Luca Belli
Nicolo Zingales
Editors

PLATFORM REGULATIONS

HOW PLATFORMS ARE REGULATED AND HOW THEY REGULATE US

Official Outcome of the UN IGF Dynamic Coalition on Platform Responsibility

Prefaces by
David Kaye
Julia Reda

FGV DIREITO RIO

Platform Regulations

How Platforms are Regulated and How They Regulate Us

Official Outcome of the UN IGF Dynamic Coalition on Platform Responsibility

United Nations Internet Governance Forum
Geneva, December 2017

Edition produced by FGV Direito Rio
Praia de Botafogo, 190 | 13th floor
Rio de Janeiro | RJ | Brasil | Zip code: 22250-900
55 (21) 3799-5445
www.fgv.br/direitorio

Platform Regulations

How Platforms are Regulated and How They Regulate Us

Official Outcome of the UN IGF Dynamic Coalition on Platform Responsibility

Edited *by Luca Belli and Nicolo Zingales*
Prefaces *by David Kaye and Julia Reda*

Printed in Brazil

1st edition finalized in 2017, November

This book was approved by the Editorial Board of FGV Direito Rio, and is in the Legal Deposit Division of the National Library.

Coordination: Rodrigo Vianna, Sérgio França e Thaís Mesquita
Book cover: Andreza Moreira
Layout: Andreza Moreira
Reviewer: Luca Belli

Ficha catalográfica elaborada pela Biblioteca Mario Henrique Simonsen/FGV

Platform regulations: how platforms are regulated and how they regulate us. Official outcome of the UN IGF Dynamic Coalition on Platform Responsibility / Edited by Luca Belli and Nicolo Zingales; preface by David Kaye and Julia Reda. – Rio de Janeiro : Escola de Direito do Rio de Janeiro da Fundação Getulio Vargas, 2017.
248 p.

Inclui bibliografia.
ISBN: 978-85-9597-014-4

1. Tecnologia e direito. 2. Redes sociais online. 3. Direito regulatório. 4. Direitos fundamentais. 5. Proteção de dados. I. Belli, Luca. II. Zingales, Nicolo. III. Escola de Direito do Rio de Janeiro da Fundação Getulio Vargas.

CDD – 341.2738

The Dynamic Coalition on Platform Responsibility (DCPR) is a component of the United Nations Internet Governance Forum. This book is the official 2017 outcome of the DCPR. The opinions expressed in this book are the responsibility of the authors.

This volume is the result of the first DCPR Call for Papers, which was open to all interested stakeholders. Submitted papers were evaluated for their novelty and academic rigor as well as the potential impact of the initiative described in the paper. All accepted submissions have been peer-reviewed.

For further information, see tinyurl.com/UNIGFplatforms

Acknowledgements

This book reflects many of the ideas discussed by the members of the Dynamic Coalition on Platform Responsibility (DCPR) of the United Nations Internet Governance Forum, between 2015 and 2017. The editors would like to express gratitude to all the DCPR members for their precious inputs and to Thaís Mesquita, Sérgio França, Renan Oliveira and Helena Ferreira for their editorial support.

Furthermore, the editors would like to thank the *Fundação Getulio Vargas Law School,*[1] which provided generous support and guidance, stimulating this research effort.

FGV DIREITO RIO

1 FGV is a world-renowned institution for research and quality education. In 2016, FGV was deemed one of the top 10 think tanks in the world, according to the *Global Go To Think Tanks Index 2016*, produced by the Pennsylvania University. The same Index consistently ranked FGV as the most influential think tank in Latin America over the past eight years. For further information, see http://portal.fgv.br/

CONTENT

PREFACE

by *David Kaye*

2017 presented increasingly difficult challenges for digital platforms such as social media and search engines. Consider the most high profile among them, Facebook. The year of challenges began in 2016 just as Donald Trump was elected president of the United States, after which public outrage – among Democrats and "Never Trump" Republicans at least – focused on the spread of "fake news" on platforms like Facebook. A *New York Magazine* headline proclaimed, "Donald Trump Won Because of Facebook,"[1] while *The New York Times*, in an editorial entitled, "Facebook and the Digital Virus Called Fake News,"[2] asserted that CEO Mark Zuckerberg "let liars and con artists hijack his platform." In fact, 2017 may well be remembered as the year when platform harms, and the demands to address them, became widely understood in the mainstream as a leading problem of public policy in digital space.

The challenges did not end with demands of platform responsibility for disinformation and propaganda. In May, Zuckerberg, evidently under pressure to respond to a range of perceived ills on his platform, posted a note[3] that began as follows:

1 See Max Read, 'Donald Trump Won Because of Facebook', *New York Magazine* (New York, 9 November 2016) <http://nymag.com/selectall/2016/11/donald-trump-won-because-of-facebook.html> [accessed 31 October 2017].

2 See Editorial, 'Facebook and the Digital Virus Called Fake News', *New York Times* (New York, 19 November 2016) <https://www.nytimes.com/2016/11/20/opinion/sunday/facebook-and-the-digital-virus-called-fake-news.html> [accessed 31 October 2017].

3 See <https://www.facebook.com/zuck/posts/10103695315624661> [accessed 31 October 2017].

The content of the note could not be a surprise to anyone who has followed the news in recent years: an admission that certain kinds of harm may occur, or be seen to occur, on Facebook, particularly through video. Zuckerberg mentions three specific harms: hate speech, child exploitation, and suicide. He could have gone further. By 3 May 2017, the list of "harms" that he and others might have proposed here could have been extensive and gone well beyond video posts: the aforementioned "fake news" or "junk news"; promotion of terrorism or 'extremism'; misogyny and gender-based harassment and bullying; hate speech in the form of *inter alia* racism, Islamophobia, anti-Semitism, homophobia; religious discrimination; reputational damage related to such doctrines as the right to be forgotten; and so on. And while Facebook surely is not alone in facing criticism – Twitter, Google/YouTube, Reddit, Snapchat and many others are in the zone, too – it is easily the largest social media forum and attracts the most attention.

