interconnection of, electronic communications networks and associated facilities (Access Directive) [2002] OJ L 108/7; Directive 2002/20/EC of the European Parliament and of the Council of 7 March 2002 on the authorisation of electronic communications networks and services (Authorisation Directive) [2002] OJ L 108/21, all amended by the Access Directive; Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/21/EC on a common regulatory framework for electronic communications networks and services, Directive 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and Directive 2002/20/EC on the authorisation of electronic communications networks and services [2009] OJ L 337/37; Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive) [2002] OJ L 108/51, amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive) [2009] OJ L 337/11; Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector [2002] OJ L 201/37 and Regulation (EC) No 2006/2004 of the European Parliament and of the Council of 27 October 2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws [2004] OJ L 364/1; Regulation (EC) No 1211/2009 of the European Parliament and of the Council of 25 November 2009 establishing the Body of European Regulators for Electronic Communications (BEREC) and the Office [2009] OJ L 337/1, repealed by Regulation (EU) 2018/1971 of the European Parliament and of the Council of 11 December 2018 establishing the Body of European Regulators for Electronic Communications (BEREC) and the Agency for Support for BEREC (BEREC Office) [2018] OJ L 321/1; Regulation (EU) No 531/2012 of the European Parliament and of the Council of 13 June 2012 on roaming on public mobile communication networks within the Union [2012] OJ L 172/10, amended by Regulation (EU) 2017/920 of the European Parliament and of the Council of 17 May 2017 as regards rules for wholesale roaming markets [2017] OJ L 147/1; Directive 2014/61/EU of the European Parliament and of the Council of 15 May 2014 on measures to reduce the cost of deploying high-speed electronic communications networks [2014] OJ L 155/1.

Directive.[20] The aim of both the old and the new legal framework for telecommunications is the harmonisation of the national legal frameworks for electronic communications networks and services, associated facilities and services and parts of end-facilities. Following the full liberalisation of the formerly state-controlled telecommunications networks, the directives and regulations aim to improve the regulation of the markets to ensure increased competition, to realise the internal market for electronic communication and, increasingly, to improve consumer protection and user rights.

The European statutory framework for telecommunications concerns the regulation of electronic communications networks and services, including specifications on the allocation of frequencies and numbers together with cross-country frequency coordination. It also includes specifications on rights of way for establishing and expanding telecommunications networks; provisions for network access and for shared use of network components and facilities; provisions on the security and integrity of networks and services; and specifications on the standardisation and interoperability of networks, services and associated facilities, including digital TV services. European telecommunications law envisages a series of procedures to implement the various provisions (including the monitoring of dominant telecommunications companies), to analyse and define relevant markets and to resolve disputes between companies.

The relevance of the statutory framework for telecommunications for the audiovisual sector is high. While European telecommunications law excludes applicability to transmitted content, providers are necessarily reliant on infrastructural services and networks to provide an audiovisual media service, and also to offer general information society services. They need a transport layer to convey their own content to those using it and, where applicable, to receive back requests from them. That layer consists of software-based telecommunications services and hardware-based telecommunications networks. Content-related services and their users are reliant on the access to and usability of the underlying transport layers and networks as channels for distribution, and feedback channels (where applicable).

Accordingly, issues and decisions in telecommunications law show direct and indirect links to certain activities to provide and disseminate information society services and to the options for receiving and using such services on the side of the user. These relate to frequency management, must-carry provisions, network neutrality, interoperability, specifications on availability and minimum quality of networks and services, the unbundling of vertically integrated services and, lastly, the scope of the intended consumer rights protection.

20 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] OJ L 201/37, as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 on privacy and electronic communications; Directive 2002/22/EC (n 20) and Regulation (EC) No 2006/2004 (n 20).

In addition to such forms of interlacing where telecommunications regulation influences the possibility and form of information society service provision, there are also instances of services which due to their nature may potentially fall directly under the provisions of the telecommunications law framework (see later).

2.2.3 Contract and Consumer Protection-Related Specifications in the Media Sector

In recent years the EU has adopted legal instruments relating specifically to electronically supplied or electronically disseminated services in addition to the general legislative framework for consumer protection (see later).

The Digital Content Directive (DCD),[21] adopted in May 2019 and to be implemented by 1 July 2021, is aimed at harmonising the framework under contract law for the provision of digital content or digital services. Its focus is on ensuring a high level of consumer protection in order to make cross-border conclusion of contracts more legally assured and to reduce the higher transaction costs which have existed to date. As a Directive governing contract law, the specifications here link to contracts on the basis of which entrepreneurs provide digital content or digital services to consumers. The decisive aspect is not payment, as the *quid pro quo* or the remuneration can also be provided through, inter alia, making personal data available. As such, the majority of media offerings and digital platforms fall under the scope of the Directive (see later). The requirements of the DCD thus become contract-related provisions which these providers too must respect, regardless of the technology used for provision or transmission. This may be software, apps and the content made available by media providers via those means (such as videos, audio files, music, games or e-publications). In addition, the Directive covers services such as cloud computing, hosting, social media and software as a service. Under the DCD, digital content is considered to be according to contract if it conforms to the statements of the contract concerning the description, quantity and quality, functionality, compatibility, interoperability and other features, and is "fit for any particular purpose for which the consumer requires it". The burden of proof that digital content or a digital service is as agreed lies with the provider. On this point, the DCD sets out requirements which are not always easy to interpret for media services and which differ from the provision of purely journalistic services. A further relevant circumstance regarding the DCD is the fact that it is a Directive which follows the approach of so-called maximum harmonisation, that is, the EU legislators have obliged the Member States to implement the specifications precisely, without leeway over transposition of normal Directives, for instance with regard to stricter or more lenient national statutory specifications.

21 Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services [2019] OJ L 136/1, corrected by [2019] OJ L 305/62.

The Portability Regulation[22] was adopted with a view to freedom of movement within the EU, aimed at ensuring the citizens can enjoy unhindered access to online content services EU-wide if they are temporarily residing in a country other than the one where they usually live. To that end, the relevant providers are obligated to make corresponding access available to their customers, including from other EU countries, with the same scope of function and without additional charges.

The Geo-Blocking Regulation[23] is similarly dedicated to consumer protection. With this regulation the EU is trying to prevent users being unjustly discriminated against when making online purchases, for instance on the basis of their nationality, their place of residence or their place of establishment in the EU. Under its provisions blocking or restricting customer access to user interfaces such as internet pages or apps, and discriminatory terms and conditions or payment demands are not permitted, for example. Web page redirections to country-specific portals or shops are regularly only permitted with explicit consent, and digital content must be available EU-wide (particularly software, apps, web hosting). In addition, providers must offer at least one free means of payment. The regulation applies only to a limited degree for services supplied electronically comprising the provision of copyright-protected works. For instance, it allows providers to operate different service conditions (prices, payment terms, delivery terms) for content offered via downloads or streaming. Information-related—e.g. journalistic—services not containing copyright-protected images or works are not covered by this exemption. Here, the provisions of the Geo-Blocking Regulation continue to apply in principle. Providers of live-streams and media libraries operated by public broadcasting companies may also freely decide to what extent they wish to follow the requirements of the regulation.

Plans and proposals by the EU to establish regulatory framing in the area of *algorithm-based decisions* generally or specifically to the media, for instance in the form of a General Algorithm Regulation, have not yet found expression in the form of draft directives or regulations. These proposals are connected with the current discussions regarding the possibilities and limits of artificial intelligence (AI) systems and the risks to fundamental rights associated with them, depending on the domain concerned.[24] Given the AI systems already in use with media producers, publishing houses and intermediaries, further developments in this area can have significant impact on media practice and public communication. Most recently, the

22 Regulation (EU) 2017/1128 of the European Parliament and of the Council of 14 June 2017 on cross-border portability of online content services in the internal market [2017] OJ L 168/1.

23 Regulation (EU) 2018/302 of the European Parliament and of the Council of 28 February 2018 on addressing unjustified geo-blocking and other forms of discrimination based on customers' nationality, place of residence or place of establishment within the internal market and amending Regulations (EC) No 2006/2004 and (EU) 2017/2394 and Directive 2009/22/EC, OJ L 60I, 2.3.2018, pp. 1–15.

24 See Commission, 'White Paper "On Artificial Intelligence—A European approach to excellence and trust"' COM (2020) 65 final.

Commission published an "AI Act" proposal as part of European legal framework for AI to address fundamental rights and safety risks specific to the AI systems.[25] Insofar as media platforms and media companies use AI (e.g. as part of recommender systems), the rules contained in the AI Act are also relevant to them.

2.2.4 Special Provisions Under Competition Law

The regulation on promoting fairness and transparency for business users of online intermediation services (P2B Regulation)[26] is an instrument under which the EU is giving consideration to the major importance of platforms and intermediaries for the visibility and dissemination of services. With regard to competency, the EU is invoking the contribution to ensuring the smooth functioning of the EU internal market. The P2B Regulation, which took effect on 21 July 2020, applies to online intermediation services and search engines, with the aid of which business users of the platform offer their products and services to end-consumers. It sets out provisions in this area aimed at ensuring transparency, fairness and effective options for remedy for business users, notably via requirements concerning general terms and conditions as well as information obligations towards business users, and the disclosure of the criteria for selection and ranking when displaying search results. From the viewpoint of media services providers, the P2B Regulation is mainly relevant because it obliges the intermediaries to disclose the basis for their ranking, to make possibly differentiated treatment clear, and to explain modalities of access to platform and user data. The parameter-related descriptions for this are to be worded in plain and intelligible language. For intermediary services the regulation provides rules for the establishment of internal complaints procedures and for the option of out-of-court dispute resolution (these rules do not apply for search engines). The specifications of the P2B Regulation extend into an area of media policy which has long been a subject of debate: the question of the transparency of selection and ranking logics for intermediaries. This would exclude intentional or targeted discrimination against particular content or providers, which could impact negatively on media diversity. In this area, the Regulation introduces a provision which could establish the corresponding transparency, albeit from the perspective of contract law and competition law, and not with regard to the individual's freedom of information or to media diversity.[27] The fact that the perspective of media diversity did not play a role of any kind as part of the legislative process is all the more notable.

25 EU Commission, Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, 21 April 2021, COM(2021) 206 final.

26 Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediary services [2019] OJ L 186/57.

27 See Maximilian Hermann, Robin L Mühlenbeck and Rolf Schwartmann, *Transparenz bei Medienintermediären* (2020) Vistas, 95.

2.2.5 Special Provisions Applicable to Intellectual Property Rights

The copyright framework plays a key role in the EU communication order through the processing, creation, publication and dissemination of content that is subject to copyright and to neighbouring rights. The legal framework is made up of several individual measures and enables holders and exploiters of intellectual property rights of protected works to exploit exclusivity rights for the commercial licensing of content. It also specifies the protection periods for such exploitation, and makes provision for key limitations to copyright.

The aim of the key 2001 InfoSoc Directive[28] was to adapt the law governing intangible assets to the consequences of digitalisation, online communication and increasing media convergence. The InfoSoc Directive harmonises the right of reproduction, the right of communication to the public and the right of distribution in accordance with the WIPO treaties. Further areas of focus were determining restrictions on copyright and the conditions and scopes if they are introduced into national copyright laws by Member States. It also sets a framework for permitted circumvention of technical protection measures, with the precise shaping of those being left to the Member States.

The most recent reform of EU copyright law came about in the Digital Single Market Directive (DSM Directive),[29] which modernises the InfoSoc Directive in a number of areas. The DSM Directive was adopted in April 2019 in the face of considerable protests ("Save the Internet"). Its focus is the statutory permission for text and data mining (TDM), collective licensing for works of visual art in the public domain and the establishment of neighbouring rights for press publishers, along with IP-related contract law and the responsibility of online content-sharing service providers. In this regard the provisions in Art. 15 which introduces a new related right for press publishers, and Art. 17 which sets out specifications on licensing obligations and on the liability of platforms with user-generated content for making copyright-protected online content accessible are of particular relevance for public communication.

The SatCab Directive[30] attempts to harmonise national copyright with regard to cross-border broadcasting via cable or satellite. The freedom to provide

28 Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society [2001] OJ L 167/10, last amended by Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market [2019] OJ L 130/92.

29 Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC [2019] OJ L 130/92, as corrected by [2019] OJ L 259/86.

30 Council Directive 93/83/EEC of 27 September 1993 on the coordination of certain rules concerning copyright and rights related to copyright applicable to satellite broadcasting and cable retransmission [1993] OJ L 248/15, amended by Directive (EU) 2019/789 of the European Parliament and of the Council of 17 April 2019 laying down rules on the exercise of copyright and related rights applicable to certain online transmissions of broadcasting organisations and retransmissions of television and radio programmes [2019] OJ L 130/82.

services guaranteed in the EU Treaty within the entire internal market of EU Member States is intended to be realised for cross-border broadcasting through this Directive. To that end, it sets out the corresponding legal conditions intended to make it easier for satellite and cable network operators to acquire the necessary broadcasting rights. In order to clarify intellectual property rights and related licencing rights it also adopts as a standard the country-of-origin principle and certain restrictions of the principle of contractual freedom. Despite the specific wording, the new Online-SatCab Directive[31] is not solely limited to online dissemination. Its aim is to promote cross-border dissemination of European television and radio programmes, including via IP networks. The regulatory subjects which it addresses extend to three main areas. These are—taking the country-of-origin principle into account—the online dissemination of certain types of TV and radio programmes in other EU Member States by the broadcasting companies themselves; the retransmission of TV and radio programmes from Member States by third parties (where mandatory collective management of rights to simplify the acquisition of rights by network and platform operators is applicable); and, lastly, the transmission of programmes using "direct injection", for which the principle applies that this is only a single instance of a public communication.

The Collective Rights Management Directive (CRM Directive)[32] is aimed at coordinating national regulations relating to organisations taking up the activity of collective management of copyrights and related rights, the modalities of their internal mode of operation and the supervision of these organisations. In particular, the Directive sets out requirements for the organisation of collective cross-border rights management, which was previously regularly exercised by national monopolies. For licensees wanting to offer a service EU-wide, it was possible to significantly simplify and shorten national licensing procedures, which had been very complex in some cases. This allows for significantly easier EU market entry for new online music and streaming services.

In addition to the media-specific legal legislative acts, which in part react to current technical and digital developments, at its "margins" the EU communications order also comprises the general specifications in quite different areas of law. Alongside many other areas of life and situations these also find application to media services and activities.[33]

31 Directive (EU) 2019/789 of the European Parliament and of the Council of 17 April 2019 laying down rules on the exercise of copyright and related rights applicable to certain online transmissions of broadcasting organisations and retransmissions of television and radio programmes, and amending Council Directive 93/83/EEC [2019] OJ L 130/82, as corrected by [2019] OJ L 296/63.

32 Directive 2014/26/EU of the European Parliament and of the Council of 26 February 2014 on collective management of copyright and related rights and on the multi-territorial licensing of rights in musical works for online use in the internal market [2014] OJ L 84/72.

33 For these, see Dreyer and others (n 9) 4.3.

3 Reform of Europe's Media Order

3.1 The Year of Reform

2022 will be a big year for European internet regulation because the legislative acts on Digital Services[34] and Digital Markets[35] (which will likely be adopted then) represent comprehensive European regulatory approaches to the platform economy. The values on which the reforms are based—maintaining the exemption from liability for third-party content while at the same time introducing transparency obligations, more rights for users and more responsibility for the platforms—are undisputed. The normative wind is blowing in this direction (even Californian laws, which are enacted in similar areas of law to European law, have long been oriented in this direction). But do the legal acts live up to their claim? Or is the claim itself overblown? Can important societal values be secured with a redesign of transparency and a special platform antitrust law, and can the platforms be better controlled (and the risks inherent in design and usage properties be assessed)? Or do we have legal acts in draft form whose normative potential remains unrealised?

The analyses of the drafts are numerous,[36] and initial assessments have also already been published.[37]

Both experience in the area of telecommunications law and regulatory theory show that the regulation of complex services and markets is strongly dependent on knowledge.[38] With regard to digital markets this applies to knowledge about the structures of the markets as the basis for appropriate, consistent and transparent regulation. In this respect, market research should be conducted in such a way that it expands knowledge about market structures and network effects and makes it easier to identify in which submarkets market entry is possible and

34 Commission, 'Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and Amending Directive 2000/31/EC' COM (2020) 825 final.

35 Commission, 'Proposal for a Regulation of the European Parliament and of the Council on Contestable and Fair Markets in the Digital Sector (Digital Markets Act)' COM (2020) 842 final.

36 Cf Jörg Uckrow, 'The EU Commission's Proposals for a Digital Services Act and a Digital Markets Act. Darstellung von und erste Überlegungen zu zentralen Bausteinen für eine digitale Grundordnung der EU' (*Institute of European Media Law*, 2021) <https://emr-sb.de/wp-content/uploads/2021/01/Impulse-aus-dem-EMR_DMA-und-DSA.pdf> accessed 7 July 2021; Daniel Holznagel, 'Chapter II des Vorschlags der EU-Kommission für einen Digital Services Act' (2021) 37 CR 123.

37 Julian Jaursch, 'The Draft DSA: Ambitious Rules, Weak Enforcement Mechanisms' (*Stiftung Neue Verantwortung*, 25 May 2021) <https://stiftung-nv.de/de/publikation/der-dsa-entwurf-ehrgeizige-regeln-schwache-durchsetzungsmechanismen> accessed 7 July 2021; Eliška Pírková, 'Access Now's Position on the Digital Services Act Package' (*AccessNow*, September 2020 <https://accessnow.org/cms/assets/uploads/2020/10/Access-Nows-Position-on-the-Digital-Services-Act-Package.pdf> accessed 7 July 2021; 'EDRi Position Paper on the Digital Services Act: Platform Regulation Done Right' (2020) <https://edri.org/wp-content/uploads/2020/04/DSA_EDRiPositionPaper.pdf> accessed 7 July 2021.

38 More generally, on the importance of knowledge in law, see, for example, Alexander Somek, *Rechtliches Wissen* (2006) Suhrkamp.

how to facilitate it. However, knowledge dependence also affects market actors' knowledge of the concepts behind the Commission's regulatory decisions. One way to promote more consistent and predictable regulation could be instruments such as explicit "regulatory concepts" (cf. Sec. 15a German Telecommunications Act), which are published by the Commission and on which future decisions are based. In any case, it hardly seems appropriate to regulate complex markets by imposing fines.

Similarly, the ambiguity of regulatory concepts seems to lead to problems in the DSA. A regulatory concept based on legally defining certain types of services and then attaching corresponding obligations to these types of services reaches its limits in digital sociotechnical ecosystems. An example of this is the question of whether the search function on a social media platform is a search service or part of the social media platform. The scale of the problem can be seen when even trained experts have difficulty classifying a central internet service like Wikipedia within the concepts and regulatory logic of the DSA. The boundaries of many types of services are difficult to define under European and Member State law—a situation that is exacerbated by the DMA.

In theory the principle of subsidiarity requires good reasons to use the legal instrument of the directly applicable regulation and thus to carry out extensive harmonisation. Against this background, the practice of using this instrument more and more frequently must be viewed critically. Even the designation as a legal act ("actification"[39]) does not protect against this criticism. The choice of regulation as legal instruments clearly restricts the ability of Member States to bring their legal traditions, cultural backgrounds and particularities of local markets into the regulatory structures. Nevertheless, there is much to be said in favour of regulation in the case of the DSM—at least at first glance—since it is globally active companies that are primarily the subject of regulation. In principle this poses the same challenges to the functioning of markets in all Member States.

In addition, given the importance of communications platforms for all measures adopted on the basis of the DMA—and also the DSA—a communication rights-related impact assessment should be carried out. Such an assessment should examine the potential impact of the measures on media providers. It should also and specifically include the benefits that the platforms themselves provide for communication and access to information. This would need to cover all delegated acts and any specific measures based on the DSA. If the assessment shows that there could be significant impacts, independent expertise would need to be consulted for the impact assessment before a decision is taken. Similarly, the legal interests enshrined in Art. 11 of the Charter of Fundamental Rights of the

39 Cf (approving of actification) Vagelis Papakonstantinou, 'The "Act-ification" of EU Law: The (Long-overdue) Move Towards "Eponymous" EU Legislation' (*European Law Blog*, 26 January 2021) <https://europeanlawblog.eu/2021/01/26/the-act-ification-of-eu-law-the-long-overdue-move-towards-eponymous-eu-legislation/> accessed 7 July 2021 ("This trend is to be welcomed insofar as it signals a new confidence and self-awareness of EU law", author's translation).

European Union should be included in the list of Art. 9(2) of the DSA (exemption for overriding reasons relating to the public interest).

Delegated acts bring challenges in terms of the democratic legitimacy of the decisions based on them. However, there is hardly any alternative when regulating complex and rapidly changing markets across the EU. In this case, the legitimacy deficits should be compensated for by other mechanisms. Against this background, it is important that the Commission regularly informs the public, the Member States and the European Parliament about its actions based on the DMA (this also applies to the DSA).

3.2 Digital Services

At the end of January 2021, Germany's Minister of Justice Christine Lambrecht let it be known that "the boundaries of our public discourse are not drawn in Silicon Valley: We Europeans define them ourselves". So what are the rules that these boundaries seek to define? First, the draft DSA ("one size doesn't fit all")[40] divides internet services into four categories. These are (in descending order): intermediary services that have an infrastructure network such as ISPs, domain name registrars; hosting services, such as cloud and web hosting services; online platforms that bring sellers and consumers together, such as online marketplaces, app stores, collaborative economy platforms and social media platforms; and the "VLOPs", the *very large online platforms* that pose particular risks of illegal content distribution and harm to society. For hosting services, there are also obligations to remedy illegal situations and to inform users.

The obligations imposed on digital services (some of which are new) are graded according to group membership. All four services must, for example, deliver transparency reports, observe fundamental rights in the terms of use, cooperate with national authorities on orders, and provide for contact points and legal representation if necessary. Online platforms below the threshold of VLOPs have four additional obligations. They must establish and maintain: a complaint and redress mechanism and out-of-court dispute resolution, the protection of whistleblowers, the reporting of crimes and the transparency of online advertising. There are additional obligations for VLOPs, such as transparency of recommender systems and choice for users in accessing information, risk management obligations and audit obligations, and the appointment of compliance officers.

While the current draft, which establishes criteria for transparency for content moderation, online advertising, or algorithmic content maintenance, is a reasonable

40 *Lambrecht* in ZEIT-Online, 22 January 2021 <www.zeit.de/digital/2021-01/digital-services-act-soziale-medien-digitalpolitik-europa-christine-lambrecht>.

start, none of these approaches is a goal in itself. If transparency is used as a regulatory tool, it should be clear who needs to understand exactly what in order to achieve the regulatory goal[41]—is it about information for users, for regulators, or for other market participants? The transparency concept should then be designed and implemented to increase the likelihood of achieving the desired objective. This can then be reviewed and the digital services coordinators must be given the authority to tighten up accordingly if it becomes apparent that the transparency goal is not being achieved. The data access rights now provided for (Art. 31) are already quite detailed, but NGOs criticise the fact that they are only available to researchers. The latter must also fight for access on an individual basis. Positive developments are emerging,[42] but in view of the practical challenges that arose, for example, in the "Social Science One" project, it remains to be seen whether such a system can function without an altruistic, or at least public, data broker.[43]

Meaningful transparency is an essential criterion for platform accountability, but other steps are needed that are noticeably absent from the draft. Some advertising technology industry practices pose systemic threats to human rights, especially when in the hands of very large online platforms.

The proposed notice-and-action mechanism is not tailored to a specific category of suspected illegal online content and needs to be further developed. The assessment of the legality under national law of reported content remains the responsibility of online platforms. From a civil society perspective, Access Now reminds the European Commission that the DSA will set a precedent for content control beyond the European Union.[44] If it is not done properly, the negative impact of this legislation could be far-reaching for human rights protections in the global online ecosystem.

There is no requirement that content providers be notified before any action is taken with respect to the reported content. Such a measure would introduce due process safeguards into the notice-and-action process. The purpose of notifying the content provider would introduce the element of procedural fairness.

41 Cf the Santa Clara Principles on Transparency and Accountability in Content Moderation, <https://santaclaraprinciples.org> accessed 7 July 2021, which also appear undercomplex here.

42 Amélie Heldt, Matthias C. Kettemann and Paddy Leerssen, 'The Sorrows of Scraping for Science: Why Platforms Struggle with Ensuring Data Access for Academics' (*Constitution Blog*, 30 November 2020) <https://verfassungsblog.de/the-sorrows-of-scraping-for-science> accessed 7 July 2021.

43 Margaret Levi and Betsy Rajala, 'Alternatives to Social Science One' (2020) 53(4) PS Polit Sci Polit 710–11.

44 'DSA: European Commission Delivers on the First Step Towards Systemic Rules for Online Platforms' (*AccessNow*, 15 December 2020) <https://accessnow.org/dsa-systemic-rules-for-online-platforms> accessed 7 July 2021.

The introduction of systemic risk assessment carried out by very large online platforms seems problematic in its current form because it is based on self-assessment by the platforms coupled with very limited public independent oversight. A public model would probably be better here, for example under the control of the Digital Services Coordinator.

With regard to the enforcement mechanism, the draft Regulation follows the principle of primacy of coordination by the institutions in the country of establishment. This approach seems to follow the same logic as the one-stop-shop mechanism in the GDPR. The supervisory structure is not the strong point of the GDPR, and despite (extensive) full harmonisation at the substantive level, national differences are again shaping up in supervision.[45] There is also the question of how the coordinators relate to other established supervisory bodies in the Member States, such as the State Media Authorities in Germany (and the data protection commissioners of the federal states), which have been given more powers by the State Media Treaty for digital platform communication. This can be seen as a challenge, but certainly also as an incentive to initiate overdue reforms in this area.

3.3 Digital Markets

In the digital markets, some large online platforms act as gatekeepers. The Digital Markets Act aims to ensure that things are fair on these platforms and, together with the Digital Services Act, is one of the core elements of the EU digital strategy.

The Digital Markets Act establishes a narrowly defined set of objective criteria for classifying a large online platform as a gatekeeper. Thus, the law remains focused on the problem it seeks to address with respect to large, systemic online platforms.

In principle, sector-specific market regulation in this area would appear to make sense due to the market structure. It has been shown that competition is not assured in certain markets where powerful players have long been allowed to make strategic acquisitions, especially in the long term. This is due to various network effects that make it difficult to challenge established market positions. It appears to be a future-proof concept, as the draft DMA provides retroactive adjustments for unfair business practices of the future and for companies that have yet to become gatekeepers. Since platform markets obviously do not tend to be competitive even in the longer term, it seems sensible to develop sector-specific competition law similar to that for telecommunications law.

45 On the dispute among data protection authorities, see, for example, Alexander Fanta, 'Accusation by Ulrich Kelber: Irish Data Protection Authority Makes "False Statements"' (*netzpolitik.org*, 18 March 2021) <https://netzpolitik.org/2021/vorwurf-von-ulrich-kelber-irische-datenschutzbehoerde-macht-falsche-aussagen> accessed 7 July 2021.

The gatekeeper criteria are met when an entity

- Holds a strong economic position with a significant impact on the internal market and is active in several EU countries,
- Has a strong intermediary position (i.e. connects a large user base with a large number of companies),
- Has (or will soon have) a consolidated and lasting market position (i.e. is stable in the long term).

Typically, the services that fall within the scope of the DMA are used for transactions, but also for communications. This overlap brings up the central question that arises with any new regulation in this area, namely how the legal tools used at the EU level for economic reasons relate to the rules enacted by Member States to safeguard freedom and diversity of expression. It would be helpful here to clarify Art. 1(5) to the effect that measures to safeguard freedom of expression and diversity are explicitly designated as a public interest that can be pursued by Member States as part of their cultural policies without prejudice to the DMA. Furthermore, procedural mechanisms—such as participation and initiative options for the Member States—are helpful in cases where a clear separation of regulatory competences is difficult or impossible to achieve.

Sensitive fines (e.g. up to 10% of yearly global turnover as a penalty) are part of the concept and could have a considerable deterrent effect even on large tech companies. However, it is not easy to determine under what conditions a forced sale of parts of a company really solves the problem at hand because there are only a few examples in the history of market regulation.

The basic approach of addressing gatekeeper power based on data ownership seems to respond to a real problem which relates to the prohibition of data use by business customers to produce competing products. Whether the general ban on the aggregation of data from different business sectors and the ban on automatic logins to multiple services is really in the interest of consumers and, moreover, a proportionate measure, cannot be judged here (but it remains open to question).

A general ban on personalised advertising—as proposed by some stakeholders as part of the DMA—should only be considered after careful consideration of the potential impact on information and communication services. As important as privacy issues are, they must be balanced with issues of freedom of communication and freedom of access to information. Plus, most of privately owned media rely on advertising funding.

4 Conclusions

European media law is fragmented and not fully coherent.[46] The provisions that impact on media law as it is broadly understood originate in varied areas of

46 Stephan Dreyer and others, 'The European Communication (Dis)Order. Mapping of EU Legal Acts Relevant to the Media and Identification of Dependencies, Areas of Intersection and Contradictions' (2020) 51 *Working Papers of the HBI* <https://doi.org/10.21241/ssoar.71720> accessed 7 July 2021.

European law, stand in different regulatory traditions, and follow logic (and use terms) which are sometimes incompatible with each other. This can lead to conflicts. European media law "of digitality" can only be rightfully considered European if legislative provisions pursue the purpose of market-related harmonisation aimed at completing the internal market (Art. 26 TFEU). This gives European media law a market-oriented slant which is counterbalanced by the Charter of Fundamental Rights of the EU.

One characteristic of European media law is the frequent introduction of new terminologies, different scopes of application and rather phenomena-led, almost "empirical", regulation. Impact assessments could avoid some of the regulatory pitfalls, but they are usually conducted long before a new legal instrument makes it "onto the market".

Most recently, European media law has been characterised by a stronger push towards ensuring public governance of private media actors, in particular platforms. The draft Digital Services Act and Digital Markets Act, coupled with the Data Governance Act and the AI Act, will provide a completely new and encompassing framework for European media law that could allay some concerns regarding coherence and the market-orientation of past regulation.

Unlike in the US, where meaningful reform of Sec. 230 seems to founder on the multiplicity of competing proposals, the Commission's consolidating (and consolidated) model is grounded in substantial research on best practices of platform governance. One success of an order a regulatory approach is if it is being replicated elsewhere. We see a preliminary "Brussels effect"[47] happening here, too. Europe appears as a normative power and has extracted key set pieces from years of engagement with the most important ideas of critical platform research by Commission staff. It also seems that the Commission wishes to reserve substantial powers to put flesh onto the bones of the new European media order by reserving for itself a large number of secondary legal acts within the framework of comitology. In any case, compensatory mechanisms must be provided here (this is also in the interest of acceptance of the new regulation on the side of the Member States as well as the companies affected).

Achieving regulatory coherence—at the European level, between EU level and Member States, and globally—is increasingly challenging.[48] Coherence could benefit from a medium-term framework that contains the principles that the EU will follow—across sectors and policies—in creating the future normative order for digital services.

At the same time, the attempted reorganisation of European platform governance must not be overburdened by unrealisable expectations. Neither new accountability and transparency rules, nor a special platform antitrust law, new data rules or a restriction on the use of artificial intelligence will—either alone or in

47 Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (2020) Oxford University Press.

48 Dreyer and others (n 46).

aggregate—reverse social trends (such as moves toward individualisation or social fragmentation or political division), or the processes of media change or changes in media usage behaviour. Attempts to "platform-proof" democracies must therefore always be accompanied by other structural measures.[49] From this point of view redesigning the legal framework for platforms is a necessary start and can be seen as the foundation of a new European communication law of digitality, but this is obviously not the end of the process of sustainably securing the freedom of democratic processes of self-determination. The task of renewing democracy begins afresh every day.

49 Matthias C. Kettemann and Martin Fertmann, 'Making Democracy Platform-proof. Social Media Councils as a Tool for Socially Reintegrating the Private Orders of Digital Platforms' Friedrich Naumann Foundation for Freedom (Potsdam-Babelsberg, May 2021) <https://shop.freiheit.org/#!/Publication/1055> accessed 7 July 2021.

Part V

Financial Regulation and Criminal Law

9 Regulating Virtual Currencies

Roland Broemel

1 Digital Currencies as a Form of Global Digitality

Digital currencies are both a specifically digital and a specifically global phenomenon.

1.1 Digital Currencies as a Digital Phenomenon

1.1.1 Blockchain as a Specifically Digital Technology

Digital currencies are—with differences depending on their respective concrete form—constituted by algorithm-based operations and are transferred by algorithm-based operations. With the blockchain, digital currencies are based on a technology that not only transfers processes existing in the analogue world to the digital world, but also creates properties that conventional means of payment do not have. The mechanism for validating a transaction, which creates confidence in the legitimacy of the contracting party and the permanence of the transaction, is based on asymmetric methods of encryption and decentralised redundant storage, which are not possible in the analogue world.[1]

1.1.2 Added Value of Payment Data

The economic characteristics of digital currencies are also important because of their specific digital character. The data generated by digital financial transactions have a considerable commercial value. Digital payment services are thus becoming a driver of complex, cross-market business models. At the same time, they are a central element of digital platforms and ecosystems.

1 Concerning Bitcoin Satoshi Nakamoto, 'Bitcoin: A Peer-to-Peer Electronic Cash System' (2008) 1 <https://bitcoin.org/bitcoin.pdf> accessed 30 November 2020: electronic payment system based on cryptographic proof instead of trust and financial institutions serving as trusted third parties to process electronic payments.

DOI: 10.4324/9781003283881-15

1.1.2.1 DATA AS A COMMERCIAL FACTOR: CROSS-MARKET BUSINESS MODELS

Digital financial transactions provide data about the object and the people involved in the transaction. Similar to other business models in digital markets, these data can be commercialised in a variety of contexts.[2] A typical feature of this commercialisation is that data items from a number of different sources are examined for correlations. Such a clustered data basis allows forecasts in unknown cases and business models based on statistical probabilities.[3]

This commercial relevance of personal data gives rise to multilateral business models that subsidise services in certain exchanges to obtain personal data so that these data can be used elsewhere.[4] Access to data, and in particular to payment data, will thus become a key factor for market position in the respective markets.[5]

1.1.2.2 IMPACT ON DIGITAL PAYMENT SERVICES AND CURRENCIES

This importance of data also concerns digital payment services and digital currencies. When using digital payment services, each transaction automatically generates personal data on the circumstances of the transaction, which can be used as a basis for both the profile of the person and for further correlations. For this reason, payment data are particularly suitable as a basis for correlation-based analyses. This added value of the data is a major reason why data-savvy platform operators such as Apple, Google, Amazon and Microsoft are developing their own payment services for mobile and digital payments.[6]

1.1.2.3 DEVELOPMENT OF DIGITAL ECOSYSTEMS IN DIGITAL FINANCIAL SERVICES

Digital payment services and currencies are becoming an element of digital ecosystems. In the case of payment services, the processing of transaction-related data forms an information basis that can be used, among other things, to optimise financial products and to assess the people involved. Typical objects of these algorithm-based analyses are the creditworthiness of persons, their preferences for certain products or insurance risks. Because the analyses based on correlations are

2 Monopolkommission, 'Competition Policy: The Challenge of Digital Markets' (Special Report No 68) 30ff.

3 For an overview see BaFin, 'Big Data Meets Artificial Intelligence' (2018) 24ff. <www.bafin.de/SharedDocs/Downloads/DE/dl_bdai_studie.html> accessed 30 November 2020.

4 Autorité de la Concurrence/Bundeskartellamt, 'Competition Law and Data' (10 May 2016) 8ff.

5 BaFin (n 3) 19–20.

6 For an overview see ibid 20–21; concerning Facebook's Libra see Valerie Khan and Geoffrey Goodell, 'Libra: Is It Really about Money?' (August 2019) <https://doi.org/10.2139/ssrn.3441707> accessed 30 November 2020.

derived from statistically determined probabilities and are transferable within the premises of these procedures, customer contact also enables forecasts to be made for people who are hardly known. Payment-related data thus holds the potential for considerable synergy effects.

An example of this is the portfolio of products and services of the Ant Financial Services Group, a fintech company that emerged as a subsidiary from the Chinese Alibaba Group. While the company was initially established to provide support in the form of payment services for the Alibaba trading platform, Alipay has moved beyond this context becoming a platform for digital payments. In addition, a credit rating system (Sesame Credit) facilitates the granting of credit and a money market fund (Yu'e Bao), which also belongs to the group, facilitating access to liquid funds as an alternative to the established credit institutions.[7] The example of the Ant Financial Services Group is based to a large extent on specific characteristics of the Chinese context. On the one hand, there is a considerable need for payment services for end customers and loans for small and medium-sized enterprises. On the other hand, the data protection legal framework as well as the social acceptance for processing personal data are favourable for data-intensive applications. Nevertheless, it cannot be ignored that the data-based synergies in the individual business areas have significantly improved the performance of the Group and its individual companies, and in particular their ability to adapt promptly to economic, regulatory or technical changes. The expected market capitalisation of the Ant Financial Group's IPO, which was recently postponed due to other concerns, reflects a market potential of conglomerate, data-based companies, which also applies, despite all differences, to corresponding markets on other continents.

For this reason, European supervisory authorities differentiate in the typification of fintech companies between such fintechs, which as start-up companies regularly focus on specific technology-based offerings, and the so-called Big Tech companies. These Big Tech companies are characterised by the fact that they have developed know-how in the analysis of large amounts of data and their commercial exploitation in a number of different markets and are entering new financial markets. They compensate for their weakness, which is typically due to their limited knowledge of the industry, including its regulatory requirements, with their strengths in access to and processing of relevant data.[8] From their point of view, the added value of offering financial services typically lies less in the revenues that

7 The Economist, 'Queen of the Colony: What Ant Group's IPO Says about the Future of Finance' (10 October 2020) <www.economist.com/briefing/2020/10/10/what-ant-groups-ipo-says-about-the-future-of-finance> accessed 30 November 2020; for a short analysis of the Ant Ecosystem see Dirk A Zetzsche and others, 'Digital Finance Platforms: Toward a New Regulatory Paradigm' (2020) 20ff <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3532975> accessed 30 November 2020.

8 BaFin (n 3) 95–96.

can be generated directly than in the enhancement of the data basis with personal data with financial reference.[9]

1.1.2.4 ECOSYSTEMS IN DIGITAL CURRENCIES

This relevance of the data-driven knowledge base for digital ecosystems also characterises the economic properties of digital currencies. Digital currencies have similar characteristics to digital platforms.[10] The operator of the digital currency infrastructure receives data on transactions not only in respect of those in which the operator is directly involved. Rather, data are generated on all transactions carried out in the respective currency.