Still, that opening paragraph deserves unpacking, especially its last eight words, which show Zuckerberg to be asking himself, 'How can we do better for our community?' Almost every word does some work here. *How:* is there a process available to address the perceived harms? *We:* is this a problem that deserves our corporate attention? *Better*: is there a standard of protection, whether of rights or physical and mental well-being, which the company seeks to achieve? *For:* Is content regulation something the company does "for" its users, top down, or something that it identifies in concert with them? *Community*: is it possible to talk about all users of a particular platform as a single community? What does the word imply about the nature of governance within it? Even in the absence of such a Talmudic evaluation of eight words, it is impossible to read the post without concluding that Facebook is looking for ways to regulate its own space. There is, for instance, no suggestion of outsourcing that regulation to external actors. It is an effort to look within, not without, for answers to fundamental questions of content regulation.

Not all actors in digital space see it the same way – or at least express their concerns in this way. Matthew Prince, the CEO of Cloudflare, a major content delivery network, faced what may

seem to some to be an easy question: whether to remove Nazis from a platform. In the wake of the white supremacist marches and attacks in Charlottesville, Virginia, Prince faced pressure to end Cloudflare's relationship with *The Daily Stormer*, a Nazi website and Cloudflare client. As he put it to his employees, "I woke up this morning in a bad mood and decided to kick them off the Internet."[4] But that was not all. He posted an essay in which he struggled[5] with this question: why, he asked, should *I* police Nazis and others online? Is that not government's function and authority? His point cannot be ignored: "Without a clear framework as a guide for content regulation, a small number of companies will largely determine what can and cannot be online."

This volume seeks to capture and offer thoughtful solutions for the conundrums faced by governments, corporate actors and all individuals who take advantage of – or are taken advantage of within – the vast forums of the digital age. They aim to capture the global debate over the regulation of content online and the appropriate definition of and responses to harms that may or may not be cognizable under national or international law. In a perfect world, this debate, and its resolution, would have been addressed years ago, in times of relative peace, when content-neutral norms might have been developed without the pressure of contemporary crises. Today, however, the conversation takes place in the shadow of grave violations of the freedom of opinion and expression and a panoply of other rights – privacy, association and assembly, religious belief and conscience, public participation. We all find it difficult to separate out the current crises and alleged threats from the need to ensure that space remains open and secure for the sharing and imparting of information and ideas.

In reading through this volume, two things are likely to become clear. First, there is a set of difficult normative questions at the heart of the platform regulation debate, centred on this: What standards should apply in digital space? Or more precisely,

4 See Kate Conger, 'Cloudflare CEO on Terminating Service to Neo-Nazi Site: 'The Daily Stormer Are Assholes'', (*Gizmodo*, 16 June 2017) <https://gizmodo.com/cloudflare-ceo-on-terminating-service-to-neo-nazi-site-1797915295> [accessed 31 October 2017].

5 See Matthew Prince, 'Why We Terminated Daily Stormer' (*Cloudflare blog*, 16 August 2017) <https://blog.cloudflare.com/why-we-terminated-daily-stormer/> [accessed 31 October 2017].

what standards should the platforms themselves apply? Are the relevant standards "community" ones, rooted in a sense of what's appropriate for that particular platform? Should they be based on norms of contract law, such that individuals who join the platform agree to a set of restrictions? Should those restrictions, spelled out in terms of service (ToS), be tied to norms of human rights law? Should they vary (as they often do in practice) from jurisdiction to jurisdiction? In accordance with the UN Guiding Principles on Business and Human Rights, what steps should companies be taking to ensure they respect rights and remedy violations?

A second set of questions is based on process. Some of them will be answered differently depending on how the standards question is answered. For instance, if we agree that the standards should be fully defined by the platforms themselves, procedural norms will likely not touch upon matters of public policy or public law. However, if the standards are tied to public law, or if government imposes standards upon the platforms, who should be adjudicating whether particular expression fails the standards? Should governments have a role, or should courts, in cases involving the assessment of penalties for online expression? Or should the platforms make those determinations, essentially evaluating the legitimacy of content based on public standards?

This is a volume for all stakeholders, reinforcing the critical – perhaps foundational – point that content regulation is a matter of public policy. As such, the debate is not one for governments and companies to hash out behind closed doors but to ensure the participation of individuals (users, consumers, the general public) and non-governmental actors. It is one that will benefit from the consideration of the role of human rights law, particularly since online platforms have indeed become the grand public forums of the digital age. It is finally one that must aim toward the protection of those rights that all too many governments seem eager to undermine.

David Kaye,
United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression

PREFACE

by *Julia Reda*

In an interconnected world, online platforms occupy a pivotal position in the governance of global communication and content dissemination. Where traditional systems of law-based governance meet limits of both jurisdiction and speed in dealing with myriads of legal and societal conflicts that arise from online communication, platforms are increasingly asked to step into the breach and take up traditionally public law enforcement functions. However, this transfer of responsibility from state actors to private companies does not happen across the board, it is comprised of a number of very specific demands made on platforms when dealing with illegal (or otherwise deemed unacceptable) content, while completely disregarding other aspects that would be required of a state actor taking on the same functions.

This phenomenon is well-illustrated by recent demands on online platforms by U.K. Prime Minister Theresa May, joined by French President Emmanuel Macron and Italian Prime Minister Paolo Gentiloni at the UN General Assembly in New York[6], to develop technologies that prevent material promoting terrorism from being uploaded in the first place, and failing that, to delete such content within two hours of it appearing online. Platforms' responsibility in relation to illegal activities on their infrastructure is framed as a responsibility to remove offending messages. Success is primarily measured in terms of minimising false negatives, i.e. recognising and removing as much illegal content as possible, and increasing the speed of removal. Other aspects such as minimising false positives, ensuring transparency and accountability of the removal system towards all affected parties, ensuring support for victims of illegal messages such as hate speech or defamation, helping law enforcement to investigate serious crimes, and promoting respect for human rights -notably by paying attention to the context in

6 U.K. Government Press Release (19 September 2017). Prime Minister Calls for Automatic Blocking of Terrorist Content. Available at <https://www.gov.uk/government/news/prime-minister-calls-for-automatic-blocking-of-terrorist-content> [accessed 24 September 2017]

which information is made available- do not appear to be at the centre of regulatory expectations towards platforms.

It is therefore no surprise that platforms are increasingly asked to rely upon automatic filtering systems to detect and remove content, with demands made on platforms playing to such technologies' strengths: They are capable of processing very large amounts of data and thereby detecting vast amounts of potentially illegal material, and take less time to do so than any human review would require.

At the same time, these filters are incapable of making fundamental rights assessments, as they are insensitive to context and therefore cannot establish the legality of content that may look similar to illegal content (for example use of copyrighted content under a copyright exception), leading to significant over-blocking. The demand for increased speed in the removal process acts as an incentive against any human involvement to mitigate the significant shortcomings of filters. But even when a hybrid system is used which leaves the ultimate decision over the removal of content to a human being, automated content monitoring poses inherent challenges in terms of users' privacy. Of course, filters as such do not contribute to transparency of a platform's policies, neither do they provide any assistance to affected parties.

Ever-shorter deadlines for the removal of offending content do not just encourage platforms to take slow and costly human assessment out of the equation and rely entirely on filters, it also nudges platforms towards using ex-ante filtering, as evidenced by the statement from Theresa May regarding promotion of terrorism, saying that platforms should "prevent it from being uploaded in the first place"[7]. From a fundamental rights perspective, this development is particularly concerning given that platforms are being strongly encouraged by state actors to employ the same kind of filtering systems that, when imposed as a legal requirement, have been considered as violating fundamental rights by the Court of Justice of the EU[8].

7 *Ibid.*

8 See Case C-360/10 (2012), *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v. Netlog NV*. EU:C:2012:85.

If automated filters end up being the only viable tool to comply with demands of the legislator and avoid stricter legislation, how "voluntary" can the use of such tools be considered to be? What responsibility do states have to not just refrain from violating fundamental rights directly, but ensure that the online environment is respectful of fundamental rights? Can the assessment of the legality of content be delegated to private actors, and ultimately to algorithms, without undermining the rule of law?

This volume takes a broader perspective on platform responsibility, critically examining both legal obligations and political pressure on platforms to employ voluntary measures with regard to the actions of their users, and makes recommendations on how platform regulation can promote policy goals such as public safety and non-discrimination, while at the same time being accountable, transparent and predictable and preserving the right to access a court. It assesses the need for a legal framework for self-regulation by platforms, in order to promote competition, maintain the rule of law and safeguard the rights of users.

These deliberations for the development of platform regulation by legal and other regulatory means are very valuable for European policy-makers, who have recently put the question of platform responsibility high on the agenda, whereas no agreement has been reached on the appropriate tools, be they legislation, self-regulation or something in between. On the one hand, Members of the European Parliament have for several years called for a legal framework for notice-and-action[9]; on the other hand, the European Commission has once again decided to take a soft-law approach that "strongly encourages" platforms to use automatic content filters[10] after having mandated the use of such filters in its recent proposal for a Directive on Copyright in the Digital Single Market[11],

9 Open letter by nine MEPs to then European Commissioner for Internal Market and Services Michel Barnier on Notice and Action (3 July 2013). Available at: <https://ameliaandersdotter.eu/sites/default/files/letter_commissioner_barnier_notice_and_takedown.pdf> [accessed 24 September 2017]; Open letter by 23 MEPs to European Vice-President for the Digital Single Market Andrus Ansip: MEPs Want Notice and Action Directive (9 May 2017).

10 Communication from the European Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Tackling Illegal Content Online. Towards an Enhanced Responsibility for Online Platforms. COM(2017) 555 final.

11 European Commission: Proposal for a Directive of the European Parliament and of the Council on Copyright in the Digital Single Market - COM(2016)593.

a proposal that was met with fierce criticism from academics[12] and a number of Member States[13].

These developments call us to pay closer attention to the fundamental rights impact of the privatisation and automation of law-enforcement, and ultimately change the political narrative to reverse this dangerous trend.

Julia Reda,
Member of the European Parliament
Vice-Chair of the Greens/European Free Alliance

12 Stalla-Bourdillon et al. (2016). 'Open Letter to the European Commission - On the Importance of Preserving the Consistency and Integrity of the EU Acquis Relating to Content Monitoring within the Information Society'. <https://ssrn.com/abstract=2850483> [accessed 24 September 2017]; Bently et al. (2017). 'EU Copyright Reform Proposals Unfit for the Digital Age (Open Letter to Members of the European Parliament and the Council of the European Union)'. <http://www.create.ac.uk/wp-content/uploads/2017/02/OpenLetter_EU_Copyright_Reform_22_02_2017.pdf> [accessed 24 September 2017].

13 Written questions from the authorities of Belgium, Czech Republic, Finland, Hungary, Ireland and the Netherlands to the Council Legal Service regarding Article 13 and Recital 38 of the proposal for a Directive on copyright in the digital single market. <http://statewatch.org/news/2017/sep/eu-copyright-ms-questions.htm> [accessed 24 September 2017]; Proposal for a Directive of the European Parliament and of the Council on copyright in the Digital Single Market - Questions by the German delegation to the Council Legal Service regarding Article 13. 12291/17 LIMITÉ. <http://statewatch.org/news/2017/sep/eu-copyright-directive-de-questions.htm> [accessed 3 October 2017].