The currency "Diem", which was announced some time ago and then abandoned, among other things, due to regulatory objectives, followed a strategy explicitly designed to link with existing platforms. In the case of Libra, the market position of the social network Meta will be used to achieve a considerable degree of dissemination with the introduction of the virtual currency. The materials provided by the consortium also suggest that the various members of the consortium will actively promote the use and hence the dissemination of the virtual currency by granting special conditions in their offers.[11] From an antitrust point of view, the Diem has already been attributed a dominant position from the time of its intended introduction due to the background of the social network Facebook.[12]

Vice versa, the introduction of such a virtual currency strengthens the market position of a social network or digital ecosystem. Not only does the use of a virtual currency generate considerable amounts of transaction-related data, the network effects associated with the virtual currency further reinforce the network effects that characterise the social network. In other words, this form of digital currency combines the characteristics of digital payment services with the economic characteristics of digital platforms.

1.2 Virtual Currencies as a Specifically Global Phenomenon

Because of its characteristics, a virtual currency is not only a specifically digital phenomenon, but also a specifically global one. From an economic point of view, globality becomes evident first of all in the volume of a virtual currency and the associated global spread. The Bank for International Settlements has introduced

9 Ibid 96.

10 Concerning payment platforms Markus K Brunnermeier, Harold James and Jean-Pierre Landau, 'The Digitalization of Money' (August 2019), 12–13.

11 For an overview of the risks of collusion see Thibault Schrepel, 'Libra: A Concentrate of "Blockchain Antitrust"' (2020) 118 Michigan L Rev 160, 164–65.

12 Volker Brühl, 'LIBRA—a Differentiated view on Facebook's Virtual Currency Project' (2019) CFS Working Paper Series No 633, 13–14 <www.econstor.eu/bitstream/10419/206412/1/1680695878.pdf> accessed 30 November 2020; generally Brunnermeier, James and Landau (n 10) 10.

the term "global stable coins" to describe a category of virtual currencies which, on the one hand, are characterised by considerable network effects for various reasons and which, on the other hand, can have significant effects, for example on monetary policy measures[13] or the stability of the financial markets.[14] The cross-border, global dimension of digital currencies is the result of several independent technical and economic factors.

1.2.1 Technical Factors of Globality

The technical side of the globality of digital currencies is clearly seen in the decentralised forms of blockchain technology, as known from the virtual currency "Bitcoin". On the one hand, the decentralised mechanism of validation of individual transactions leads to the fact that the individual Bitcoin exists independently of the legal recognition by a single state. Virtual currencies, which create units exclusively by code, thus elude classification as national or international from the outset. Such a virtual currency can no longer be assigned to a particular nation state. It typically does not even have a particular local centre. Accordingly, a major economic advantage of virtual currencies lies in their fast, worldwide and cost-efficient transferability. Since virtual currencies require only access to the internet, they offer global availability and transferability, which in the case of sovereign currencies must be provided by an infrastructure. Such infrastructure is typically based both on cooperation between the participating central banks[15] and private credit institutions or other commercial providers whose services are based on the infrastructure provided. In other words, the globalisation of established sovereign currencies, even in digital form as scriptural money, typically relies on the intermediary services of private intermediaries, which leads to additional costs. The costs of international transactions are therefore one of the reasons why central banks (i.e. central bank digital currencies) are considering issuing digital currencies.[16]

On the other hand, decentrally designed blockchain systems rely on a decentralised distribution of the nodes to ensure security against manipulation. The trust in the integrity of the blockchain is based precisely on the decentralised nature of the nodes, which are designed and coordinated as independent units in the algorithm.[17] Variants of the design, in which one actor or a defined group of actors retains sole or decisive control over the ongoing development of the blockchain (i.e. the transactions are not validated by decentralised, independent but coordinated operations) require less effort in coordination. Especially with

13 Brühl (n 12) 15ff.
14 G7 Working Group on Stablecoins, 'Investigating the Impact of Global Stablecoins' (October 2019), 12ff.
15 European Central Bank, Guideline on a Trans-European Automated Real-time Gross Settlement Express Transfer System (TARGET2) of 5 December 2012 (ECB/2012/27).
16 European Central Bank, 'Report on a Digital Euro' (October 2020) 9ff.
17 Nakamoto (n 1) 1.

increasing volumes, the effort, including energy and computing power, for the validation of individual transactions is significantly lower. Moreover, the confirmation and registration of the transaction requires less time. Nevertheless, systems that concentrate influence and control at one point are automatically more susceptible to external manipulation.

1.2.2 Economic Factors of Globality

Virtual currencies, such as stablecoins, which link virtual units with real collateral such as securities or sovereign currency, depend on their integration into a legal system through this linkage. Although they are typically global in nature, this link makes the virtual currency an object of national legislation, and consequently raises a number of issues in the treatment of cross-border situations, such as private international law, supervisory cooperation or mutual recognition.[18] The linking of the virtual currency to a real security binds the virtual currency to a legal system and thus reintroduces the distinction between national and international. Notwithstanding the legal factors of globality, virtual currencies, especially if there is a platform or network behind the issue, are globally distributed for economic reasons.

1.2.2.1 EXCHANGE COSTS AND ECONOMIC FUNCTIONS OF MONEY

The direct and indirect network effects associated with this platform generate switching costs for users.[19] Such switching costs could arise from the fact that a significant number of transaction partners use the respective virtual currency on an ongoing basis or that significant amounts are held in the respective currency. More precisely, the type and intensity of the exchange costs result from the function of the use of the virtual currency in the individual case and its respective framework conditions. While conventional currencies issued by the sovereign are characterised from an economic perspective by three functions, namely the storage of values, the unit of account and the transfer of values,[20]

18 For an analysis of aspects of international private law D Martiny, 'Virtuelle Währungen, insbesondere Bitcoins, im Internationalen Privat- und Zivilverfahrensrecht' [2018] IPRax 553.

19 Brunnermeier, James, and Landau (n 10) 9–10. These switching costs can also be a reason for the reluctance of private virtual currencies such as Bitcoin to be used in comparison with officially recognised currencies, William J Luther, 'Cryptocurrencies, Network Effects, and Switching Costs' (2018) Mercatus Center Working Paper No 13–17 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2295134> accessed 30 November 2020.

20 Brunnermeier, James, and Landau (n 10) 7: traditional definition of money; on the heterogeneous understanding in the legal sciences Katja Langenbucher, 'Digitales Finanzwesen' (2018) 218 AcP 385, 386–87; Gerald Spindler and Martin Bille, 'Rechtsprobleme von Bitcoins als virtuelle Währung' [2014] WM 1357, 1360.

virtual currencies fulfil these functions to a very different extent depending on their characteristics.

Virtual currencies with high volatility, for example, are less suitable for storing values. Their suitability for short-term transfer, on the other hand, depends largely on the acceptance of the virtual currency by other potential transaction partners and the costs of a single transfer. Virtual currencies, which are typically transferred at low cost and are accepted by a large number of players, are also suitable in this case for transferring values even if their value is subject to considerable fluctuations in the medium term. In this case, users will utilise the virtual currency exclusively for the transfer and then change the virtual unit to a less volatile unit as required. If the conversion of the virtual units is possible at low transaction costs, the digitisation of the currency leads to a separation of the functions which, in the case of conventional currencies, have coincided.[21] Virtual currencies may only be suitable for some of the functions and are used for precisely those functions because of the facilitated convertibility. Furthermore, the characteristics of the virtual currency, in particular its suitability for the one or other function, depend largely on the technical design and the economic connection to a platform. In the case of stablecoins, it is above all the linking of the unit to a real security that increases the stability of value. In addition to the technical framework conditions of validation, the suitability for the transfer of values depends essentially on the acceptance of the unit, which can be increased considerably by linking it to an existing social platform.

1.2.2.2 PART OF THE NETWORK INSTEAD OF A GEOGRAPHICAL AREA

As a consequence of these exchange costs, the users of a virtual currency form a network which, in contrast to currencies issued by the state, is not concentrated in a specific local area but is characterised by participation in the digital ecosystem and thus by the network effects.[22] Similar to other digital platforms, the link between users of virtual currencies and their connection to the digital ecosystem is created through use, although the intensity of the link varies depending on the design of the platform.

2 Legal Framework of Virtual Currencies

These specific characteristics of digital currencies entail a number of different consequences for the legal framework. On the one hand, legal facts are typically tailored to situations that imply certain technical characteristics of the transaction or certain modalities of communication. The legal classification of facts that are implemented in the digital environment then typically requires adaptation

21 Brunnermeier, James, and Landau (n 10) 9ff: unbundling of money.
22 Ibid 11.

or translation. The need for such adaptation efforts, which are triggered by digitisation phenomena, is not limited to the field of payment services or virtual currencies.[23]

On the other hand, the particular characteristics of digital currencies raise regulatory issues that require specific measures. Such specificities concern certain risks inherent in the characteristics of digital currencies, for example in the areas of combating money laundering or terrorist financing, investor and consumer protection and the stability of financial markets.

2.1 Adaptation

2.1.1 Banking Supervision Law

The need for legal adaptation in the regulation of virtual currencies under financial market law essentially arises from the fact that the digitisation of the unit of value, both in terms of its issuance and its transfer between private individuals, differs in some, particularly technical, points. For market participants, the virtual currency constitutes a functional equivalent of a sovereign currency. One of the difficulties of prudential treatment is to assess the extent to which the individual activities fall within the established facts and categories of banking supervision law.

2.1.1.1 VIRTUAL CURRENCY AS CATEGORY: UNIT OF ACCOUNT OR CRYPTO VALUE

Paradigmatic for difficulties in categorisation in German law is the classification of the individual units of virtual currencies as financial instruments in the banking supervisory sense. Both the qualification as a credit institution and as a financial services institution are linked, with the corresponding consequences for the regulatory requirements, to a catalogue of activities which to a large extent relate directly or indirectly to financial instruments.

The German supervisory authority understands the concept of "units of account"[24] as a kind of catch-all concept, which also includes artificial currencies such as special drawing rights, or currencies issued in the private sector, especially virtual ones.[25] In the literature this interpretation is quite controversial.[26] It has

23 They concern for instance labour law, competition law, insurance law and media law.

24 Section 1 para 11 sentence 1 no 7 KWG.

25 BaFin, 'Notes on Financial Instruments in Accordance with Section 1 Para 11 Sentences 1 to 5 KWG' (2011, edited 2020) point 2.b) gg) <www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Merkblatt/mb_111220_finanzinstrumente.html> accessed 30 November 2020.

26 Lars Klöhn and Nicolas Parhofer, 'Bitcoins sind keine Rechnungseinheiten—ein Paukenschlag und seine Folgen' [2018] ZIP 2093ff; Andreas Rolker and Marcus Strauß 'Bitcoin & Co.—eine angemessene Regulierung auf dem Weg?' [2019] WM 489 ff; Gerald Spindler and Martin Bille, 'Rechtsprobleme von Bitcoins als virtuelle Währung' [2014] WM 1357, 1362.

also been rejected in a decision of the Higher Regional Court (*Kammergericht*) of Berlin in connection with the application of a criminal provision contained in the German Banking Act (KWG), which has attracted considerable attention in Germany.[27] This assessment is based, on the one hand, on the assumption that the concept of "unit of account" also requires a certain stability of value and general recognition in order to ensure comparability.[28] On the other hand, German constitutional law places greater demands on interpretation in the case of criminal offences. The wording constitutes the limit of permissible variants of interpretation. Analogies which establish criminal liability are thus prohibited.[29] Since the German supervisory authority has maintained its legal interpretation of the concept of units of account,[30] the literature has analysed to what extent this "split interpretation" can be justified by the methodological differences between supervisory law on the one hand and criminal law on the other.[31] This research is a typical consequence of the need to legally qualify previously unknown facts involving digital objects into existing legal categories. The categorisation requires an examination of the methodological premises and their relation to individual elements of the context.

In addition to these adjustments to the categorisation, the German legislator has also introduced a new category, "cryptographic values",[32] and a new, related category of "crypto-custody business" into the catalogue of supervisory facts.[33] With the introduction of the category of crypto values as a financial instrument, the supervisory authority now has a means of reference that is independent of qualification as an "accounting unit".[34]

2.1.1.2 REGULATORY ASSESSMENT OF THE ACTIVITIES

Beyond this classification of virtual units as financial instruments, the scope of application of banking supervision presupposes that the activities in question meet the definition of particular forms of banking transactions or financial services. For example, the creation of virtual currencies, such as the mining of Bitcoin, and

27 Kammergericht Berlin, decision of 25 September 2018, 161 Ss 28/18 (35/18).
28 Ibid paras 8ff.
29 GG art 103 para 2; BVerfGE 91, 1 (12); 126, 170 (197–98).
30 BaFin, 'Notes on Financial Instruments in Accordance with Section 1 para 11 Sentences 1 to 5 KWG' (2011, edited 2020) pt 2. b) gg) <www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Merkblatt/mb_111220_finanzinstrumente.html> accessed 12 January 2021.
31 Dörte Poelzig, 'Die "gespaltene Auslegung" von Verhaltensnormen im Straf-, Aufsichts- und Zivilrecht oder wer gibt den Ton an?' (2019] 31 ZBB 1.
32 German Banking Act (Gesetz über das Kreditwesen, KWG) section 1 para 11 sentence 1 no 10 and sentences 4 and 5.
33 KWG Section 1 para 1a no 6.
34 The BaFin subsequently classifies virtual currencies both as a unit of account and as a crypto value, BaFin, 'Notes "Virtual Currency"' (2020) <www.bafin.de/DE/Aufsicht/FinTech/VirtualCurrency/virtual_currency_node.html> accessed 30 November 2020.

their subsequent use for the company's own purposes does not in itself constitute the taking over of a financial instrument for placement at the company's own risk and thus not yet an issuing transaction.[35] Nor is it a financial service in the form of the placement of financial instruments without a firm underwriting commitment, so-called placement business.[36] Finally, the subsequent use of the virtual units as a means of exchange or payment does not constitute either the brokerage of transactions for the acquisition or sale of financial instruments (investment brokerage) or their acquisition or sale on behalf of third parties (acquisition brokerage).[37] The creation of virtual units, even if the unit itself is to be classified as a financial instrument, is in principle not regulated, because the supervisory rules refer to further activities relevant to financial markets.[38] However, something else may result from the structure of the creation process, for example, if several participants join together in a so-called mining-pool, jointly provide the computing power required for the creation of a unit and the cooperation involves the administration of funds or units for others.[39]

Finally, gaps in the prudential framework for digital currencies may arise from the fact that activities requiring regulation differ between digital and conventional currencies and that the differences cannot be addressed even by a teleological interpretation. Such gaps require amendments or adjustments to the legal framework. For example, the newly introduced crypto-custody business covers certain activities for which there is no comparable need for regulation when dealing with conventional currencies, namely the management and protection of cryptographic assets including private cryptographic keys. The facts of the case thus represent a specific supplement to the existing regulations for digital matters.[40]

2.1.2 Stablecoins as E-Money?

In the law on payment services, a similar aspect of categorisation concerns the question whether stablecoins can be classified as electronic money. National rules on electronic money are based on a European Union Directive which already defines the notion of electronic money.[41] It defines electronic money as any monetary value stored electronically in the form of a claim on the issuer which is issued in exchange for a sum of money with a view to making certain payment transactions and which is accepted by natural or legal persons other

35 Section 1 para 1 sentence 2 no 10 KWG.
36 Section 1 para 1a sentence 2 no 1c) KWG.
37 Section 1 para 1a sentence 2 nos 1 and 2 KWG.
38 See Eduard Hofert, *Regulierung der Blockchains* (2018) Mohr Siebeck, 143ff.
39 Ibid 147.
40 Johannes Blassl and Philipp Sandner, 'Kryptoverwahrgeschäft' [2020] WM 1188, 1190ff.
41 Directive 2009/110/EC on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC [2009] OJ L267/7 (Dir 2009/110/EC).

than the issuer of electronic money.[42] Whereas in the case of virtual currencies consisting exclusively of blockchain-based units, there is no claim against an issuer from the outset; in the case of stablecoins, the linking of the virtual unit to a security can lead to a payment claim by the holder of the stablecoin if the holder requests the exchange into a sovereign currency. Whether such a claim exists is, of course, a question of the contractual arrangement. It is moreover an open question whether it is also sufficient that the claim for payment is not directed against the legal entity which issued the virtual currency, but against another person, typically the authorised reseller.[43] Above all, the concept of e-money is designed to digitally represent the value of a sovereign currency.[44] Electronic money should therefore have a face value and be exchangeable at any time at that face value.[45] There is no nominal value for stablecoins, where the terms of redemption depend on market developments. Their market value is based on the supply and demand for the stablecoin on the one hand and on the market development of the underlying collateral on the other. The better reasons therefore suggest that stablecoins do not fit into the category of e-money, at least *de lege lata*.[46] Nevertheless, the classification of stablecoins as electronic money is controversial.[47] This divergence in categorisation illustrates both the difficulty and the leeway in concretising legal concepts such as e-money and their impact on the qualification of digital currencies.

The European Commission perceives this legal uncertainty and the limits in the scope of the rules on electronic money as gaps in the protection of users. In essence, the existence of a claim by the holder of the virtual units for payment in a nominal currency is a conceptual precondition for the existence of e-money under the current rules. Virtual units, which as so-called stablecoins are secured by a nominal money currency, but for which a claim to payment is not provided at all or only to a limited extent, therefore do not fall under the definition of stablecoin. However, precisely this restriction does entail risks for users. The Commission's proposal for

42 Ibid art 2 no 2; Section 1 para 2 sentence 3 German Payment Services Supervision Act (Gesetz über die Beaufsichtigung von Zahlungsdiensten, ZAG).

43 The German supervisory authority BaFin advocates a broad understanding of the term, which also covers claims against third parties, BaFin, 'Merkblatt Hinweise zum Zahlungsdiensteaufsichtsgesetz (ZAG)' (2011, edited 2017) pt 4. a) aa) <www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Merkblatt/mb_111222_zag.html> accessed 30 November 2020.

44 Tobias Adrian and Tommaso Mancini-Griffoli, 'The Rise of Digital Money' (2019) IMF Fintech Note 19/01, 4 <www.imf.org/en/Publications/fintech-notes/Issues/2019/07/12/The-Rise-of-Digital-Money-47097> accessed 30 November 2020.

45 Dir 2009/110/EC (n 41) art 11 paras 1 and 2, recital (18); Section 33 para 1 ZAG.

46 Cf the categorial distinction between virtual currencies and e-money in Tobias Adrian and Tommaso Mancini-Griffoli (n 46) 3ff; Gerald Spindler and Martin Bille, 'Rechtsprobleme von Bitcoins als virtuelle Währung' [2014] WM 1357, 1361.