About the Authors

Luca Belli is Senior Researcher at the Center for Technology and Society (CTS) of Fundação Getulio Vargas Law School, Rio de Janeiro, where he heads the Internet Governance Project. Luca is also associated researcher at the Centre de Droit Public Comparé of Paris 2 University. Before joining CTS, Luca worked as an agent for the Council of Europe Internet Governance Unit; served as a Network Neutrality Expert for the Council of Europe; and as a consultant for the Internet Society. Over the past decade, Luca has authored and/or edited more than 30 research outputs on topics such as Internet and human rights, net neutrality, connectivity models, data protection and Internet governance institutions. Luca's works have been used i.a. by the Council of Europe to elaborate the Recommendation on Network Neutrality; quoted by the Report on Freedom of Expression and the Internet of the OAS Special Rapporteur for Freedom of Expression; and featured in several media outlets, including Le Monde, The Hill, O Globo, El Tiempo and La Stampa. Luca is currently the co-chair of the UN IGF Dynamic Coalitions (DCs) on Community Connectivity, on Platform Responsibility and on Network Neutrality.

David Erdos is University Senior Lecturer in Law and the Open Society and Deputy Director of the Centre for Intellectual Property and Information Law (CIPIL) at the University of Cambridge's Faculty of Law, as well as being WYNG Fellow in Law at Trinity Hall, one of the University's colleges. His current research principally explores the nature of data protection especially as it intersects with freedom of expression. His work to date has principally focused on developments within the EU/EEA and has deployed rigorous quantitative and qualitative social science methodology as well as traditional social science analysis. His involvement within the ESRC's Human Rights, Big Data and Technology (HRBDT) project has explored similar issues concerning the structure and nature of data protection, especially as it interacts with competing rights, but from a more global vantage point.

Maryant Fernández Pérez is Senior Policy Advisor at European Digital Rights (EDRi) and a lawyer admitted to the Madrid Bar association since 2012. Maryant defends human rights and fundamental freedoms online in the European Union. She works on intermediary liability (e-commerce, hate speech, counter-terrorism, child protection), digital trade, network neutrality, transparency and internet governance. Maryant is the author of several publications and speaker at multiple conferences in Europe and around the world. Prior to joining EDRi in 2014, she gained experience at the law firm CCA-ONTIER, Décathlon, the Spanish Ministry of Public Works and the CEU San Pablo University. Maryant received her education from the CEU San Pablo University, the Université Catholique de Lille, the Instituto de Empresa and the Universidade Católica Portuguesa. She holds an LLM in Law in a European and Global Context.

Pedro Augusto Francisco is PhD Candidate in Cultural Anthropology at the Federal University of Rio de Janeiro (UFRJ) and holds a Master´s degree in Cultural Anthropology at the same institution. Pedro is a Project Leader and researcher at the Center for Technology and Society at FGV Law School, where he is currently working on the Brazilian component of the "Copyright in the Digital Economy" research project: a qualitative research on the online video production ecosystem in Brazil. He is also a collaborator at the Research Group on Culture and Economy, at UFRJ. Pedro conducts research at the intersection between Anthropology of Science and Technology, Economic Anthropology and Political Anthropology, working mainly with the following subjects: new technologies and Internet; intellectual property and piracy; circulation of goods.

Krzysztof Garstka holds the position of Information Governance Research Associate on the Human Rights, Big Data & Technology project. He is a member of the University of Cambridge, its Faculty of Law, as well as the Centre for Intellectual Property and Information Law. His research interests lie primarily in the fields of information technology law, intellectual property and data protection, with particular interest in online content regulation. He holds an LLB (University of York) and an LLM (University of

Edinburgh). In 2016, he successfully defended his PhD thesis at the University of Nottingham, entitled "S(h)ifting the Cyberspace - Searching for effectiveness and human rights balance in the realm of online enforcement schemes aimed at digital content infringing copyright, trademarks, privacy or reputation." This project focused on finding the most adequate set of pan-European legal tools aimed at the removal of access to online content infringing copyright, trademarks, privacy or reputation. Krzysztof's work was published in international journals such as the International Review of Intellectual Property and Competition Law, and the European Journal of Law and Technology. He is also a regular speaker on IP and IT law conferences and workshops in Europe and beyond.

Judith Herzog is Senior Policy Officer at the French Digital Council where she has extensively worked on online platforms policy-related challenges, especially from an antitrust perspective. Beforehand she graduated with a Master's degree in Law with a specialisation in competition law and policy as well as a master's degree in Management from Audencia business school in Nantes, France.

Krisztina Huszti-Orban is Senior Researcher with the Human Rights, Big Data and Technology Project, funded by the Economic and Social Research Council and based at the University of Essex's Human Rights Centre. Her work focuses on the human rights impact of data-driven technologies, including on regulatory and governance responses to the use of such technologies at the international and multi-stakeholder level. Prior to joining the University of Essex, Krisztina worked with the Office of the United Nations High Commissioner for Human Rights in Geneva, where she provided legal and policy advice on the protection and promotion of human rights in armed conflict and other situations of violence as well as in the context of countering terrorism and violent extremism. She has also worked with the European Court of Human Rights, the International Committee of the Red Cross, the Geneva Centre for the Democratic Control of Armed Forces, and the United Nations Office of Amnesty International in Geneva. Krisztina holds a PhD in international law from the Graduate Institute of International and Development Studies, LLM degrees

from the Geneva Academy of International Humanitarian Law and Human Right and the Andrassy Gyula University, and an LLB from the Babes-Bolyai University.

David Kaye is Professor of law at the University of California, Irvine, and the United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. Appointed by the UN Human Rights Council in June 2014, his rapporteurship has addressed, among other topics, encryption and anonymity as promoters of freedom of expression, the protection of whistleblowers and journalistic sources, and the roles and responsibilities of private Internet companies. Early in his career, he was a lawyer in the U.S. State Department, handling issues such as the applicability of the Geneva Conventions in the wake of the attacks of September 11, 2001. His academic research and writing have focused on accountability for serious human rights abuses, international humanitarian law, and the international law governing use of force. A member of the Council on Foreign Relations and former member of the Executive Council of the American Society of International Law, he has also published essays in such publications as Foreign Affairs, The New York Times, Foreign Policy, JustSecurity and The Los Angeles Times.