47 For an overview of the German discussion see Katja Langenbucher, Marc Hoche, Jasper Wentz, in Katja Langenbucher, Dirk H Bliesener and Gerald Spindler (eds), *Bankrechtskommentar* (3rd edn, 2020) C.H.Beck, ch 11 paras 45ff.

a Regulation on Markets in Crypto-Assets[48] therefore provides for the introduction of a new category of "e-money tokens", which generally subject crypto values based on a sovereign currency to regulatory requirements.[49] According to the proposal, e-money tokens should be defined as a type of crypto-asset, the main purpose of which is to be used as a means of exchange and that purports to maintain a stable value by referring to the value of a fiat currency that is legal tender.[50] Under the proposed new rules, both the public offering of e-money tokens and their trading on a cryptographic trading platform in the European Union will in principle require authorisation, including prior authorisation as a bank or as an e-money institution.[51] In addition, the public offering of e-money tokens and the admission to trading will in future require the prior publication of a crypto-asset white paper by the issuer, including a detailed description of the actors involved, the rights and obligations associated with the e-money token and the risks.[52] Finally, holders of e-money tokens will in future have a mandatory claim against the issuer based on the nominal value of the token.[53]

2.1.3 Civil Law

The virtual character of digital currencies also causes considerable difficulties regarding categorisation in civil law. As virtual currencies, unlike cash, are not physical objects, it is unanimously agreed upon that they do not constitute objects[54] within the meaning of German civil law.[55] Moreover, in contrast to scriptural money, for example, the ownership of individual units of virtual currency is not linked in principle[56] to any individual claim.[57] Finally, it would be conceivable to qualify the individual units of virtual currency as a form of intellectual property rights. However, in the case of copyright as the most feasible IP right, the creation of a unit, such as the mining of a Bitcoin, lacks the necessary personal creative effort by a person.[58] Units of virtual currency are neither a thing nor a claim, even though they are used as de facto functional equivalents to cash or scriptural money. They can only be classified as "other objects" in the German civil law

48 Commission, 'Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and Amending Directive (EU) 2019/1937' COM (2020) 593 final.
49 Ibid recital (10).
50 Ibid art 3 para 4.
51 Ibid art 43 para 1.
52 Ibid art 46 paras 1 and 2.
53 Ibid art 44 paras 2–4.
54 German Civil Code (Bürgerliches Gesetzbuch, BGB) section 90.
55 Langenbucher (n 20) 405; Langenbucher, Hoche, Wentz (n 47) ch 11 paras 45ff.
56 The situation is different for electronic money and, depending on its design, for so-called stablecoins.
57 Langenbucher (n 20) 405.
58 German Copyright Act (Urheberrechtsgesetz, UrhG) Section 2 para 1; Markus Kaulartz, 'Die Blockchain-Technologie' [2016] CR 474, 478.

system. These legal differences in categorisation have consequences both in the transfer and in the integration into contractual and legal obligations.[59]

In the absence of a physical object, the ownership of virtual currency cannot be transferred in accordance with the rules on the transfer of movable property.[60] Similarly, the rules on the assignment of claims do not directly cover the transfer of the purely actual position.[61] The predominant view in the literature therefore assumes a transfer of the units of virtual currencies according to the rules for other items.[62]

When applying the rules on contractual obligations, the units of virtual currencies cannot be understood as "money" in the civil law sense because they are not officially recognised.[63] Consequently, contracts such as, in particular, contracts of sale involving the payment of money in return cannot be directly applicable to situations in which virtual currencies are to be used as consideration. Nevertheless, such situations can generally be represented as exchange contracts with the respective implications, for example, for warranty law.[64]

More difficult to establish is the legal protection of virtual units against persons who are not contractual partners. The typical tort law general clause in German tort law presupposes that the ownership of a physical object or other right is affected.[65] As a result of this limitation, case law has in a number of examples concerning digital matters referred to the corresponding data storage media. The claim for an infringement of ownership of the physical data storage medium also covers damage that has occurred to the data stored on it. However, this dogmatic construction does not work for virtual currencies, which cannot be attributed to a specific physical hardware. Damage to units of virtual currency cannot typically be understood as indirect damage resulting from a violation of physical property. The attribution of virtual units as other rights in the sense of the German general clause on tort law also presupposes a comparable legal attribution of the digital unit to its owner, which is lacking or at least dubious in the absence of legal regulations.[66] Similar gaps arise essentially in other bases of claims of further legal obligations, especially in the law of unjust enrichment.[67]

As an interim result for the civil law protection of virtual currencies, it can be said that contract law is reasonably flexible in dealing with virtual units which cannot be classified in the familiar categories of physical and digital means of

59 On law of succession see Anja Amend-Traut and Cyril H Hergenröder, 'Kryptowährungen im Erbrecht' [2019] ZEV 113.
60 BGB (n 54) section 929ff; Katja Langenbucher (n 20) 410.
61 Langenbucher (n 20) 410.
62 Ibid.
63 Matthias Terlau, in Herbert Schimansky, Hermann-Josef Bunte and Hans Jürgen Lwowski (eds), *Bankrechts-Handbuch* (5th edn, 2017) C.H.Beck, § 55a paras 151ff.
64 Langenbucher (n 20) 413; Terlau (n 63) § 55a para 157.
65 BGB (n 54) section 823 para 1 BGB; Langenbucher (n 20) 410.
66 In favour of a classification of value-bearing data that can be acquired and disposed of as other rights Langenbucher (n 20) 409.
67 Ibid 408–09.

payment. However, the civil law framework of virtual currencies has gaps in relation to third parties with whom there are no contractual relations, and in particular in the protection against unauthorised access or manipulation.[68] With virtual currencies such as Bitcoin, these gaps may be understood as being inherent in the concept. A virtual entity, which sees itself as independent of a specific legal system, provides protection against unauthorised access according to its own understanding through the design of the algorithm, most notably through the mechanism of validation of transactions on the blockchain.[69] However, if, on the one hand, virtual currencies are to be integrated into existing instruments such as consumer protection law or securities law and, on the other hand, are to be linked to other collateral as stablecoins, more extensive civil law recognition of virtual units would be beneficial.

Such civil recognition could consist in introducing a separate category of property for virtual currencies and treating them as a physical object. Such a solution would treat virtual currencies like cash in many instances. However, in some cases, such as transfers, the rules explicitly link them to the possession of physical objects. Another solution could be to make the transfer and entitlement to virtual currencies conditional upon registration in a register.

2.1.4 Securities Law

In the case of bonds, for example, the German legislator recently introduced a securities register in which registration replaces the existing requirement for a securities certificate, while at the same time ensuring the protection of ownership and legal certainty in legal transactions.[70]

In addition to a central register of electronic securities,[71] the category of "crypto asset register" is to be established as the electronic securities register for crypto-assets, in which transaction-relevant data is stored decentrally, chronologically and tamper-proof.[72] The registry administrator is appointed by the issuer of the crypto-asset and can therefore, in contrast to the central register for electronic securities, be selected from a variety of private parties. The legal regulations impose certain requirements, in particular on the operation of the register including liability,[73] the content of the register including consultation,[74] supervision[75] and the publication of the issue.[76] Following the registration in the register, the

68 Ibid 406: In certain contexts, a solution under company law may also be considered, in which all actors involved in the issue and use of a virtual currency are linked by a special relationship. However, such a construction is limited to closed user groups.

69 See 1.1.1).

70 Bill on the introduction of electronic securities (Gesetz zur Einführung elektronischer Wertpapiere, eWpG), 3 June 2021, Federal Law Gazette 2021, 1423.

71 eWpG (n 70) section 12 para 1.

72 Ibid section 16 para 1.

73 Ibid section 7.

74 Ibid sections 10, 17.

75 Ibid section 11.

76 Ibid section 20.

law lays down separate rules for disposal of electronic securities, including rules for transfers and acquisitions in good faith.[77]

2.2 Specific Challenges of Digitality

In addition to these issues of the classification of digital facts in legal categories, the characteristics of digital currencies pose significant challenges regarding supervision. Banking supervision law sometimes reacts with a regime specific to virtual currencies.

2.2.1 Prevention of Money Laundering and Financing of Terrorism

This specific regime concerns firstly the prevention of money laundering and terrorist financing. Privately issued virtual currencies are particularly susceptible to misuse, especially if they can be operated worldwide, independently of government recognition, and allow anonymous transactions. Nevertheless, the technical characteristics of virtual currencies also offer opportunities to combat money laundering activities which do not exist in this form for cash or scriptural money. For example, the origin and progress of incriminated funds can be permanently traced by means of the blockchain, even if the actors behind individual addresses may be unknown. The specific risk profile as well as the measures required by the supervisory authorities therefore depend largely on the technical characteristics of the virtual currency in question. Applications such as mixers or thumblers, which, by mixing transaction flows, are intended to exclude or impede traceability on the blockchain, increase the degree of suspicion and thus make specific anti-money laundering treatment necessary.[78] At the same time, the fight against money laundering and the financing of terrorism highlights the international dimension of supervisory law. Without cross-border coordination of measures and standards, the ability of individual states to assess and contain risks without unduly impairing legal financial flows is limited. For this reason, the Financial Action Task Force, an intergovernmental body, constantly monitors the global activities of money laundering and terrorist financing, including their economic and technical facets,[79] and develops indicators[80] and recommendations on this basis, in particular for virtual currencies including stablecoins.[81]

77 Ibid sections 24ff.

78 Hofert (n 38) 102ff.

79 See lately FATF, 'The Impact of COVID-19 on the Detection of Money Laundering and Terrorist Financing' (*webinar*, 31 July 2020) <www.fatf-gafi.org/publications/methodsandtrends/documents/covid-19-webinar-mltf-detection.html> accessed 30 November 2020.

80 FATF, 'Terrorist Financing Risk Assessment Guidance' (5 July 2019).

81 FATF, 'Virtual Asset Red Flag Indicators of Money Laundering and Terrorist Financing' (31 July 2020), discerning red-flag indicators related to transactions, to transaction patterns, to anonymity, to geographical risks as well as indicators about senders or recipients or in the source of funds or wealth; FATF, 'Report to G20 on So-called Stablecoins' (7 July 2020); FATF, 'Virtual Currencies: Key Definitions and Potential AML/CFT Risks' (27 June 2014).

2.2.2 Investor and Consumer Protection in the Issuing of Virtual Currencies

In the past, the issue of virtual units by individual actors has in some cases led to considerable losses for investors.[82] Such so-called Initial Coin Offerings provided the issuing company with functional equivalents for forms of capital raising which are much more strictly regulated and thus ensure a higher level of investor and consumer protection. The differences in the level of regulation are also due to the fact that, although the virtual units may have the same significance as shares, depending on the design of the tokens they may not fall into the categories of securities law.[83] The Commission's proposal for a Regulation on Markets in Crypto-Assets therefore provides for more detailed requirements for the issuance of crypto-assets.[84] In particular, issuers of cryptographic assets are required to prepare a crypto-asset white paper with detailed descriptions of the project, the legal structure and the risks[85] and to notify this white paper to the competent authority.[86] Both the issuers and its management bodies should in future be liable for damages caused by incomplete or misleading information in the white paper.[87]

2.2.3 Specific Regulatory Requirements for "Value-Referenced Tokens"

The proposal for a Regulation on Markets in Crypto-Assets also provides for a new category of "value-referenced tokens". These are crypto tokens that are linked to a security in order to increase value stability. This security can consist of sovereign currencies, goods, other cryptographic values or a combination thereof.[88] The new rules to be introduced for value-referenced tokens serve on the one hand the protection of consumers and investors, but also the stability of the financial markets. Issuers of value-referenced tokens require admission for the public offering of the tokens or admission to trading on a trading platform, which

82 For an overview of potential risks see European Securities and Markets Authority, 'Advice Initial Coin Offerings and Crypto-Assets' (9 January 2019) ESMA50–157–1391, 13–14.

83 See Peter Zickgraf, 'Initial Coin Offerings—Ein Fall für das Kapitalmarktrecht?' [2018] AG 293.

84 Commission, 'Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and Amending Directive (EU) 2019/1937' COM(2020) 593 final, art 4 para 1; particular crypto-assets are excluded by art 4 para 2; according to art 3 para 1(2) of the proposal, crypto-asset means a digital representation of value or rights which may be transferred and stored electronically, using distributed ledger technology or similar technology.

85 Ibid art 5 para 1.

86 Ibid art 7.

87 Ibid art 14 para 1.

88 Ibid art 3 para 1 no 3 and 4 (as distinct from e-money tokens, value-referenced tokens refer to different nominal currencies and their main purpose need not be to serve as a medium of exchange).

also requires, among other things, the publication of a crypto-asset value white paper.[89] The crypto-asset white paper will contain, *inter alia*, detailed descriptions of the asset reserves, the custody arrangements, the modalities of investment of the reserve assets and the legal positions of the token holders.[90] As in the case of the white papers for crypto-assets, both the issuer and its management body are liable for damages resulting from incomplete, incorrect or misleading information in the white paper.[91] In addition issuers should also be required to communicate fairly, clearly and not misleadingly, including in marketing communications.[92]

In addition to these investor protection requirements, the further requirements for issuers of value-referenced tokens approximate the regulatory situation of credit institutions.[93] These include requirements relating to the internal corporate structure, internal compliance strategies and experience, and the reliability of the members of the management bodies,[94] but also requirements relating to equity capital.[95] The proposal for a Regulation on Markets in Crypto-Assets also provides for detailed rules on the custody and management of the reserve assets, including the issuer's access to the reserve assets to satisfy redemption requests.[96] Finally, the redemption option for token holders will be ensured by requiring issuers to either provide clear and enforceable redemption rights vis-à-vis issuers or in respect of reserve assets, or to ensure that a sufficient number of third-party providers offer redemption at market conditions.[97]

Specific obligations are also envisaged for so-called significant value-referenced tokens, which are intended to further increase protection against non-payment in view of the special network effects of digital ecosystems and also to ensure redeemability during operation. The classification of value-referenced tokens as significant is based on six factors. Similar to credit institutions, the factors are related to volume[98] and the interdependence with the financial system.[99] However, due to the transfer of network effects from the digital ecosystem,[100] the size of the customer base of companies behind the value-referenced token is also

89 Ibid arts 15 and 16.
90 Ibid art 17 para 1.
91 Ibid art 22 para 1.
92 Ibid arts 23 and 25.
93 Similarly, regulatory gaps have been identified in the United States in the supervision of peer-to-peer payment platforms and stablecoins and the introduction of a National Money Act has been called for, Dan Awrey, 'Bad Money' (2020) Cornell Law School Research Paper No 20–38 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3532681> accessed 30 November 2020.
94 COM(2020) 593 final (n 84) art 30 paras 1–3.
95 Ibid art 31.
96 Ibid arts 32–34.
97 Ibid art 35 paras 1–4.
98 In terms of the tokens issued, the transactions made with them and the volume of the reserve.
99 COM(2020) 593 final (n 84) art 39 para 1.
100 See I.1.b) cc).

taken into account.[101] As a consequence, for issuers of significant value-referenced tokens, requirements are envisaged in terms of a risk-friendly remuneration policy, ensuring redemption possibilities via third-party providers, monitoring liquidity management and the level of equity capital.[102]

3 Conclusion

The prudential treatment of digital currencies is to a large extent characterised by the classification and adaptation of digital issues into the established categories. However, digital currencies have technical and economic characteristics which distinguish them structurally from sovereign currencies, especially with regard to their cross-border circulation. These differences remain even if sovereign currencies are digitised in the form of scriptural money. These characteristics give rise to specific prudential needs, in particular for investor and consumer protection and the prevention of money laundering and terrorist financing. Stablecoins can also, if they reach a certain volume, affect the stability of financial markets or the effectiveness of monetary policy measures by central banks. Proposals to regulate crypto-assets, including virtual currencies, are aimed at allowing their issuance and trading within the European Union only under certain conditions. The categories newly introduced for different forms of crypto-assets bring virtual currencies closer to the established regimes of prudential regulation. In doing so, they adopt particular rules which take account of the specific characteristics of digital currencies.

101 COM(2020) 593 final (n 84) art 39 para 1 lit) a): size of the customer base of the promoter of the asset-referenced tokens, the shareholders of the issuer of asset-referenced tokens or of any of the third-party entities that are involved in the operating, investment, custody or distribution of the reserve assets.

102 Ibid art 41 paras 1–4.

10 Criminal Law of Global Digitality

Characteristics and Critique of Cybercrime Law

Beatrice Brunhöber

Along with the growth of digital activity in past decades, harmful behavior is on the rise in "cyberspace" where it threatens commerce, businesses, private communications and public institutions.[1] Governments quickly realized that this global phenomenon cannot be addressed by domestic laws alone and turned to international organizations to protect society against threats in "cyberspace". In the 1990s, the Council of Europe became one of the first and the leading multilateral institution to respond to this growing problem with a call for criminalizing certain harmful digital activities. This led to the adoption of the Council of Europe Convention on Cybercrime in 2001.[2] Since the 1990s, the United Nations has also addressed cybercrime with several policy measures focusing especially on capacity building and sharing technical knowledge among developing countries in the area of criminal prosecution.

This contribution serves as critique of current criminal law regulations of global digitality. First, it defines criminal law of global digitality as "cybercrime" and examines the history and shortcomings of the term "cybercrime". Next follows an analysis of the particular global challenges which arise from cybercrime. In the next two sections, the analysis differentiates between legislative and policy approaches to cybercrime, before examining the specific regulations and policies implemented in past decades. It concludes with a discussion of the characteristics of global digitality criminal law and the weaknesses of current cybercrime law.

In what follows, I argue that individual liberties are threatened by cybercrime prohibitions (substantive criminal law). Technical developments and cybercrime regulations also increase the possibilities of surveillance of law enforcement authorities ranging from satellite tracking to data mining. Furthermore, respect for the suspect's procedural rights, privacy rights and rule-of-law values plays a minor role in cybercrime legislation (procedural criminal law). In addition, the global dimension of cybercrime provokes jurisdictional conflicts that must

1 For an overview of damages from cybercrime see Nir Kshetri, *The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives* (2010) Springer, 4–6.

2 Budapest Convention on Cybercrime (adopted 23 November 2001, entered into force 1 July 2004) 2296 UNTS 167 (Convention on Cybercrime).

DOI: 10.4324/9781003283881-16

be addressed, for example, when it comes to determining where the crime was committed.[3] However, these challenges raise different issues of principle that are widely debated among critics of cybercrime law.

1 Defining Criminal Law of Global Digitality

1.1 From Computer Crime to Cybercrime

Currently "cybercrime" is the prevailing academic and legislative term used in discussing regulation of digital activity through criminal law. However, difficulties arise in defining the term stemming from its history, the scope of "cyberspace", the crossborder character of digital activity, and the lack of theoretically driven research.[4]

Scholars differ on what to name the criminal regulation of digital activity, so that numerous alternative proposals are in circulation for "cybercrime"—a term coined relatively recently. Prior to this, the term "computer crime" had a widespread use. Donn B. Parker probably first defined it in 1976 as crime in which a computer is (1) the object of the crime, (2) the environment where the crime takes place, (3) the instrument for committing the crime, or (4) the symbol of a crime (e.g. to pretend using a computer program to enable a crime).[5] Even though "cybercrime" is now in the ascendancy, recent definitions still closely rely on Parker's criteria for its content. Most contemporary definitions hold that "cybercrime" entails either using a digital device like a computer as an integral part of committing a crime or making a computer system the object of the crime.[6]

"Computer crime" and similar terms fell into disuse because of their limitations in describing the multiplying types of criminal regulation of digital activity.[7]

3 On the lack of adequate privacy protections, see, for example, Susan W Brenner, 'The Council of Europe's Convention on Cybercrime' in Jack M Balkin and others (eds), *Cybercrime: Digital Cops in a Networked Environment* (2007) NYU Press, 215; Patrick Breyer, 'Die Cyber-Crime-Konvention des Europarats' (2001) 10 DuD 592, 595; on unjustified expansion of investigative powers see Brian Valerius, 'Der Weg zu einem sicheren Internet?' (2004) 11 K&R 513, 517–18; Laura Huey and Richard S Rosenberg, 'Watching the Web: Thoughts on Expanding Police Surveillance Opportunities under the Cyber-Crime Convention' (2004) 46(5) CICCJ 597; on jurisdictional conflicts see Susan W Brenner and Bert-Jaap Koops, 'Approaches to Cybercrime Jurisdiction' (2004) 4(1) J High Tech L 10; Amalie M Weber, 'The Council of Europe's Convention on Cybercrime' (2003) 18(1) Berkeley Technology LJ 425, 427, 444.

4 Brian K Payne, 'Defining Cybercrime' in Thomas J Holt and Adam M Bossler (eds), *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, (2020) Palgrave Mcmillian, 3–4; Kyung Shick Choi and others, 'Historical Evolutions of Cybercrime: From Computer Crime to Cybercrime' in ibid 27.