Emily B. Laidlaw is Associate Professor in the Faculty of Law at the University of Calgary. She spent almost ten years in the United Kingdom where she completed her LLM and PhD at the London School of Economics and Political Science and was a lecturer at the University of East Anglia. She researches, consults and teaches in the areas of the technology law, privacy, media law, intellectual property law and human rights. Her book, Regulating Speech in Cyberspace: Gatekeepers, Human Rights and Corporate Responsibility, was published by Cambridge University Press in 2015. She is currently an advisor to the Law Commission of Ontario concerning defamation law in the age of the Internet.

Orla Lynskey is Assistant Professor in Law at the London School of Economics. Her primary area of research interest is EU data protection law. Her monograph, The Foundations of EU Data

Protection Law (OUP), was published in 2015. Orla is an editor of International Data Privacy Law, the Modern Law Review and the European Law Blog. Orla is also a member of the European Commission's Multistakeholder Expert Group on the GDPR. Orla holds an LLB in Law and French from Trinity College Dublin, an LLM in EU law from the College of Europe (Bruges) and a PhD in EU law from the University of Cambridge. Before entering academia, she worked as a Competition lawyer in Brussels and as a teaching assistant at the College of Europe.

Lofred Madzou is Policy Officer at the French Digital Council where he works specifically on online platforms regulation. Beforehand, he completed a master's degree in Data and Philosophy at the Oxford Internet Institute (University of Oxford). His expertise focuses on the ethical challenges associated with the development of data science.

Joe McNamee is Executive Director of European Digital Rights (EDRi), an association of privacy and digital civil rights organisations from across Europe. He has worked on Internet-related topics since 1995, having started his online career as a technical support advisor for an Internet provider in 1995. He was responsible for three independent studies for the European Commission on local loop unbundling, on convergence and on telecommunications and the information society in eight former Soviet states. McNamee led EDRi's work on the data protection package and worked on various international data protection initiatives. He has a particular interest in the trend to devolve online law enforcement to Internet intermediaries and its effect on privacy, legal certainty and free speech. Mr McNamee studied Modern Languages at the University of the West of England at Bristol (UWE) (BA), European Politics (MA) in Swansea and International Law (LLM) at the Brussels Schools of International Studies.

Julia Reda was elected to the European Parliament for the Pirate Party in 2014. She is a Vice-Chair of her parliamentary group, the Greens/European Free Alliance. In the European Parliament, she serves as a coordinator for the Greens/EFA in the Committee on Internal Market & Consumer Protection (IMCO), as a member

of the Legal Affairs (JURI) and Petition (PETI) Committees and was elected to the Enquiry Committee on the Emissions Scandal ("Dieselgate"). She co-founded the Digital Agenda intergroup. Her legislative focus is on copyright and Internet policy issues. In 2015, she was responsible for the Parliament's evaluation of the Copyright Directive. Born in Bonn in 1986, Julia Reda was a member of the German Social Democrats for six years before joining the Piratenpartei in 2009 amidst a debate on Internet blocking. She served as chairwoman of the party's youth wing from 2010 to 2012 and is a founder of the Young Pirates of Europe. She holds an M.A. in political science and communications science from Johannes-Gutenberg-University Mainz, Germany.

Marc Tessier graduated from the National School of Administration, which is a French higher education establishment, created to democratise access to the senior civil service. Upon graduation he embarked on a great career as a senior civil servant, initially at the Inspectorate General of Finances, an interdepartmental auditing and supervisory body from 1973 to 1979. Then, he was successively Director General of the Havas Agency (1981-1987), Canal+ (1984-1986), canal+ international (1987-1995). In 1999, he was appointed Director General of France Televisions that he left in 2005 to become Director General of Netgem Media Services, then VidéoFutur.

Natasha Tusikov is Assistant Professor of criminology in the Department of Social Science at York University in Toronto, Canada. Natasha is also a visiting fellow at the RegNet School of Regulation and Global Governance at the Australian National University. Prior to her appointment to York University, she was a postdoctoral fellow in interdisciplinary legal studies at the Baldy Centre for Law and Social Policy at the State University of New York in Buffalo. Her research interests focus on technology, regulation and social control with a particular focus on the regulatory capacity of Internet intermediaries. Her book, Chokepoints: Global Private Regulation on the Internet (University of California Press, 2016) is the first book-length examination of intermediaries' work as gatekeepers for intellectual property rights holders (like Gucci) to police the

online trade in counterfeit goods. In this book, Natasha concludes that this type of informal private regulation is fundamentally reshaping the ways that states and powerful corporations control online behaviour and global flows of information. Before her work in academia, she was a researcher and intelligence analyst for the Royal Canadian Mounted Police.

Célia Zolynski is Associate Professor of private law at the University of Versailles Saint Quentin. She is co-director of the Intellectual Property and Digital technologies Master's Degree as well as the PID@N Master's Degree of the University of Paris Saclay. Her research and teaching activities focus on digital law, intellectual property law, business and consumer law, as well as the sources of law. She is the author of various publications in these fields, notably on the links between national and European law. She co-directs the Intellectual Property and Digital Law division of the Trans Europe Experts network and runs several multidisciplinary working groups, in particular on the protection and enhancement of data in the Big Data era. Since 2015, she is a member of the CNIL prospective committee.

Rolf H. Weber is Director of the European Law Institute and of the Center for Information Technology, Society and Law at the University of Zurich; in addition, he serves as a co-director of the University Priority Research Program "Financial Market Regulation". Having received his education in Switzerland and at Harvard Law School (Visiting Scholar 1980/81) Dr. Rolf H. Weber was ordinary Professor for Civil, Commercial and European Law at the University of Zurich, Switzerland from 1995 to 2016. From 2000 to 2015, he also was a permanent Visiting Professor at the Law Faculty of Hong Kong University, Hong Kong, and short-term senior lecturer at several European Universities. His main fields of research and practice are Internet and Information Technology Law, International Business Law, Competition Law and International Financial Law. From 2008 to 2015 Rolf H. Weber was member (Vice-Chairman) of the Steering Committee of the Global Internet Governance Academic Network (GigaNet). Rolf H. Weber serves as co-editor of several Swiss and international legal periodicals

and widely publishes in his research fields with particular emphasis to the legal challenges caused by the globalization. Besides that, he is engaged as an attorney-at-law.