5 Donn B Parker, *Crime by Computer* (1976) Charles Scribner's Sons.

6 See for example Convention on Cybercrime (n 2) art 1(a).

7 Payne (n 4) 10.

"Computer crime"[8] does not cover the multifarious activities in which newly developed digital devices such as smartphones are used instead of computers. The terms "digital crime"[9] and "information and communication technology crime"[10] are more apt. However, they suggest that committing the crime requires "digital" or "technological" skills on the part of the perpetrator. Calling it "internet crime"[11] leaves out offenses that solely rely on a computer or on merely manipulating a computer system without using the internet. The terms "technocrime"[12] and "information and communication technology crime" suggest that the phenomenon is confined to the technological sphere. However, many cyber offenses also occur in the analog world (e.g. fraud, defamation). The word "virtual crime"[13] was proposed to only designate crimes committed in video game settings, and therefore would only cover a tiny part of the cyber offense spectrum.

The term "cybercrime" may also be criticized on several grounds, but will be used in this chapter because of its prevalence. Nevertheless, its blind spots and path dependencies call for examining it critically. The term could be said to fall short due to its non-academic evolution, its vagueness, the crossborder character of digital conduct and the predominance of practical research.

The term "cybercrime" did not originate in academia. As postmodern deconstruction theories show, definitions and narratives greatly influence how a phenomenon is analyzed.[14] In the academic sphere, initially the term "cybernetics"

8 Robert Richardson, '2008 CSI Computer Crime and Security Survey' (2008) 8 Computer Security Issues and Trends 1; Richard C Hollinger and Lonn Lanza-Kaduce, 'The Process of Criminalization: The Case of Computer Crime Laws' (1988) 26(1) Criminology 101.

9 Greg Gogolin, 'The Digital Crime Tsunami' (2010) 7(1–2) Digital Investigations 3; Hollinger and Lanza-Kaduce (n 8); Richardson (n 8); Panagiotis Kanellis, *Digital Crime and Forensic Science in Cyberspace* (2006) Idea Group Inc; Robert W Taylor and others, *Digital Crime and Digital Terrorism* (3rd edn, 2015) Pearson.

10 'IuK Kriminalität' (short for "Informations- und Kommunikationstechnologie Kriminalität", in English "information and communication technology crime") was the predominant term in use by German criminal lawyers as well as German law enforcement authorities for the last two decades; today, the term "cybercrime" has been adopted, for example, by the German Federal Police (Bundeskriminalamt); Christoph Keller and others, *Cybercrime* (2019) Deutsche Polizeiliteratur, 13.

11 David Wall, 'Policing Identity Crimes' (2013) 23(4) Policing and Society 437; Yvonne Jewkes and Majid Yar, *Handbook of Internet Crime* (2010) Willan; Maxwell Taylor and Ethel Quayle, *Child Pornography: An Internet Crime* (2003) Routledge.

12 See Kevin F Steinmetz and Matt R Nobles (eds), *Technocrime and Criminological Theory* (2018) Routledge; David O Friedrichs, *Trusted Criminals* (4th edn, 2010) Cengage Learning.

13 F Gregory Lastowka and Dan Hunter, 'The Laws of the Virtual Worlds' (2004) 92 Cal Crim Law Rev 73; Susan W Brenner, 'Is There Such a Thing as "Virtual Crime"' (2001) 4 Cal Crim Law Rev 1.

14 See generally Jacques Derrida, *De la Grammatologie* ([1967] 1997) Les Éditions De Minuit; on the "cyber" prefix see Adrienne L McCarthy and Kevin F Steinmetz, 'Critical Criminology and Cybercrime' in Thomas J Holt and Adam M Bossler (eds), *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (2020) Palgrave Mcmillian 612–16; Brian G Sellers and Bruce A Arrigo, 'Postmodern Criminology and Technocrime' in Kevin F Steinmetz and Matt R Nobles (eds), *Technocrime and Criminological Theory* (2018) Routledge, 133.

was used to designate the study of machines and feedback systems.[15] US researchers may have ceased using the term when Soviet scientists also started referring to the new information technologies as "cybernetics".[16] "Cyberspace" was first used by science fiction novelist and essayist William Gibson in 1982, who earned his principal claim to fame as the creator of the subgenre of cyberpunk literature dealing with the impact of technological developments on humans.[17] Since the 1990s, the trend has been what might be called "cyberhype", as McKenzie Wark put it, to refer to new possibilities derived from proliferating information technologies by attaching the prefix "cyber" to them with a positive connotation (cyberspace, cybershopping, cybersex, cybersurfing).[18]

For the past two decades, the word has no longer been used for new technology applications; instead, it now designates harmful or illicit conduct (cyber harassment, cyber racism, cyberterrorism, cyberwar, etc.).[19] However, the term "cyber" does not explain the phenomenon to which it is attached; it rather implies that there is a specifically technical challenge that requires a technical solution. These challenges are not treated as social conflicts and problems that were prevalent in the "offline" world long before they became "online" challenges (harassment, racism, terrorism, war, etc.). The focus on "new technology creates new criminal opportunities" obscures vested economic as well as state interests that may motivate calls for criminalizing activities, such as the call for penalizing "digital piracy" to protect copyrighted content.[20]

"Cyberspace", as the place where cybercrime presumably happens, recently has radically expanded its boundaries in large measure. Arguably, cyberspace was never a scientifically definable "space" but instead a fictional description (William Gibson) of the digital world. Today computers and other devices connected to the internet are ubiquitous, making it difficult to distinguish between behavior in "cyberspace" on the one hand and in the "offline" world on the other hand. Offenders are likely to use information technology even if it consists only

15 Thomas Rid, *Rise of the Machines* (2016) W.W. Norton and Company; Norbert Wiener, *Cybernetics: Or Control and Communication in the Animal and the Machine* (1948) The MIT Press.

16 Felix Stalder, *Kultur der Digitalität* (4th edn, 2019) Suhrkamp, 82.

17 David S Wall, 'Cybercrime and the Culture of Fear' (2008) 11(6) Inf Commun Soc 861, 867; David S Wall, *Cybercrime: The Transformation of Crime in the Information Age* (2007) Polity; William Gibson, 'Burning Chrome' (1982), in William Gibson (ed), *Burning Chrome* (1986) Arbor House, 168.

18 McKenzie Wark, 'Cyberhype' in Ashley Crawford and Ray Edgar (eds), *Transit Lounge* (1997) Craftsman House, 154.

19 Steinmetz and Nobles (n 12) 3; McCarthy and Steinmetz (n 14) 606; Majid Yar, *The Cultural Imaginary of the Internet* (2014) Palgrave Pivot; David S Wall, 'The Devil Drives a Lada: The Social Construction of Hackers as Cyber-Criminals' in Christina Gregoriou (ed), *Constructing Crime: Discourse and Cultural Representations of Crime and Deviance* (2012) Palgrave Mcmillian, 5; Jussi Parikka, *Digital Contagions. A Media Archaeology of Computer Viruses* (2007) Peter Lang Inc.

20 McCarthy and Steinmetz (n 14) 601.

of their mobile phone or a car with a navigation system. As David Wall states: "Particularly confusing is the tendency to regard almost any offense that involves a computer as a cybercrime".[21] New technologies such as the Internet of Things contribute to the nebulous nature of the "cyberspace" realm. Since early on in the discussion, therefore, multiple commentators have categorized cybercrime as merely ordinary crimes that happen to be committed by using or by targeting a computer system.[22]

The crossborder nature of cybercrime complicates the search for definitions. Crime is often defined according to cultural conceptions of social conflicts and harms. For example, what is seen as illicit prostitution may differ across cultures. If there is a crossborder dimension, the conduct may only be seen as harmful from the perspective of one of the countries involved. The definition of "cybercrime" may also be shaped by legal requirements that differ from country to country. Especially when it involves content offenses, the constitutional restrictions on criminalizing certain types of speech differ greatly. For example, the German Criminal Code prohibits holocaust denial,[23] whereas in the US it is protected by the constitutional right to free speech.

A number of academic books and articles on "cybercrime" focus on its technical and practical aspects, for instance, explaining the technical aspects of malware, DoS attacks, etc. or detailing the kinds of evidence for use by law enforcement authorities.[24] These presentations, instead of engaging in systematic or critical analysis, are merely descriptive and frequently cannot be scientifically validated.[25] As critical criminology points out, often such works embrace the idea that new technologies create new opportunities for criminal conduct simply by relying on subjective reports of increased harms from copyright companies, cybersecurity companies, media and governments.[26] Most authors of such surveys do not treat cybercrime as a social construct; hence, they are unable to question the normative assumptions or the economic interests that go into qualifying specific

21 David S Wall, 'What Are Cybercrimes' (2004) 58(1) Criminal Justice Matters 20.

22 For example, Brenner (n 13) 11, para 32–99; Eric J Sinrod and William P Reilly, 'Cyber-Crimes: A Practical Approach to the Application of Federal Computer Crime Law' (2000) 16(2) Santa Clara Computer & High Tech LJ 177, 180.

23 German Criminal Code (Strafgesetzbuch) sec 130(3).

24 See for example Gogolin (n 9) 3–8.

25 Neil Boister, *An Introduction to Transnational Criminal Law* (2018) Oxford University Press, 12–13; Peter Andreas, 'Illicit Globalization: Myths, Misconceptions, and Historical Lessons' (2011) 126(3) Political Sci Q 403, 408.

26 McCarthy and Steinmetz (n 14) 601; Kevin F Steinmetz and Alexandra Pimentel, 'DeLiberating the Information Commons: A Critical Analysis of Intellectual Property and Piracy' in Steven C Brown and Thomas J Holt (eds), *Digital Piracy: A Global, Multidisciplinary Account* (2018) Routledge, 185; Majid Yar, 'The Global "Epidemic" of Movie "Piracy": Crime-wave or Social Construction?' (2005) 27(5) Media Cult Soc 677; Lawrence Lessig, *Free Culture* (2004) Penguin Press. On transnational criminal law generally see Boister (n 25); Jude McCulloc, 'Transnational Crime as a Productive Fiction' (2007) 34(2) Soc Justice 19.

digital activities as harmful, such as hacking or digital piracy.[27] These analyses may overlook the fact that the rising volume of damages documented may simply reflect how ubiquitous the use of information technology has become in business, government and everyday life.

1.2 Cybercrime Offenses

Most definitions of "cybercrime" differentiate between "cyber-enabled" crime and "cyber-dependent" crime.[28] "Cyber-enabled" crime is conventional crime committed by using information technology (a "computer system" as instrument, e.g. as in cyberfraud, cyberstalking). "Cyber-dependent" crime targets information technology devices or infrastructures (a "computer system" as the object, as in computer hacking, malware). Computer systems are commonly defined as devices that process data automatically pursuant to a program.[29] Since this would encompass an electronic typewriter, some authors suggest defining cybercrime specifically in reference to its targets or intentions, for instance, as "computer-mediated activities which are either *illegal or considered to be illicit* by certain parties and which can be conducted *through global electronic networks*".[30] However, such a narrow definition would exclude crimes that skirt the internet or other networks usually listed in transnational treaties such as the Convention on Cybercrime, for example, the use of a physical device (e.g. a USB flash drive) to "infect" a computer with malware.[31]

Even the wider definition may require expansion in light of information technology's ubiquity today. In recent years, information technology has increasingly united the "physical, digital and biological domains"[32] as exemplified by the Internet of Things, "smart" homes, cloud computing, semi-automated driving, etc. More and more, devices are connected to the internet (mobile phones, cars, printers). Due to its evolving omnipresence, criminals increasingly resort to information technology in myriad ways. Consequently, most scholars and legislators

27 McCarthy and Steinmetz (n 14) 601; Majid Yar, 'The Rhetorics and Myths of Anti-piracy Campaigns: Criminalization, Moral Pedagogy, and Capitalist Property Relations in the Classroom' (2008) 10(4) New Media Soc 605.

28 See, for example, Choi and others (n 4) 27–43; David Maimon and Eric R Louderback, 'Cyber-dependent Crimes: An Interdisciplinary Review' (2019) 2(1) Annu Rev Criminol 191; Christopher Ram, 'Cybercrime' in Neil Boister and Robert J Currie (eds), *The Routledge Handbook of Transnational Criminal Law* (2015) Routledge, 379–80; Steven Furnell and others, 'The Challenge of Measuring Cyber-dependent Crimes' (2015) 10 Comput Fraud Secur 5; UNODC, *Comprehensive Study on Cybercrime* (2013) 11; Marc D Goodmann, 'Why the Police Don't Care about Computer Crime' (1997) 10(3) Harv J L & Tech 465, 469; Kyung Schick Choi, *Cybercriminology and Digital Investigation* (2015) Lfb Scholarly.

29 Convention on Cybercrime (n 2) art 1(a).

30 Chris Hale, 'Cybercrime: Facts and Figures Concerning This Global Dilemma' (2002) 18 Crime and Justice International 5.

31 Marco Gercke, *Understanding Cybercrime* (2009) ITU, 18.

32 Klaus Schwab, *The Fourth Industrial Revolution* (2017) Currency, 16.

agree that there exists no catch-all definition for "cybercrime", but instead it is useful to describe the discrete acts constituting cybercrime.

This capitulation is another indication that "cybercrime" is not a term suited for use in academic research, as noted earlier (see Section 1.1).

Most commonly, the so-called "basket of acts" is based on the three distinct groups of offenses covered by the Convention on Cybercrime arranged in three different categories (see Section 3.3): First, *access offenses*, or acts against the confidentiality, integrity and availability of computer data and systems (especially computer hacking).[33] Second, *use offenses*, or conventional offenses committed by using an information technology device for personal or financial gain or harm (e.g. computer forgery, cyberfraud).[34] Lastly, *content offenses* that are content-related crimes committed over the internet or other networks for distribution, acquisition, consumption and the like (e.g. computer-based child pornography, computer-related infringement of copyrights, "hate speech").[35]

2 The Challenging Global Dimension of Cybercrime

2.1 Global Challenges

Cybercrime's crossborder dimension poses its greatest challenge, first, because states treat their criminal law as an expression of sovereignty. It provides them with a powerful weapon for social control that protects victims, but also curtails individual liberties and thus has to be justified. Criminal law is also often shaped by and linked to (national) cultural conceptions of deviant behavior. The scope of criminal prohibitions and procedural safeguards very much depends on differing (national) constitutional requirements. Put differently, criminal law is primarily national law, and it is mainly enforced by national authorities.[36]

Second, "cyber activity" is an inherently crossborder phenomenon.[37] Most data transfer processes, from writing an email to accessing a website, take place in more than one country because any action by an internet user involves the use of servers usually located abroad. Critical infrastructures such as the water supply and everyday life activities such as driving a car are increasingly run by information technology and often integrated into computer networks,

33 Convention on Cybercrime (n 2) Title 1.

34 Ibid Title 2.

35 Ibid Title 3.

36 Henning Rosenau, 'Zur Europäisierung des Strafrechts' (2008) 1 ZIS 9; Kai Ambos, 'Is the Development of a Common Substantive Criminal Law for Europe Possible? Some Preliminary Reflections' (2005) 12(2) Maastricht J Eur Comp L 173.

37 See Jonathan Clough, 'A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonisation' (2014) 40(3) Mon U L Rev 698, 700; Marco Gercke, 'Hard and Soft Law Options in Response to Cybercrime' (2012) 3 CRi 78; Abraham D Sofaer and Seymour E Goodman, 'Cyber Crime and Security—The Transnational Dimension' in Abraham D Sofaer and Seymour E Goodman (eds), *The Transnational Dimension of Cyber Crime and Terrorism* (2001) Hoover Institution Press, 1.

turning them into targets for cybercrime that also can easily be committed from foreign soil. The internet has also facilitated increased crossborder trade, services, communications, etc. Consequently, crimes that used to be confined to one country now often involve more than one country if they are committed using the internet (e.g. computer fraud in trading or business contexts or slander on a social network). Attacks on computer systems can be easily orchestrated and carried out from abroad through the internet.

Such crimes necessitate investigations and involvement by law enforcement authorities in different countries; however, investigating in another country and enforcing the law abroad conflicts with state sovereignty.[38] The classic approach to circumventing this barrier in such cases is by countries rendering each other mutual legal assistance.

However, mutual legal assistance, especially extradition, usually requires double criminality, the prerequisites for which may not be met.[39] Dual criminality means that the act qualifies as a crime in both states. Under this principle, a suspect can be extradited from one state to be prosecuted for committing a crime in another only if a similar crime is on the books in the extraditing state. If country A has no laws against creation of malware, for example, the principle of double criminality could prevent the suspect's extradition from country A to face charges of malware creation in country B. In the case of one of the most destructive computer viruses in history, the "ILOVEYOU" computer worm, which infected over ten million computers worldwide in 2000, the authorities quickly traced it to its creator in the Philippines.[40] However, as a legal resident there, he could not be prosecuted since at the time he created the malware, it was not regarded a crime in the Philippines.

Moreover, rendering mutual legal assistance through formal channels may take too long to allow successful investigations and law enforcement. For instance, traffic data that may be relevant evidence of a crime are quickly deleted, and formal procedures to obtain evidence from another country can take weeks if not months.[41]

Last but not least, this situation may in effect create safe havens, meaning territories where certain cybercrimes are not subject to prosecution even if they have damaging effects in other countries.[42]

38 Marco Gercke, 'Vorbemerkung' in Gerald Spindler and Fabian Schuster (eds), *Recht der elektronischen Medien* (4th edn, 2019) C.H.Beck, part 9 Strafgesetzbuch para 19.

39 Ibid; David Weissbrodt, 'Cyber-Conflict, Cyber-Crime, and Cyber-Espionage' (2013) 22 Minn J Int'l L 347, 370; Weber (n 3) 427; Marc D Goodman and Susan W Brenner, 'The Emerging Consensus on Criminal Conduct in Cyberspace' (2002) 10 Intl J L & Info Tech 139, 141.

40 Paul John Cana, 'The Filipino Creator of the "Iloveyou" Virus Just Did It so He Could Get Free Internet' (*Esquire Magazine*, 4 May 2020) <https://web.archive.org/web/20200607094321/www.esquiremag.ph/culture/tech/filipino-creator-of-the-i-love-you-virus-free-internet-a00289-20200504> accessed 10 February 2021; Stefan Ernst, 'Hacker und Computerviren im Strafrecht' (2003) 45 NJW 3233, 3234.

41 Gercke (n 31) 80.

42 The problem has been addressed by several international responses to cybercrime; see for example UN-Resolution 55/63: "States should ensure that their laws and practice eliminate safe havens for those who criminally misuse information technologies" and the G 8 Ten-Point-Action Plan: "There must be no safe havens for those who abuse information technologies".

2.2 Approaches to Addressing Global Cybercrime

The two major approaches for dealing with cybercrime as a global phenomenon are legislation and policy measures. Legislation can be national, transnational and international. Both transnational and international legislation aim at harmonizing domestic substantive criminal law, because interstate cooperation often requires double criminality. A second main goal is to establish procedural rules for interstate cooperation to strengthen crossborder investigations and law enforcement. Policy approaches focus on capacity building in legislation or in law enforcement, support for cooperation in investigations, as well as on technical and educational measures. They aim at improving the skills and knowledge of social actors fighting cybercrime and of potential victims of cybercrime as well as fostering structures of interstate cooperation.

3 Legislative Approaches

At first glance, one might think due to its global reach, cybercrime must be regulated by international criminal law. However, cybercrime is to a great extent regulated by what many authors call transnational criminal law.

3.1 Distinguishing International From Transnational Criminal Law

There is broad consensus among commentators that drawing a distinction between international criminal law and transnational criminal law matters.[43] The arguments are that each establishes a different control regime, especially with regard to jurisdiction, and each underpins different justification needs.[44] Concepts that do not distinguish between international and transnational law[45] obscure the highly differentiated character of those regimes.[46]

Transnational law was originally framed by Philipp Jessup as "all law which regulates actions or events that transcend national frontiers".[47] Accordingly,

43 George P Fletcher, 'Parochial versus Universal Criminal Law' (2005) 3 JICJ 20, 23; Boister (n 25) 30–42; Vespasian V Pella, 'Towards an International Criminal Court' (1950) 44 AJIL 37, 54.

44 See Boister (n 25) 32.

45 For example, the German doctrine of "Internationales Strafrecht" (International Criminal Law) which is conceptualized as a general term. It includes all of the doctrinal categories that involve international facets of criminal law and criminal law aspects of international law: Völkerstrafrecht (international criminal law in a strict sense), Europäisches Strafrecht (European Criminal Law), Strafanwendungsrecht (criminal jurisdiction), internationale Zusammenarbeit in Strafsachen (international cooperation in criminal matters) and increasingly Transnationales Strafrecht (treaty-originating criminal law dealing with crimes of transnational character). See Kai Ambos, *Internationales Strafrecht* (5th edn, 2018) C.H.Beck.

46 See Peer Zumbansen, 'Defining the Space of Transnational Law: Legal Theory, Global Governance and Legal Pluralism' (2012) 21(2) Transnat'l L & Contemp Probs 305, 307.

47 Philipp Jessup, *Transnational Law* (1956) Yale University Press, 2.

transnational *criminal* law is law dealing with crime that transcends state borders. Transnational criminal law is established by bilateral or multilateral treaties committing each state that is a party to the treaty to criminalize certain conduct (suppression regime), and to apply corresponding criminal law to individuals in fulfilment of its treaty obligations. The suppression regimes, rather than being self-executing, require legislative acts by each treaty state. The treaties usually only contain a set of standards for definitions, elements of crime, forms of conduct, responsibility of the actors and the like. They also specify minimum rules for sanctions necessary for producing the degree of conformity between national definitions of crimes required for interstate law enforcement, especially for double criminality as the prerequisite for extradition.[48] For example, the 1988 UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances obliges the state parties to criminalize the use and distribution of certain listed substances such as heroin. The state parties fulfill the requirements by including the required drug offenses in their domestic criminal law and by prosecuting violations domestically.

In contrast, the four core international crimes stipulated by the 1998 Rome Statute of the International Criminal Code—genocide, war crimes, crimes against humanity and crimes of aggression[49]—are directly applicable to individuals.[50] The International Criminal Court can prosecute and convict individuals for international crimes committed (if states are unable or unwilling to do so themselves).[51] The state parties do not have to conform their domestic criminal law to the core international crimes addressed in the Code.

Because the foundations of transnational and international law differ, transnational criminal law is more difficult to justify. International crimes are solely serious offenses that have their source in internationally shared values, such as human dignity. Criminalization is based on the idea that causing serious harm by violating human rights or other globally shared principles must be sanctioned. In contrast, transnational criminal law only sporadically includes *crimes mala in se*. Instead, it tends to focus on regulatory offenses in connection with controlling certain markets for goods and services (e.g. drug trafficking, copyright material, illicit trade in tobacco products).[52] The resulting offenses do not have their origin

48 Boister (n 25) 25.

49 Rome Statute of the International Criminal Court (adopted 17 July 1998, entered into force 1 July 2002) 2187 UNTS 3 (Rome Statute of the International Criminal Court) art 6 to 8 *bis*.

50 Elies van Sliedregt, 'International Criminal Law' in Markus D Dubber and Tatjana Hörnle (eds), *The Oxford Handbook of Criminal Law* (2014) Oxford University Press, ch 49, 1137, 1140.

51 Rome Statute of the International Criminal Court (n 49) art 17; see van Sliedregt (n 50) 1145–46.

52 For example, the 2012 Protocol to Eliminate Illicit Trade in Tobacco Products; 1961 Single Convention on Narcotic Drugs; Boister (n 25) 24–25.

in the intrinsic harmfulness of the activity[53] but in the need for cooperation in transcending the barriers that sovereignty raises to the effective application of criminal law outside state borders.[54] For example, it is virtually impossible to control the illicit drug trade if the neighboring states do not prohibit the production and distribution of those drugs. However, unlike in the case of genocide or war crimes, it is unclear whose rights are violated or what harms are incurred by not observing market regulating rules (e.g. by selling untaxed tobacco products or by using drugs).[55] In sum, while the core international crimes can easily be justified as protecting fundamental rights and claims, transnational criminal law cannot be considered unobjectionable per se and often requires further justification.

3.2 United Nations Measures

The United Nations has not yet developed cybercrime legislation, as it already has for drug trafficking[56] or terrorist offenses.[57] The UN Office on Drugs and Crime has so far conducted only a few studies on the challenges of cybercrime.[58] It has also appointed expert groups, such as the open-ended expert group meeting on cybercrime to examine the legal and technical responses to cybercrime.[59] A UN convention on cybercrime has been debated since 2010.[60] However, the focus of the UN has shifted from legislation to policy measures because states that are party to the Council of Europe Convention on Cybercrime strenuously resisted negotiating another international treaty on cybercrime, given that the Convention is already open to non-Member States.[61] Current UN measures include the

53 An exception are human trafficking and terrorism because their "production" of the services is violent, see Boister (n 25) 24.

54 Johan David Michels, 'Keeping Dealers Off the Docket: The Perils of Prosecuting Serious Drug-related Offenses at the International Criminal Court' (2009) 21(3) Fla J Int'l L 452.

55 Beatrice Brunhöber, 'Drug Offenses' in Markus D Dubber and Tatjana Hörnle (eds), *The Oxford Handbook of Criminal Law* (2014) Oxford University Press, ch 35.

56 UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (adopted 20 December 1988, entered into force 11 November 1988) 1582 UNTS 95.

57 For example, the UN International Convention for the Suppression of Terrorist Bombings (adopted 15 December 1997, entered into force 23 May 2001) 2149 UNTS 256.

58 See for example UNODC, 'The Globalization of Crime: A Transnational Organized Crime Threat Assessment', ch 10 on cybercrime <www.unodc.org/unodc/en/data-and-analysis/tocta-2010.html> accessed 2 February 2021; UNODC (n 28).

59 General Assembly Resolution 65/230. The first session of the expert group was held in January 2011 in Vienna.

60 At the 12th UN Congress on Crime Prevention and Criminal Justice in April 2010, see Eric Hilgendorf and Brian Valerius, *Computer- und Internetstrafrecht: Ein Grundriss* (2nd edn, 2012) Springer, sec 1 para 91. In December 2019, the General Assembly requested the expert group to elaborate a comprehensive international convention on cybercrime (Resolution 74/247). The first session took place in February and March 2022.

61 Gercke (n 38) para 26.

establishment of a cybercrime repository[62] with a database on national cybercrime legislation, jurisdiction and tools for capacity building.[63] It is especially designed to help developing countries implement cybercrime legislation and to share technical knowledge with regard to law enforcement.

Cybercrime offenses also did not make it into the Rome Statute alongside the four core international crimes listed in it. Although core international crimes in principle can be committed with a computer system as an essential instrument of the crime or by specifically targeting a computer system as its object,[64] to date these crimes would only tangentially involve actions categorizable as cybercrimes.

Academic researchers have advocated setting up an International Criminal Tribunal for Cyberspace.[65] Its jurisdiction would be limited to cybercrimes of most serious concern to the international community, such as ones violating a global treaty on cybercrime or launching cyberattacks against critical domestic infrastructures. However, to date the concept only exists on paper. This may be explained by the suggestion tending to include a great variety of offenses which would give an international court broad jurisdiction, severely limiting state sovereignty with regard to digital activity.

3.3 The Council of Europe Convention on Cybercrime

The law dealing with cybercrime to a large degree is transnational law. In the West, the major portion of national criminal law dealing with cybercrime is harmonized, if not driven, by the Council of Europe Convention on Cybercrime[66] and, within the European Union, by corresponding Framework Decisions and Directives.

The Convention on Cybercrime is the major multilateral treaty on cybercrime—a legal regime that many commentators categorize as transnational, not international criminal law.[67] Despite the fact that it is far less successful than other transnational conventions such as the UN Convention against Transnational Organized Crime, the Convention on Cybercrime is still the most influential

62 Available at <www.unodc.org/unodc/en/cybercrime/cybercrime-repository.html> accessed 5 February 2021.

63 UNODC Global Programme on Cybercrime <www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html> accessed 16 February 2021.

64 For example, a military-led cyber-attack on critical infrastructure could be considered aggression, Rome Statute of the International Criminal Court (n 49) art 8 *bis*; Weissbrodt (n 39) 369; Ellen S Podgor, 'Cybercrime: National, Transnational, or International?' (2004) 50(1) Wayne Law Rev 97, 105.

65 J Stein Schjolberg, Recommendations for Potential New Global Legal Mechanisms Against Global Cyberattacks and Other Global Cybercrimes: An International Criminal Tribunal for Cyberspace (ICTC), 2012 <www.cybercrimelaw.net/documents/ICTC.pdf> accessed 14 February 2021.

66 Convention on Cybercrime (n 2).

67 Boister (n 25) 187 with further references.

legal instrument for regulating cybercrime globally.[68] As of February 2021, 68 states have signed on, with 65 having ratified it. The signatories include most members of the Council of Europe, foremost Germany, France, Italy and the United Kingdom.[69]

States that are not members of the Council of Europe may be admitted to the Convention with the unanimous consent of the signatories. This category includes the US, Canada, Japan, Australia as well as several African (e.g. South Africa, Ghana, Senegal) and Latin American states (Argentina, Chile, Peru). A host of skeptics have cast doubt on how much influence the Convention exerts on global cybercrime law[70] because it has not been signed by Russia and China—excluding roughly 50% of global internet activity.[71] However, within the last three years, an additional ten states signed the Convention. Brazil has recently started the accession process for joining the Convention. In addition, the Convention on Cybercrime exerts great influence on cybercrime regulation by non-Member States, for example, in Egypt, Nigeria and Pakistan.[72] It pioneered a technology-neutral approach with regard to cyber offenses that lets it adapt to new technological developments, an approach that has become a standard in cybercrime law.[73] In sum, the Convention serves as model for cybercrime laws in most of the West but also in Asia, Africa and South America. The Convention obliges the state parties to criminalize the set of conduct regarded as cybercrime as well as to inter-state cooperation in law enforcement and has led to widely harmonized national cybercrime control regimes in the states adhering to the Convention.

Not all national cybercrime regulations implement the Convention on Cybercrime, although instances of this are rare among the state parties or otherwise influenced countries. Most domestic cybercrime regulation in the West is aligned with or at least influenced by the Convention due to its exhaustive coverage of acts that must be criminalized. Furthermore, some cyber activity has no crossborder dimension (e.g. fraudulent cyber activity targeting persons within a country). However, this kind of activity will also usually fall under national

68 Different Gercke (n 38) para 32–34.

69 Council of Europe, 'Chart of Signatures and Ratifications of Treaty 185' <www.coe.int/de/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=M5hBFxph> accessed 9 February 2021. Sweden, Ireland and South Africa have not ratified the treaty.

70 Adrian Haase, *Computerkriminalität im Europäischen Strafrecht: Kompetenzverteilung, Harmonisierung und Kooperationsperspektiven* (2017) Mohr Siebeck, 159; Marco Gercke, '10 Years Convention on Cybercrime' (2011) Comput Law Rev Int 142–43.

71 As long as Brazil has not joined. Keller and others (n 10) 13; Roderic G Broadhurst and Yao-Chung Chang, 'Cybercrime in Asia: Trends and Challenges' in Jianhong Liu and others (eds), *Handbook of Asian Criminology* (2013) Springer, 58.

72 Dominik Brodowski, 'Transnational Organised Crime and Cybercrime' in Pierre Hauck and Sven Peterke (eds), *International Law and Transnational Organised Crime* (2016) Oxford University Press, 334, 342.

73 Boister (n 25) 189.

criminal law, that is based on the Convention on Cybercrime. As with transnational law in general, the required criminal provisions usually do not require crossborder conduct elements but include conduct whether or not it has a transnational dimension.[74] This may reflect the aim of the suppression regimes: They ought to prohibit certain conduct not only in crossborder situations but within states on the assumption that the conduct will ultimately produce crossborder effects. This guarantees interstate law enforcement, especially through double criminality, which is usually required for extradition, and prevents safe havens.

The Convention on Cybercrime stipulates requirements for the criminalization of "cyberactivity" (substantive criminal law) as well as for prosecuting cybercrime (procedural criminal law) and for jurisdictional conflicts. The rulings on the latter two will not be presented because this contribution focuses on the criminal prohibitions.

As a consequence of the aforementioned definition problems (see Section 1), the Convention on Cybercrime does not define cybercrime as such. Instead, it limits itself to requiring penalties for three different types of specified "cyberconduct" offenses, namely (1) access, (2) use and (3) content offenses. The Convention introduced a technology-neutral approach which enables it to adapt to new technologies.

The Convention's section on terminology only defines "computer systems", "computer data", "service provider" and "traffic data" (Art. 1). A "computer system" means any device or a group of interconnected or related devices, one or more of which automatically processes data pursuant to a program (ibid.). The computer system can be a standalone system.

The first title on offenses aims at protecting the integrity of computer systems. It requires the criminalization of acts "against the confidentiality, integrity and availability of computer data and systems" (so called CIA offenses).[75] This includes illegal access (especially "computer hacking") (Art. 2), defined as unauthorized intentional access to all or part of a computer system. These offenses usually set the stage for further crimes such as modifying or acquiring stored data.[76] Consequently, the Convention offers state parties the possibility to limit criminal liability by including restrictive elements of crimes, such as infringement of security measures (e.g. bypassing password authentication), dishonest intent or the offense having to be committed against a computer system *through a network*.[77]

Article 3 focuses on protecting data integrity and confidentiality. It calls for criminalizing intentional illegal interception of "non-public" (confidential)[78] transmissions of data from or within a computer system, for example, "stealing"

74 Ibid 25.
75 Boister (n 25) 189.
76 Gercke (n 31) 113.
77 Convention on Cybercrime (n 2) art 2 sentence 2.
78 Council of Europe, *Explanatory Report to the Convention on Cybercrime No 54.*

data during transfer over a wireless network (WLAN). Again, parties may add restrictive elements of crime, such as dishonest intent. Data espionage without previous illegal access is not categorized conduct to be criminalized (e.g. copying files while doing maintenance on a computer).[79] Some countries have expanded protection by penalizing data espionage that either only involves specific information (e.g. 18 U.S.C. Sec. 1831 with regard to trade secrets) or any kind of stored computer data (German Criminal Code Sec. 202a).

Article 4 addresses data interference offenses, thus protecting the integrity of computer data, including the damaging, deleting, etc. of computer data. Parties to the Convention may require that the interference results in serious harm.[80]

Article 5 aims to protect the integrity of computer systems by penalizing system interference, meaning the intentional, serious unauthorized tampering with a computer system's functionality (e.g. denial-of-service attacks that make a website temporarily unavailable to legitimate traffic; attacks on the functioning of critical infrastructure such as water supplies run by computer systems). This does not include manipulations of computer systems other than interference (e.g. adding data).[81] Unlike the preceding articles, this one does not explicitly provide optional restrictive elements. However, the interference must be "serious", leaving it to the state parties to determine the criteria for seriousness which they can use for limiting the offense. For example, they may stipulate significant detrimental effects on the ability to use the system or to communicate with other systems[82] (thus excluding spamming from criminal liability).[83]

Article 6 takes aim at the use of "hacker tools". It exclusively penalizes potentially dangerous acts usually preceding the established offenses.[84] It calls for criminalizing acts of intentionally producing, selling or otherwise making available devices designed or adapted primarily for the purpose of committing any of the established offenses or for compromising passwords, access codes and the like, with the intent of using them in the commission of the stipulated offenses (Art. 6(1)(a)). Article 6(1)(b) requires penalizing the mere intentional possession of such tools with intent of using them in the commission of any of the established offenses. Parties to the Convention may require a certain number of such items to be in possession before criminal liability is triggered. In addition, state parties are permitted to only criminalize sale, distribution or otherwise making available of the items referred to, specifically excluding mere possession (Art. 6(2)). These offenses are controversial because it cannot be clearly established when the offender has sufficient intent to be held liable.[85] Security specialists, for

79 Gercke (n 31) 118.
80 Convention on Cybercrime (n 2) art 4 sentence 2.
81 Brodowski (n 72) 334, 344.
82 Council of Europe, *Explanatory Report to the Convention on Cybercrime No 67.*
83 Brodowski (n 72) 334, 344.
84 Council of Europe, *Explanatory Report to the Convention on Cybercrime No 71.*
85 Boister (n 25) 192.

example, may risk criminal liability when they buy or use such tools professionally (dual use tools).[86]

The second title of offenses calls for criminalizing certain "offline" crimes in which computer systems are used for personal or financial benefit. The aim is to protect property, financial assets and the authenticity of documents.[87] Article 7 requires states to criminalize computer-aided forgery with the intent of creating inauthentic data to be considered or acted upon for legal purposes as if they were authentic. A party may require intent to defraud or similar dishonest intent. Article 8 obliges parties to penalize computer-related fraud.

The third title on offenses relates to content. Article 9 invokes penalties for conduct involving child pornography, including its intentional production, sale and procurement using a computer system (i.e. buying it) as well as mere possession. Parties have leeway for not criminalizing the latter two offenses. Overall, Art. 9 mainly covers acts that are the source of child abuse (in the course of producing child pornography) but do not exploit children sexually themselves. Since most countries already penalize the abuse of children as well as traditional means of distribution, Art. 9 mainly seeks to harmonize differing regulations on child pornography especially with regard to age. It also covers preliminary activities such as creating fictional images, which do not violate children's rights but might be used to bait children into participating in pornographic acts.[88]

Article 10 serves to protect intellectual property rights, because violations involving digital distribution of copyrighted material have increased exponentially. It calls for penalizing deliberate computer-related infringement of copyrights and related rights as defined under national law pursuant to international obligations.[89] Since most countries already criminalize copyright violations, Art. 10 mainly provides basic principles.[90] It only calls for criminalization of infringements on a commercial scale (Art. 10(1)). Parties may reserve the right not to criminalize conduct, provided that other effective remedies are available (Art. 10(3)).

Because the parties negotiating the Convention could not agree on criminalizing computer-related "hate speech", related provisions were segregated in a First Protocol to the Convention.[91, 92] It obliges the parties to criminalize the use of computer systems for disseminating racist and xenophobic material, for making racist and xenophobic threats or insults, and for denying, grossly minimizing, approving or justifying genocide or crimes against humanity (e.g. holocaust

86 Brodowski (n 72) 334, 345.
87 UNODC (n 28) 96.
88 Council of Europe, *Explanatory Report to the Convention on Cybercrime No 102.*
89 Therefore, it is only binding for the parties that have signed these international treaties.
90 Council of Europe, *Explanatory Report to the Convention on Cybercrime No 109.*
91 2003 Additional Protocol concerning the criminalization of acts of a racist or xenophobic nature committed through computer systems (adopted 28 January 2003, entered into force 1 July 2004) 2466 UNTS 205.
92 Council of Europe, *Explanatory Report to the Convention on Cybercrime No. 4.*

denial). Only 45 states have signed the Additional Protocol, with merely 32 having ratified it to date.[93] Many state parties, such as the United States, deem the Protocol's requirements to be incompatible with their constitutionally guaranteed freedom of speech. The resulting lack of harmonizing "hate speech" regulations leads to difficulties in prosecuting it if it occurs in an interstate context, which happens frequently.[94]

The Convention calls for criminalizing even attempting to commit the offenses listed and for aiding or abetting them (Art. 11) as well as for the criminal liability of legal persons, including internet providers (Art. 12). The Convention also recommends the imposition of effective, proportionate and dissuasive sanctions, including deprivation of liberty (Art. 13), but does not stipulate minimum sanctions.