Nicolo Zingales is Lecturer in competition and information law at Sussex Law School, in Brighton (UK). He is also affiliated researcher to the Stanford Center for Internet and Society (CIS), the Tilburg Institute for Law, Technology and Society (TILT) and the Tilburg Law and Economic Center (TILEC). His research spans across different areas of Internet law and governance, particularly concerning the roles and responsibilities of intermediaries in the online ecosystem. He is an editor of Medialaws, co-founder and co-chair of the UN Internet Governance Forum's Dynamic Coalition on Platform Responsibility, a member of the Observatory of Experts of the Internet & Jurisdiction Project, and a non-governmental advisor to the International Competition Network.

1 Online Platforms' Roles and Responsibilities: a Call for Action

Luca Belli and *Nicolo Zingales*

Since the World Summit on Information Society (WSIS) in 2005, Internet governance has been widely understood as the development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet. This definition has fostered a lively and interdisciplinary debate on what roles and responsibilities might be attributed to different stakeholder groups and in different contexts, particularly considering the extent to which their actions affect Internet users and society more broadly. In that regard, one of the most fertile grounds of discussion has been the **evolving notion of liability of Internet intermediaries**, defined by the OECD as entities that "bring together or facilitate transactions between third parties on the Internet"[14]. Originally, the focus of that discussion was on the need to provide intermediaries with legislative protections from liability for third party content, which appeared insufficient and inconsistent across domains and jurisdictions. Then gradually, the initial scepticism by some stakeholders matured into a shared understanding of the importance of these protections and the recognition of **best practices**, thanks also to consensus-building civil society initiatives such as those led by the Association for Progressive Communication[15] and by the Electronic Frontier Foundation, ultimately producing a set of guidelines entitled "Manila Principles on Intermediary Liability."[16]

14 See OECD, *The economic and social role of Internet intermediaries* (OECD Publications,,2010), <https://www.oecd.org/internet/ieconomy/44949023.pdf> [accessed 31 October 2017].

15 See Emilar Vushe Gandhi, 'Internet intermediaries: The dilemma of liability in Africa', (*APC News*,19 May 2014). <https://www.apc.org/en/news/internet-intermediaries-dilemma-liability-africa> accessed 31 October 2017; Nicolo Zingales, 'Internet intermediary liability: identifying best practices for Africa', (APC Publication, 2013), <https://www.apc.org/sites/default/files/APCInternetIntermediaryLiability_BestPracticesAfrica_20131125.pdf> [accessed 31 October 2017]

16 See 'Manila Principles on Intermediary Liability. Best Practices Guidelines for Limiting Intermediary Liability for Content to Promote Freedom of Expression and Innovation' (24 March 2015), <https://www.eff.org/files/2015/10/31/manila_principles_1.0.pdf> [accessed 31 October 2017].

While the need for the spreading of those best practices remains current and even increased after the submission of certain legislative proposals under consideration in a number of jurisdictions around the globe, a parallel discussion began to unfold concerning the potential effects on individuals of the private actions taken by intermediaries -in response to liability threats or otherwise-, in particular when it comes to the exercise of their fundamental rights. Participants in this discussion observe the negative consequences arising from the proliferation of private ordering regimes, and interrogate themselves about conceptual issues concerning the **moral, social and human rights responsibility** of the private entities that set up such regimes. The increasing importance of this notion of "responsibility" has not gone unnoticed, having been captured for example by the special report prepared by UNESCO in 2014[17], the study on self-regulation of the Institute for Information Law of the University of Amsterdam[18], the 2016 Report of the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression[19], the Center for Law and Democracy's Recommendations on Responsible Tech[20] and most recently, the Council of Europe's draft Recommendation on the roles and responsibilities of Internet intermediaries[21].

At the same time, the notion of "intermediary" is increasingly replaced in common parlance by the more palatable term of "platform", which evokes a role that goes beyond one of mere messenger or connector, and extends to the provision of a shared

17 Rebecca MacKinnon et al., *Fostering freedom online: the role of Internet intermediaries* (UNESCO Publication, 2014). <http://www.unesco.org/new/en/communication-and-information/resources/publications-and-communication-materials/publications/full-list/fostering-freedom-online-the-role-of-internet-intermediaries/> [accessed 31 October 2017].

18 Cristina Angelopoulos et al., 'Study of fundamental rights limitations for online enforcement through self regulation' (IVir, 2015) <https://www.ivir.nl/publicaties/download/1796> [accessed 31 October 2017]. .

19 Report of the the Special Rapporteur to the Human Rights Council on Freedom of expression, states and the private sector in the digital age, A/HRC/32/38 (11 May 2016) <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G16/095/12/PDF/G1609512.pdf?OpenElement> [accessed 31 October 2017].

20 Center for Law & Democracy, 'Recommendations for Responsible Tech' <http://responsible-tech.org/wp-content/uploads/2016/06/Final-Recommendations.pdf> [accessed 31 October 2017].

21 Council of Europe, Recommendation CM/Rec(2017x)xx of the Committee of Ministers to member states on the roles and responsibilities of internet intermediaries. https://rm.coe.int/recommendation-cm-rec-2017x-xx-of-the-committee-of-ministers-to-member/1680731980 [accessed 31 October 2017].

space defined by the applications within which users can carry out their activities and generate value. It is at this juncture that, at the 2014 Internet Governance Forum, the **Dynamic Coalition on Platform Responsibility** was created. The DCPR is a multistakeholder group established under the auspices of the United Nations Internet Governance Forum dedicated to the analysis of the role and responsibilities of online platforms from a technical, legal, social or economic perspective. Since its inception, DCPR has facilitated and nurtured a cross-disciplinary analysis of the challenges linked to the emergence of digital platforms and has promoted a participatory effort aimed at suggesting policy solutions.