3.4 European Union Framework Decisions and Directives Addressing Cybercrime

In the European Union, the crimes covered by the Convention on Cybercrime are included in various EU Framework Decisions and Directives, particularly in the Directive on attacks against information systems (2013).[95]

With the Lisbon Treaty (2009),[96] almost all criteria marking a material difference between criminal law and other policy areas in the European Union were dropped—most commonly seen as the development of a new kind of transnational criminal law that is often called supranational criminal law.[97] EU criminal regulations, however, are still not directly binding in almost all areas[98] and must be implemented in domestic criminal law as it is the case with transnational law. Nonetheless, the legislative process and the enforceability of EU requirements for domestic criminal law have significantly changed due to the replacement of Framework Decisions by Directives (Art. 83(2) TFEU). In particular, this resulted in measures for controlling and encouraging implementation as well as sanctioning non-compliance (infringement proceedings for late or incorrect transposition of Directives, Art. 258 TFEU). This has

93 Council of Europe, *Chart of Signatures and Ratifications of Treaty 189* <www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189/signatures?p_auth=zu8UKAZO> accessed 10 February 2021.

94 Marco Gercke, 'The Slow Wake of a Global Approach Against Cybercrime' (2006) Comput Law Rev Int 140, 142.

95 2013/40/EU of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA.

96 Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community (adopted 13 December 2007, entered into force 1 December 2009) 2701 UNTS.

97 Kimmo Nuotio, 'European Criminal Law' in Markus D Dubber and Tatjana Hörnle (eds), *The Oxford Handbook of Criminal Law* (2014) Oxford University Press, 1125–32.

98 An example of an exception is TFEU art 325 para 2 to counter fraud and any other illegal activities affecting the financial interests of the European Union.

significantly enhanced harmonization of constitutive rules for crime definition and punishment, resulting in a vast number of amendments to the national criminal codes within the EU.

The evolution of EU criminal law was fostered by the adoption of the mutual recognition rule (Art. 82 TFEU), which created a European criminal law system of enforcement of decisions and judgments.[99] One of the milestones within this development was the replacement of extradition procedures by the European Arrest Warrant (EAW) that does not require double criminality in both states involved in executing it.

In contrast to the Convention on Cybercrime, the Directive on attacks against information systems only requires EU Member States to criminalize the so-called CIA offenses (see Section 3.3).[100] These are the access offenses regulated in Title 1 of the Convention on Cybercrime, although with some exceptions. The Directive calls for criminalizing "computer hacking", illegal interception of "non-public" transmissions of computer data from or within a computer system, interference offenses (Arts. 3–6) as well as intentional production, sale or distribution of the relevant tools (Art. 7). Member States may limit the scope of the access offenses to cases that are not minor. Illegal system interference is expanded to include the interruption of systems, and the offense of simply rendering data inaccessible qualifies as criminal conduct (Art. 4). In addition, the Directive calls for aggravation of the interference offenses if the real identity of the perpetrator is concealed, if they involve organized crime, or if tools designed to attack a significant number of information systems or critical systems are used (Art. 9).

The Directive does not cover computer-related versions of traditional crimes or content-related crimes. However, these are dealt with separately in other EU regulations, such as the Directive on combating the sexual abuse and sexual exploitation of children and child pornography (2011).[101]

3.5 Economic Community of West African States Directive on Fighting Cybercrime

Several African regional intergovernmental organizations have addressed cybercrime with their own directives. Among them is the Directive on Fighting Cybercrime within the ECOWAS[102] adopted in 2011 by 15 West African

99 Robert Esser, *Europäisches und Internationales Strafrecht* (2nd edn, 2018) C.H.Beck, sec 1.

100 See Haase (n 70) 156–61.

101 2011/92/EU of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography and replacing Council Framework Decision 2004/68/JHA.

102 C/DIR 1/08/11 of 19 August 2011 on fighting cybercrime within ECOWAS (ECOWAS Cybercrime Directive).

states[103] after it became apparent that some of them had become the main sources of worldwide email scams and advance fee fraud.[104] The Directive can be categorized as transnational cybercrime law in that it obliges the Member States to harmonize their cybercrime laws by criminalizing specified crimes[105] and to cooperate in investigations.[106] In the context of substantive criminal law, the Directive is wider in scope than the Cybercrime Convention. This is because it covers all crimes whose detection requires electronic evidence. Furthermore, it calls for criminalizing the offenses of illegally remaining on a computer system, knowingly using forged data or illicitly manipulating data even if only through negligence.[107]

The Directive's requirements were to be adopted by January 2014.[108] However, as of March 2019, at least one-third of the members had yet to implement any cybercrime laws and other required measures.[109] Obstacles include the different priorities of impoverished countries, the lack of capacity for legislating on cybercrime, and the absence of ways and means for fostering effective cooperation.[110] It might have helped if the Directive had included infringement proceedings as the European Union does.[111] However, such control mechanisms do not help if states are simply not able to implement the laws for lack of the necessary governmental and legislative capacities and resources. It would be better to focus on capacity building and providing financial support for improving interstate investigations and law enforcement, in other words, on policy approaches.

4 Policy Approaches

As mentioned earlier, the focus of the UN has shifted from a legislative to a policy approach, even though there are tentatives in progress for developing an international convention on cybercrime.[112] Several regional policy measurement programs are also under way.

103 Benin, Burkina Faso, Cape Verde, Cote d'Ivoire, the Gambia, Ghana, Guinea, Guinea-Bissau, Liberia, Mali, Niger, Nigeria, Senegal, Sierra Leone and Togo, see <www.ecowas.int/> accessed 10 February 2021.

104 See Uchenna J Orji, 'A Review of the ECOWAS Cybercrime Directive' [2019] Comput Law Rev Int 40.

105 ECOWAS Cybercrime Directive (n 102) art 4–23.

106 Ibid art 33; Nicola D Guarda, 'Governing the Ungovernable: International Relations, Transnational Cybercrime Law, and the Post-Westphalian Regulatory State' (2015) 6(1) Transnatl Leg Theory 211, 227, 237.

107 ECOWAS Cybercrime Directive (n 102) art 6, 13, 12; Boister (n 25) 196.

108 Ibid art 35.

109 Orji (n 104) 51.

110 Ibid 51–52.

111 Ibid.

112 The General Assembly established an open-ended ad hoc intergovernmental committee of experts with representatives from all regions to elaborate a comprehensive international convention on cybercrime (Resolution 74/247).

4.1 United Nations Policy Measures for Addressing Cybercrime

In 2011, the UN established an expert group tasked with examining the current legal and other responses to cybercrime and with developing new ones.[113] The expert group presented the Comprehensive Draft Study on Cybercrime in 2013,[114] which still furnishes the basis for the UN's other policy programs today.

The UN Global Programme on Cybercrime[115] supports capacity building, prevention and education, international cooperation and study of the phenomenon in developing countries.[116] Tools include building a database on cybercrime laws and technical knowledge relevant for investigations and law enforcement (see Section 3.2). The program seeks to raise efficiency of investigations and prosecutions, to support national responses to cybercrime through legislation and law enforcement. It further aims to increase public knowledge of cybercrime challenges by strengthening exchanges between governments and information technology companies.

4.2 Regional Policy Strategies for Dealing With Cybercrime

A number of complementary regional policy strategies are in place to strengthen the states' capacities for responding to cybercrime. The EU's and Council of Europe's "Capacity building on cybercrime and e-evidence" joint project (GLACY) that was ongoing from 2013 to 2016 is a good case in point.[117] The project encouraged the seven priority countries (Mauritius, Morocco, Philippines, Senegal, South Africa, Sri Lanka and Tonga) to adopt or harmonize their cybercrime laws in line with the standards set forth in the Convention on Cybercrime. All of them have signed on to the Convention since then. The training of judges and prosecutors as well as law enforcement officers was strengthened by introducing modules on cybercrime into the judicial training academy curriculums and by providing training materials and tools to cybercrime law enforcement authorities (e.g. on data forensics, standard operating procedures). The priority countries also improved their ability for international cooperation, for example, by connecting their cybercrime law enforcement authorities with EUROPOL and INTERPOL.

The OECD, the Asia-Pacific Economic Cooperation Forum (APEC), the Commonwealth, the Arab League and the Gulf Cooperation Council (UAE)

113 General Assembly Resolution 65/230.

114 UNODC (n 28).

115 Based on General Assembly Resolutions 65/230 and Commission on Crime Prevention and Criminal Justice Resolutions 22/7 and 22/8.

116 United Nations Office on Drugs and Crime 'Cybercrime' <www.unodc.org/unodc/en/cybercrime/index.html> accessed 16 February 2021.

117 Non-paper about GLACY submitted by the European Union to the Expert Group to Conduct a Comprehensive Study on Cybercrime (6 April 2017) UNODC/CCPCJ/EG.4/2017/CRP.2.

and the Organization of American States (OAS) all have cybercrime initiatives under way. These organizations mainly address the cybercrime challenges along the lines of the UN policies by establishing expert groups, conducting analytical studies and making (non-binding) recommendations.[118] Specific plans for fostering capacity building or international cooperation as well as for harmonizing cybercrime laws, however, are still few and far between.

5 Characteristics and Weaknesses of Global Digitality Criminal Law

5.1 Characteristics of Current Global Digitality Criminal Law

Global digitality criminal law is administered differently in different regions of the world. However, most cybercrime regulations have certain characteristics in common, which are highlighted in this section.

Due to its crossborder dimension (see Section 2), the global digitality criminal law is largely *transnational criminal law* (see Section 3). Transnational criminal law consists of a bilateral or multilateral convention that obliges the state parties to include certain offenses in their domestic criminal law (suppression regime). The requirements generally include certain elements of crime, *mens rea*, and *actus reus* requirements, as well as minimum standards for sanctions. To improve cooperation in crossborder investigations and law enforcement, transnational criminal law aims at establishing double criminality, which normally is a prerequisite for interstate collaboration, for instance for rendering mutual legal assistance. Double criminality is achieved by harmonizing domestic criminal laws in line with the requirements of the suppression regime.

National criminal law that implements the requirements of transnational suppression conventions often *prohibits crossborder as well as merely domestic conduct* because transnational crimes rarely include transnational factors in their conduct elements. This is because suppression regimes also aim to prohibit certain conduct within states on the assumption that it entails long-term crossborder effects (e.g. drug production within a country tends to lead to drug distribution in other countries).[119] In addition, global or at least regional criminalization helps to prevent the establishment of safe havens where certain conduct is beyond prosecutorial reach. Therefore, transnational suppression regimes in general and cybercrime regulation in particular lead to broad-spectrum controls on all kinds of behavior regardless of their crossborder dimension.

The *far-reaching control of all kinds of behavior* inherent in transnational criminal law is even more extensive for cybercrime suppression regimes for two reasons: First, cybercrime suppression regimes not only regulate "cyber-dependent" (computer system as an object), but also "cyber-enabled" crime (computer

118 See the overview by Gercke (n 31) 78–87.
119 Boister (n 25) 25.

system as an instrument) (see Section 1.2). The latter category tends to expand the range of penalized conduct significantly, because the use of information technologies has vastly increased over the past decade (see Section 2.1). If everyone uses online banking, all fraudulent behavior involving bank transactions will be categorized as cybercrime and controlled by cybercrime suppression regimes. Second, distinct from other areas of criminal law, cybercrime is categorized by the tools used or the items targeted (i.e. computer systems) (see Section 1.2). In contrast, many authors and legislators categorize offenses according to the legal interests they protect, for example offenses against personal liberty (duress, kidnapping, etc.) on the one hand and offenses against physical integrity (assault, etc.) on the other. This categorization results in restricting the scope of criminal prohibitions when interpreting the law. For example, to spit at someone is not prohibited by offenses against physical integrity such as assault because it does not cause *physical* harm.[120] This possibility of restrictive interpretation is lost if criminal law uses a category like "cybercrime" which is distinguished by the instruments used or the objects targeted.

Since the main goal of transnational criminal law is to foster interstate cooperation in investigations and law enforcement, *substantive criminal law requirements and procedural law requirements are often strongly entangled* in cybercrime regulations. Global digitality criminal law regulations such as the Convention on Cybercrime usually include not just requirements for substantive criminal law (see Section 3.3). They also set standards for procedural criminal law, especially with regard to the collection and preservation of electronic evidence, as well as for jurisdictional conflicts.

Considering that the aim of cybercrime regulations is not so much to prevent or sanction harm but to improve interstate law enforcement, they often require penalizing *conduct that advances the harmful or dangerous conduct* to enable states to investigate at an early stage. For example, the Convention on Cybercrime not only requires criminalizing illegal access to a computer system, but also the mere intentional possession of tools that could be used to illegally access a computer system (see Section 3.3).[121] As a consequence, the hurdles for initiating investigations are much lower. According to the principles of criminal law, sufficient initial proof that someone committed a crime needs to exist before law enforcement authorities are permitted to investigate. Criminalizing the mere possession of "hacker tools" obviates the need for evidence of actually accessing a computer system to initiate an investigation. Evidence that the suspect merely possesses hacking tools on a computer suffices.

Nearly all existing cybercrime regulations not only include access and use offenses but also content offenses (i.e. online "hate speech") as for example the 2003 Additional Protocol to the Convention on Cybercrime (see Section 3.3).

120 Spitting at someone may be subject to defamatory offenses that impose lower penalties than assault offenses.

121 Convention on Cybercrime (n 2) art 6(1)(b).

Content offenses are harder to justify than the first two offense categories, because they *affect the constitutional right to freedom of speech* of the "speaker".

The cybercrime suppression regimes *rarely include procedural rights of the suspect* despite the fact that they usually specify guidelines for investigations, law enforcement and jurisdictional conflicts which affect those rights. The reason for the silence on the suspect's rights may be that the suppression regimes strongly focus on improving the efficiency of criminal prosecution in crossborder situations. That efficiency, however, may be impeded by strong, enforceable rights of the suspect.

In sum, global digitality criminal law has a few characteristics that distinguish it from other areas of criminal law. Global digitality criminal law is transnational law. It calls on states to establish certain crimes in their national criminal law to improve interstate cooperation. Characteristically, it prohibits a wide range of behavior beyond crossborder conduct, beyond the protection of certain legal interests, beyond cyber-dependent crime and especially beyond conduct immediately causing harm. It is also characterized by a strong entanglement of substantive and procedural criminal law, but it usually lacks safeguards for the suspect.

5.2 Weaknesses of Present Global Digitality Criminal Law

While a great deal of academic attention has been paid to the erosion of rights of the (future) suspect in cybercrime regulations,[122] the individual liberties restricted by cybercrime prohibitions (substantive criminal law) have suffered from relative neglect. For this reason, the present contribution concentrates on this facet of the larger topic of weaknesses of current global digitality criminal law.

Since most global digitality criminal law is primarily transnational law, both concepts have a number of weaknesses in common.

The main goal and chief value of transnational law is to field more effective measures for suppressing transnational crime (see Section 3.1).[123] Such an approach focuses neither on legal interests to be protected by criminal law nor on individual liberties being limited by criminal prohibitions. The aim is instead pragmatic: to operate a well-functioning control system for deviant behavior.[124] With this as the goal, decriminalizing certain areas of transnational crime, such as the recreational use of cannabis or some forms of hacking, becomes almost impossible. This is especially troubling, since transnational criminal law mainly covers *crimes mala prohibita*, meaning regulatory offenses whose wrongfulness is derived from violating a regulation based on a specific state policy (see Section 3.1). Transnational criminal law tends to overcriminalize the activities

122 See references in n 3 earlier.

123 Boister (n 25) 20; Ethan A Nadelmann, "Global Prohibition Regimes: The Evolution of Norms in International Society' (1990) 44(4) Int Organ 479.

124 Supporting Garland's general observation of an emerging culture of control; see David Garland, *The Culture of Control: Crime and Social Order in Contemporary Society* (2001, reprinted 2011) University of Chicago Press, 139–66.

mentioned solely in the interest of effective crime control. For example, the Convention on Cybercrime requires criminalizing copyright infringements[125] (see Section 3.3), even though copyrights may already be protected by civil remedies (damages, injunctive relief, etc.).

In addition, transnational criminal law quite often broadens the scope of criminal liability. It routinely calls for criminalizing not only traditional inchoate offenses such as attempt, but also preparatory and preliminary conduct not immediately and not necessarily causing harm (e.g. offenses of possessing goods considered to be dangerous such as drugs, weapons or hacking tools).[126] For example, the Convention on Cybercrime as well as the Directive on attacks against information systems call for criminalization of the mere possession of tools that may be used when committing the other established cyber offenses (see Sections 3.3 and 3.4). Such preventive criminal offenses limit freedom to a greater extent than traditional criminal offenses that sanction harm caused or endangerment.[127] Preventive criminal offenses lower the threshold for being prosecuted significantly. Even inchoate offenses usually require the intent to cause the circumscribed harm and substantive steps toward that end. Preventive criminal offenses often do not require further steps toward harming someone and often not even the intent to do so. For example, the Convention on Cybercrime calls for criminalizing "computer hacking" but does not require further elements of a crime, such as the infringement of security measures or the intent to "steal" data (even though the parties to the Convention may include these elements) (see Section 3.3).[128] This has led to criminalizing "hacking" for entertainment or as a form of protest[129] in some Member States and has grossly limited the rights of "hackers" who often do not have malicious intentions but "hack" just for the thrill of it or to raise awareness for deficits in security measurements, data protection and the like.

Transnational law limits sovereignty and democratic self-governance.[130] States regard their criminal law as an expression of their sovereignty. Criminalizing conduct seriously limits liberty in certain areas. Criminal law is a means for social

125 Parties may reserve the right not to criminalize conduct, provided that other effective remedies are available.

126 Boister (n 25) 26.

127 See Beatrice Brunhöber, *Strafrecht im Präventionsstaat* (2014) Franz Steiner; Beatrice Brunhöber, 'Von der Unrechtsahndung zur Risikosteuerung durch Strafrecht und ihre Schranken' in Roland Hefendehl and others (eds), *Festschrift für Bernd Schünemann* (2014) De Gruyter, 3; Andrew Ashworth and Lucia Zedner, *Preventive Justice* (2014) Oxford University Press, 95.

128 Convention on Cybercrime (n 2) art 2.

129 Noah C N Hampson, 'Hacktivism: A New Breed of Protest in a Networked World' (2012) 35(2) BC Int'l & Comp L Rev 511.

130 Allen Buchanan, 'The Legitimacy of International Law' in Samantha Besson and John Tasioulas (eds), *The Philosophy of International Law* (2010) Oxford University Press, 79.

control that is often strongly entangled with cultural preferences and beliefs.[131] For these reasons, criminal law is one of the legal areas that especially demand democratic debates and democratic decisions. Nevertheless, the development of transnational criminal law is peculiarly non-transparent and dominated by technical legal experts at the international level. "The public often has very little knowledge about and say"[132] in the development of the norms or mechanisms, a fact often ignored by the domestic legislatures transforming international treaty obligations into domestic law. The history of the Convention on Cybercrime is exemplary for the lack of democratic participation in crafting it.[133] The Convention was drafted beginning in 1997 by a Council of Europe expert group that included prosecutors, judges and criminal law researchers with expertise in cybercrime, but excluded democratically elected representatives.[134] The first public release of the draft treaty was in its 19th version[135] shortly before it was finalized by the Committee of Ministers and opened for signature. That left precious little time for a public debate that could have influenced its content. The Convention obliges state parties that ratify it to insert the required crimes including the preventive offenses in their domestic law without the possibility of an open debate about the scope of those crimes.

The democratic deficit becomes particularly troubling when the policies in question are transferred from developed to developing countries.[136] Often developing countries do not participate actively in drafting transnational conventions, as indeed was the case with the Cybercrime Convention (see Section 3.3).[137] In most cases, they can only choose to sign on to a treaty that is carved in stone (as the priority countries in the GLACY program, see Section 4.2). As a consequence, neither their specific situations nor the structure of their law are taken into consideration. For instance, with regard to cybercrime, developing countries are often "exporters" rather than "importers" of crime, which leads to the prohibitions restricting the liberties of much more people in developing than in developed

131 Thomas Weigend, 'Strafrecht durch internationale Vereinbarungen: Verlust an nationaler Strafrechtskultur?' (1993) 105 ZStW 774, 789.

132 Boister (n 25) 36.

133 See Ryan M F Baron, 'A Critique of the International Cybercrime Treaty' (2002) 10(2) CommLaw Conspectus 263, 265.

134 Specific Terms of Reference of the Committee of Experts on Crime in Cyber-Space, Council of Europe's Fight Against Corruption and Organised Crime, sec 5(c) 583rd Meeting.

135 In April 2000, a draft of the treaty was made available to the public after being discussed in newsgroups (USENET) with a press release from the Dutch Minister of Justice stating that this was the "[f]irst draft of international convention released for public discussion" while it was in its 19th revision (Baron [n 133] 266 at fn 33 with references).

136 Boister (n 25) 35; Dimitri Vlassis, 'The United Nations Convention Against Transnational Organised Crime and Its Protocols: A New Era in International Cooperation' in *The Changing Face of International Criminal Law: Selected Papers* (2002) 75, 76.

137 The only developing country that participated (as observer) was the Republic of the Philippines.

countries. For example, the ECOWAS Directive on Fighting Cybercrime was initiated because some of the Member States had become the main sources of worldwide email scams and advance fee fraud (see Section 3.5). In these cases the offenders were predominantly residents of West African countries whereas the victims were residents of European countries or the United States.

With its tendency to overreach as described, transnational criminal law threatens to grievously curtail individual liberties. For this reason, it raises questions of justification, which, however, play only a minor role in the treaty negotiation processes. Suppression regimes do not pay much attention to the affected liberties since their main aim is effective crime control (see Section 5.1). Even with respect to individuals affected by law enforcement, they usually rely on existing human rights obligations, meaning that the individual protection depends on the coincidental human rights protection level in the involved states (e.g. the provision of enforceable rights).[138] The problem of justification is reinforced due to theoretical problems of limiting preventive criminal law. If the limiting principle is to balance security against liberty, such law can easily be justified by arguing that security of the many outweighs individual liberty of the few.[139]

The threat to individual liberties is an important objection to cybercrime law. Content-related offenses make up an essential portion of cybercrime offenses. Therefore, the potential for threatening the freedom of expression and the use of cybercrime offenses as vehicle for censorship and state control have been sources of concern. More than half of the state parties to the Convention including "big players" such as the United States have not signed or ratified the Additional Protocol concerning the criminalization of acts of racist or xenophobic nature committed through computer systems[140] because they regard its requirements as conflicting with their constitutional rights of freedom of speech (see Section 3.3). Article 15(1) of the Cybercrime Convention reflects on this and asks for implementation to meet human rights standards and proportionality.[141] However, restricting the standards to safeguards in the respective domestic laws and in international treaties means that these limitations will only be effective in states with such standards in their legal codes.

Another weakness of current cybercrime law is the focus on the means and objects of the crime ("computer systems") (see Section 5.1). From this angle, the

138 Boister (n 25) 40.

139 Brunhöber (n 127); Ashworth and Zedner (n 127) 109–15; Jeremy Waldron, *Torture, Terror and Trade-Offs: Philosophy for the White House* (2010) Hart Publishing, 36; Lucia Zedner, 'Securing Liberty in the Face of Terror: Reflections from Criminal Justice' (2005) 32(4) J Law Soc 507; Ronald Dworkin, 'Terror and the Attack on Civil Liberties' (2003) New York Review of Books <www.nybooks.com/articles/2003/11/06/terror-the-attack-on-civil-liberties/> accessed 18 February 2021.

140 Council of Europe, *Chart of Signatures and Ratifications of Treaty 189* <www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189/signatures?p_auth=zu8UKAZO> accessed 10 February 2021.

141 Boister (n 25) 196.

legal interests to be protected as well as the individual liberties affected garner little interest. Discussions center mainly on questions such as how new technologies and new ways of harmful use are to be integrated into the control systems. The Convention on Cybercrime, for example, is often criticized for not keeping pace with the rapid developments in information technology (e.g. the development of social networks and arising problems of communication in social networks such as cyberbullying).[142] This criticism leads to calls for criminalizing more and more conduct. It is often overlooked that new prohibitions restrict individual liberties and that problems like cyberbullying are social issues that would be better addressed by social responses.

6 Conclusion

Lawrence Lessig stated as early as 1996 "that there is a decision to be made about the architecture that cyberspace will become, and the question is how that decision will be made. Or better, *where* will the decision be made".[143] The answers were given by governments all too quickly without public debate and democratic participation under the impression of urgent threats in "cyberspace" and rising costs of criminal prosecution. Individual liberties were sidelined. Only if it becomes clear which liberties are restricted by criminal prohibitions will there be a standard for identifying over-criminalization—which is omnipresent in cybercrime law with its mere possession offenses, access offenses without intent to cause harm, content offenses and so forth. The time has come to think about alternatives to criminal prohibitions as responses to harmful cyberactivity. A social problem should be addressed by social prevention strategies including awareness raising and promoting simple prevention mechanisms which will prevent the vast majority of cybercrime cases.[144]

142 For example, Jonathan Clough, 'The European Council of Europe Convention on Cybercrime: Defining "Crime" in a Digital World' (2012) 23 Crim Law Forum 363, 374–91.

143 Lawrence Lessig, 'The Zones of Cyberspace' (1996) 48 Stanford Law Rev 1403, 1411.

144 Travis C Pratt and Jillian J Turanovic, 'Low Hanging Fruit: Rethinking Technology, Offending and Victimisation' in Kevin F Steinmetz and Matt R Nobles (eds), *Technocrime and Criminological Theory* (2017) Routledge, ch 10.

Conclusion

The Law of Global Digitality: Findings and Future Research

Matthias C. Kettemann and Alexander Peukert

1 The Theme

The story of digitality is one of transcendence, deep mediatisation[1] and convergence. Milton L. Mueller reminds us that we used to have different tools and gadgets "to place telephone calls, watch live or record video, browse libraries and download or play music".[2] Now we just have—as a medium—the internet. The different media—TV, books, radio, CDs, newspapers—were once regulated by different regimes. Their content is now being delivered through internet protocol (IP)-based services: through "the Internet".[3] As channels that deliver content are reduced, the numbers of service providers multiply. How many streaming services can you name? How many TV channels did we use to have?

In light of these substantial challenges—including new instruments of regulation and new actors—the law has changed. Even if not every current social development can be attributed to "digitalisation", the digital transformation has substantial disruptive potential. Of course, the legal system, which is changed by digitalisation, also changes the status quo. It is this interaction between digitality, the market and the law that make this field both exciting and challenging. We see throughout the contributions to this book that the functionality and integrity of the internet itself is essential for online markets to function and rights to be protected; but that both markets and rights (and social cohesion) also need to be protected from threats inherent to technology, mediated through information and communication technologies (ICTs), and increased through technological factors and choice architectures. Decisions taken by normative actors that influence the behaviour of internet users are taken within a "technologically concealed and institutionally complex ecosystem of governance".[4]

1 Andreas Hepp, Andreas Breiter and Uwe Hasebrink (eds), *Communicative Figurations. Transforming Communications in Times of Deep Mediatization* (2018) Palgrave Mcmillian.
2 Milton N Mueller, *Networks and States. The Global Politics of Internet Governance* (2010) The MIT Press, 9.
3 Cf ibid 10.
4 Laura DeNardis, *The Global War for Internet Governance* (2014) Yale University Press, 1.

DOI: 10.4324/9781003283881-17

This ecosystem of governance is at the centre of this book, which makes a first serious effort across legal disciplines and across continents to describe these fundamental and dynamic developments and their implications. As explained in the introductory chapter, the distinctive feature of the book is that it assembles studies of six different areas of law, namely intellectual property (IP), data protection/privacy, consumer contracts, media law, financial market regulation, and criminal law. By comparing how these areas of law have reacted to and at the same time shaped global digitality, we aimed to identify structural regulatory patterns that occur across all fields. We noticed that something is changing, and we wanted to know precisely what and how. If, according to our hypothesis, a certain type of regulation, a substantive principle or another legal aspect could be observed in many or even all of these very diverse fields, it would be plausible to assume that the recurring feature represents a specific characteristic of digital law and not just a variant of pre-digital law (aka "law of the horse"). Such a legal feature would be the "smoking gun" with which the early cyberlaw exceptionalists would eventually win their old battle with un-exceptionalists, if only in certain respects.[5]

2 The Findings

A review of the contributions confirms the fruitfulness of the approach taken. The book not only corroborates *that* "something" is changing[6] but it also reveals *what and how*.

On the one hand, the case studies show that the law of digitality cannot be adequately described and understood as a completely separate system. Interactions between digitality and originally non-digital orders such as law and the marketplace are momentous and constant. Digitality is ordered out of necessity, both externally (hetero-constitution) and internally (auto-constitution). The hetero-constitutionalisation of the normative order of the internet encompasses all processes by which national legal orders (e.g. EU data protection laws) and the regime of international law (e.g. in the area of IP or cybercrime) influence the development of the principles and processes of the internet's normative order. At the same time, we observe that the autonomous regime-internal "thickening" of the norms and normative processes can take place independently of other regimes and traditional forces of constitutionalisation, such as nation-state norms. The development of such rules of digitality inevitably leads to frictions and even to a substantial critique of the regulating power of the non-digital over the digital: the elimination of restrictions through time, cost, space, cognition (AI), and

5 Supra, Introduction.

6 Paul Schiff Berman, 'Introduction' in Paul Schiff Berman (ed), *Law and Society Approaches to Cyberspace* (2007) Ashgate, xxiii; see also Andrea M Matwyshyn, 'The Law of the Zebra' (2013) 28 Berkeley Tech LJ 155, 155 ("At the dawn of internet law, scholars and judges debated whether a 'law of the horse'—a set of specific laws addressing technology problems—was ever needed. Time has demonstrated that in some cases, the answer is yes.").

data storage (and processor speed) changes the fundamental framework conditions of our values, their implementation and enforcement and their institutions. Conversely—as the contributions show—it is also apparent that new normative demands are being placed on digitality. User-friendly services, all-available systems and fast communication require a corresponding legal infrastructure. In general, the power of digitality is becoming increasingly clear: new actors are being constituted, power is being redefined and redistributed, the value of resources is changing, and established checks and balances need to be refined.

On the other hand, this collection reveals that the number of specifically digital and global phenomena, which raise unique regulatory questions, is increasing. In the early days of cyberlaw, the domain name system was the prime and often sole example for such a "new" issue.[7] Nowadays, ubiquitous automated data processing and decision-making,[8] two-sided platforms setting and enforcing communication rules for billions,[9] and digital currencies[10] pose important regulatory challenges unknown in the pre-digital era. In addressing these challenges, lawmakers are confronted with the fundamental distinction between the digital and the non-digital, often leading to a mixture of traditional pre-internet laws and new rules, for example for virtual currencies.[11] Whereas in the past, digitality was often perceived through the lens of similar constellations in the offline world, whose regulation was applied to the digital by analogy,[12] the perspective has gradually shifted. In the area of EU consumer contract law, for example, the law of the digital now spills over into and influences the law of the non-digital.[13] Digital law, in other words, is becoming the new regulatory normal.

The contributions to this book have carved out several specific characteristics of this digital law. Firstly, the law of digitality, in particular on a cross-border, global scale, is largely a product of private ordering, that is, the establishment of rules by private parties within primarily private settings in which terms of service are prima facie the "law of the land".[14] If there is one key distinguishing feature of the law of digitality, it is most likely this: Whereas international law, national laws

7 See, for example, Marcelo Halpern and Ajay K Mehrotra, 'From International Treaties to Internet Norms: The Evolution of International Trademark Disputes in the Internet Age' (2000) 21 U Pa J Int'l Econ L 523, 561.

8 See the contributions by Krotoszynski and Spiecker gen. Döhmann.

9 See the contribution by Peukert.

10 See the contribution by Broemel.

11 See in particular the contributions by Broemel and Brunhöber.

12 For copyright law see the contribution by Riis and Schovsbo, for media law the contributions by Goodman and Dreyer et al.

13 See the contributions by Maultzsch (rules on the sale of tangible goods) and Brunhöber (cyber-enabled offenses).

14 See, in particular, the contributions by Riis and Schovsbo (shift from State-enacted law to contract and code, implemented by private parties within certain "autonomy spaces"), Peukert (transnational IPR enforcement and Open Content Licences), Spiecker gen. Döhmann (application of data protection law to private actors); Broemel (private digital currencies).

and transnational regulatory arrangements interact seamlessly, private orders are only corrected by public values and public-interest interventions in exceptional cases and are thus of paramount importance. In particular, multinational online companies tend to implement their locally grown standards on a worldwide scale.[15] In response, European data protection laws have shifted their focus from the State to the private sector, thereby exhibiting a global regulatory perspective on ubiquitous data processing.[16]

A second, closely related characteristic of the law of global digitality is that it is, to a large extent, standardised across jurisdictions, based on standard terms and conditions and enforced transnationally via code. This phenomenon can be observed in most areas studied in this book, namely in IP, data protection, consumer contract, media, and financial market scenarios. The emerging answer of the law to this standardisation challenge is that legal norms are implemented deeply in the design of the online service at stake.[17] Law transforms from an external, non-digital force into an order embedded in the digital. It is thereby necessarily "infected" by the binary, algorithmic logic of the digital.[18]

A third insight provided by this collection is that the private, contract, and code-based law of digitality can be conceived of as a function of global digital capitalism. In the EU, the U.S. and many more jurisdictions, commercial online activities may be started without prior authorisation. Private commercial initiatives are thus a major if not the most important driver of the digital ecosystem. They are perceived as market activities and regulated accordingly. Legal intervention is therefore considered appropriate in cases of "market failure", "information asymmetries", or a "restriction or distortion of competition". Such economisation of legal issues was observed in the contributions on IP, data protection, consumer contract and financial market laws.[19] Only few legal issues transcend this economistic logic, most notably human rights and criminal law.[20]

At the same time, and this is the fourth and final finding we want to highlight, there is no such thing as a uniform global law of digitality. Many online services continue to be directed to certain local markets and recipients primarily for business reasons (price discrimination) and because of linguistic diversity and divergent consumer habits. Legal compliance fortifies this tendency because few if any legal questions are completely harmonised on a worldwide scale. It is true that

15 See the contributions by Bradley, Goodman, Dreyer et al.

16 See the contribution by Spiecker gen. Döhmann.

17 See Mireille Hildebrandt, *Smart Technologies and the End(s) of Law* (2015) Edward Elgar, 218, 226 and in particular the contribution of Spiecker gen. Döhmann.

18 Regarding art 17 of Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market [2019] OJ L130/92 see the contribution of Riis and Schovsbo.

19 See the contributions by Riis and Schovsbo, Krotoszynski ("commodification"), Spiecker gen. Döhmann ("data protection law as a new tool and vehicle for control of fair markets and fair trade"), Maultzsch ("market-centred perspective"), Broemel.

20 See the contributions by Dreyer et al. and Brunhöber.

international law provides rules and principles for global digitality, most notably in the areas of copyright and criminal law.[21] Beyond these segments of global harmonisation, however, legal fragmentation dominates. National approaches persist in particular in the areas of consumer contracts, data protection/privacy and media law, for which the contributions to this book document fundamental differences between European and U.S. approaches.[22] Even in an area as extensively and deeply harmonised as copyright law, hard cases at the borderline between infringement and lawful uses such as the liability of sharing platforms are still handled on a national, territorial basis.[23] Worse still, core aspects of digital law, in particular U.S. data privacy and consumer contract law and EU media law are highly fragmented, complex, and unstable on their own terms.[24] In sum, the law of digitality is rightly understood as a common term denoting a multiplicity of laws of digitality.

3 Suggestions for Future Research

Whereas this collection reveals several characteristics of the law of global digitality—transnational standardisation via private ordering, economisation, persistent and possibly deepening legal fragmentation—further research of concrete questions of digital law and of overarching theoretical issues is definitely needed.

Regarding the former, one can point, for example, to the unclear determination of the asset value of personal and other data, some of which are already regarded as money equivalents in law.[25] The legal discussion on how to effectively and legitimately regulate the behaviour of, in part, new, but in any case powerful actors of digitality is also still in its early stages. This applies, for example, to the regulation of media intermediaries, to the governance of cryptocurrencies, but also to financial market supervision in general. There is also a considerable need for research into how the combined use of Big Data and AI can be reconciled with the requirements of data and anti-discrimination laws and, more generally, with the fundamental order of freedom. Another unresolved issue concerns the relationship between law and regulation via code/algorithms. Does the law endorse, limit, or prohibit the use of algorithmic decision-making or geo-blocking, and should it? All of these concrete application-related questions have so far been addressed by lawyers only partially.

As regards our overarching theoretical question of whether one can observe a specific mediality of digital law, additional legal areas could be included in the

21 See the contributions by Peukert and Brunhöber.

22 See the contributions by Krotoszynski, Spiecker gen. Döhmann, Bradley, Maultzsch, Goodman and Dreyer et al.

23 See the contribution by Peukert.

24 See the contributions by Krotoszynski, Bradley, and Dreyer et al.

25 See Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services [2019] OJ L136/1, arts 2(7), 3(1).

analysis, in particular telecommunication and competition/antitrust laws. An important methodological insight for such analyses following from this book is the distinction between the study of uniquely digital phenomena (such as digital platforms, goods, currencies, and cyber-dependent offenses) as opposed to originally non-digital phenomena and rules exposed to digitalisation (e.g. the sale of tangible goods or cyber-enabled offenses). Our fragmentation thesis also awaits further clarification by more comparative research, especially as regards China and other non-Western jurisdictions. Do national/regional laws of digitality converge or diverge? Are we witnessing the emergence of several regional versions of the internet, and if yes, in which respect?[26]

Last but not least, future research will have to draw conclusions as to how the law of global digitality should develop—with the overarching importance of ensuring individual spheres of freedom and social cohesion in mind. Complexity of a relational space is one factor suggesting that more norms are necessary. In the law of digitality—characterised, as we have seen, by complexity, national and regional peculiarities—a flexibilisation of tools, a horizontalisation of duties, an enrichment of the actor sphere—in sum, a need for normativity becomes apparent. *Ubi societas, ibi ius*. There is *societas* on the internet, therefore *ius*, too.

26 Cf Eric Schmidt and Jared Cohen, *The New Digital Age* (2013) Knopf, 126 (in ten years the relevant question will no longer be whether a society uses the internet, but which version it uses).

Index