The **Recommendations on Terms of Service and Human Rights**,[22] whose development was facilitated by the DCPR in 2015, constitute a prime example of such efforts. The Recommendations represent a first important step in identifying criteria through which platforms' private orderings can be held accountable for their impact on users' fundamental rights to freedom of expression, privacy and due process. More efforts of this type are encouraged to extend the discussion to other rights, recognise the appropriate role for public policy, and define sound mechanisms guiding platforms in their response to requests for removal, including any balancing of conflicting rights and interests. While the extent to which this type of work should be conducted at the global, regional or national level remains one of the governance challenges of our generation[23], the urgency of this discussion can hardly be overstated.

Hence, this book offers a response to the DCPR's call for **multistakeholder dialogue**, made ever more pressing by the diverse and raising challenges generated by the platformisation of our economy and, more generally, our society. Despite the evident need to address these challenges, finding consensus and a sense of shared purpose is not always an easy task. For example, significant controversy exists concerning the very **notion of "platform,"** and the type of actors whose responsibilities should take the

22 The Recommendations on Terms of Service and Human Rights are annexed to this book and can be found at <http://tinyurl.com/toshr2015> [accessed 31 October 2017].

23 See the work carried out to streamline the interactions between different regimes by the Internet & Jurisdiction Project, described at https://www.internetjurisdiction.net/.

centre stage in this discussion.[24] The above-mentioned DCPR Recommendations adopted a high-level definition, which is neutral as to the type of involvement in content creation or distribution, but refers to a specific type of intermediation that runs at the application and content layers, allowing users to "seek, impart and receive information or ideas according to the rules defined into a contractual agreement".

This definition excludes prima facie, from this particular discussion, telecommunications companies and Internet Access Providers (IAPs), which remain at the core of other forums such as the Telecommunications Industry Dialogue and the Global Network Initiative. Nevertheless, as an attentive reader of the present volume will notice, legal developments on the rights and obligations of "upstream" intermediaries such as IAPs and domain name registrars (and registries) are considered to the extent they inform, corroborate or anticipate the emergence of analogous legal issues "downstream". By way of example, the discussion arising from the pulling out of neo-Nazi content from certain domain name providers and content delivery networks (see e.g. David Kaye's mention of Cloudflare in his preface of this volume) closely follows the thread of combating "**hate speech**" that led to the adoption of similar measures by social media companies; it should therefore be considered as part of that broader tendency. Discussing in isolation from parallel developments at the upstream level carries the risk of missing important insights on legal remedies available to users affected by private measures, as is illustrated by the evolution of the legal framework concerning injunctions against innocent third parties in chapter 2.

The increasing centrality of digital platforms, both, in the collection and processing of personal data and in the production and dissemination of content, has attracted growing political and regulatory pressure over rights and responsibilities that ought to be

24 For example, the relatively specific definition adopted by the European Commission in its consultations on online platforms – focused on the connection between two interdependent user groups – has been criticised for casting too wide regulatory net, catching a wide range of actors, business models and functionalities. Nor did the European Commission achieve more consensus with its narrower notion of "platforms making available large amounts of copyrighted content" identified as targets of heightened duty of care in the proposal for a copyright directive. Indeed, this latter definition triggering discussion as to the meaning of "large amount" and whether this should be defined (also) in relation to the profits made through the provision of access to such copyrighted material.

attributed to them; and expectations are increasingly being placed on the role of large platform operators to provide "**safe**" online spaces for user engagement. This trend is visible in the legislative proposals that have emerged in various countries demanding social media companies to prevent hate speech, incitement to violence or hatred, and "dangerous **terrorist** recruitment material." In that regard, this volume offers some reflections on online platforms' roles and responsibilities in the eyes of regulators, warning about the dangers associated with an increasing instrumentalisation of these entities for the pursuit of a wide range of (often ill-conceived) public policy measures.

Over the last year, one of the most visible trends of platform regulation has manifested itself in the context of the identification and prevention of "**fake news**", stirring controversy over the role and impact of online platforms in influencing the shape and content of relevant discussions the public sphere. This discussion offers a perfect example of a recurring problem with platform regulation: an important part of the content that is supposed to be prohibited escapes clear legal definition. It comprises a variety of different phenomena and, therefore, arguably requires a combination of a wide range of measures that should not be based on vague terminology. While some proposals have called for special legislation to restore trust and create a level playing field, major platforms such as Google and Facebook have been quicker in putting forward solutions for those concerns, including structural responses and tools for users to limit their exposure to such misinformation.

A different but related problem has arisen regarding "**brand safety**", i.e. the concerns of advertisers in relation to the association of their ads with certain types of content deemed to be "inappropriate". In March 2017, following a letter by the Guardian and many brands pulling their ads from YouTube, Google announced to have heard concerns "loud and clear" and raised its bar for "hateful, offensive and derogatory content" which will be excluded from the association with Google ads. Much like in the context of fake news, swift response by the platforms to a pressing societal problem serves as a backstop to the spreading of harm, preventing possible legislative intervention. Yet, important questions remain

regarding the transparency, proportionality and effectiveness of the measures these companies have taken, and of their impact on small and independent news providers and for content creators, some of whom (particularly, those who offer content characterised as "sensitive") have seen their ad revenues dramatically reduced since Google adopted this revised policy. Similar questions arise in relation to the recent emphasis by the European Commission on platforms' responsibilities to protect users and society at large against the exploitation of their services for the dissemination of "**illegal content**", a concept which is left for platforms to determine on the basis of EU and national law[25].

In addition to these content-related trends, platforms are increasingly under the scrutiny of regulators for various concerns relating to **market power**, information asymmetry and **use and collection of personal data**. For example, the European Commission is considering the adoption of special legislation to assuage concerns of contractual exploitation towards platform-dependent businesses[26]. **Exploitation** is also a central concern of the criticism being levelled to platforms for their relationships with workers/employees, leading most recently to several tech companies developing a code of ethics for worker values[27]. Finally, there are multiple investigations on the possible exploitation of personal data, relating both to their unlawful acquisition and their misuse leading to discrimination and consumer harm.

Against this backdrop, the need for a **multistakeholder discussion** on the role and responsibilities played by online platforms in our society becomes crucial. This book is built on the previous efforts of the DCPR and, although it does not pretend to offer definitive solutions, it provides some elements of reflection that should be carefully

25 Communication from the European Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Tackling Illegal Content Online. Towards an Enhanced Responsibility for Online Platforms. COM(2017) 555 final.

26 Communication from the Commission to the European Parliament, The Council, The European Economic and Social Committee and the Committee of Regions on the Mid-Term Review on the implementation of the Digital Single Market Strategy A Connected Digital Single Market for All, COM (2017) 228 final.

27 Michael J. Coren, 'Silicon Valley's finest are finally developing a code of ethics' (Quartz, 20 April 2017), <https://qz.com/964159/the-president-of-y-combinator-sam-altman-is-leading-an-effort-to-develop-a-code-of-ethics-for-silicon-valley-in-response-to-president-donald-trump/> [accessed 31 October 2017].

considered by all stakeholders in their effort to shape sustainable policies addressing shared problems regarding digital platforms.

1.1 Exploring the Human Right Dimensions

This first part of the book explores some of the most pressing challenges regarding the impact that public regulations targeting digital platforms and self-regulation developed by such entities may have on their users' fundamental rights. Although human rights constitute a central topic of discussion throughout the whole book, what distinguishes this part is its focus on ways in which the human rights risks associated with platform law-making can be viewed and addressed.

In their opening chapter on "**Law of the Land or Law of the Platform? Beware of the Privatisation of Regulation and Police**," Luca Belli, Pedro Francisco and Nicolo Zingales argue that digital platforms are increasingly undertaking regulatory and police functions, which are traditionally considered a matter of public law. The authors emphasise that such functions have been growingly delegated to platforms by public regulation while, on the other hand, platforms are self-attributing such functions to avoid liability, de facto becoming private cyber-regulators and cyber-police. After highlighting the tendency towards delegation of public functions to private platforms, Belli, Francisco and Zingales provide concrete examples of such phenomenon. For example, the chapter scrutinise three types of delegations of public power: the imposition of open-ended injunctions against innocent intermediaries, typically for content removal or website blocking; the implementation of the right to content delisting against search engines, also known as the "right to be forgotten"; and the enlisting of numerous IT companies into a voluntary scheme to counter "illegal hate speech". The authors show in all these cases that the amount of discretion conferred on platforms is problematic from the standpoint of the protection of individual rights. Furthermore, the paper reviews the parallel copyright regime developed and implemented by YouTube, thereby emphasising another collateral effect of the privatisation of regulation and police functions: the extraterritorial application of a national legislation – US copyright,

in this case – which de facto turns the platform into a private proxy for global application of national regulation. The authors conclude highlighting some of the challenges and viable solutions for the protection of individual rights in an era of increasing privatisation of regulation and police.

In her chapter on "**Online Platform Responsibility and Human Rights**," Emily Laidlaw explores the human rights responsibilities of online platforms at the intersection of three areas: human rights, corporate social responsibility (CSR) and regulation. In this conceptual paper, Laidlaw untangles the governance problems in framing platform responsibility, focusing on the uneasy relationship between CSR and law, and identifying the difficulties in articulating what it means for a platform to respect human rights. The paper highlights the benefits and challenges in considering CSR as part of the relevant regulatory framework, in particular when it comes to the implementation of the UN Guiding Principles on Business and Human Rights. She concludes by identifying three key challenges for the future of platform governance: defining appropriate (and where possible uniform) rules for intermediary liability; clarifying the scope of application of the duty of respect; and developing the linkage between alternative dispute resolution mechanisms and human rights.

In "**Regulation *by* Platforms: the Impact on Fundamental Rights**," Orla Lynskey points out that the relationship between platforms and regulation is two-fold: in addition to the various forms of regulation affecting platforms, the latter also constitute a regulator themselves through "private ordering", with notable implications for economic, social, cultural and political dimensions of our lives. Lynskey explores, in particular, both direct and indirect ways in which platforms influence the extent to which we can exercise our rights, and argues that these implications are exacerbated when these platforms are in a position of power, for instance because of the number of individuals that use them. Importantly, she suggests that competition law is not sufficient to constrain platform behaviour, in particular when it comes to addressing "data power" (the power to profile and to exacerbate asymmetries of information) and "media power" (the power to influence opinion

formation and autonomous decision-making) which transcend the economic notion of market power. The chapter illustrates this point by reference to two examples (search engines and app stores) and concludes briefly identifying some of the options and challenges which policy-makers are confronted with when trying to tackle these issues.

In their chapter on "**Fundamental Rights and Digital Platforms in the European Union: a Suggested Way Forward**," Joe McNamee and Maryant Fernandez emphasise that it is important to understand which actors we are addressing when referring to "digital platforms": it may be counterproductive to categorise players as different as AirBnB, Google News and YouTube, to name but a few examples, as the same type of business. In this sense, the authors usefully suggest five classifications of platforms based on the relationship with consumers or businesses and based on the transactional nature of the relationship. Furthermore, this chapter notes that standard content guidelines of digital platforms do not necessarily respect the principle of legality or comply with fundamental human rights. In this regard, so called "community guidelines" often ban content, which is lawful and/or protected by European human rights law, often in an arbitrary and unpredictable way. McNamee and Fernández Pérez offer several examples of bad practice to corroborate their thesis and to conclude that, worryingly, neither governments nor Internet intermediaries appear to feel morally or legally responsible/accountable for assessing the durability or potential counterproductive effects of the measures that they implement. Importantly, the authors conclude the paper recommending the essential points that that future platform policies should incorporate in order to abide fully to the obligations prescribed by the Charter of Fundamental Rights of the European Union.

1.2 Data Governance

The second part of this volume is dedicated to the analysis of one of the most crucial elements concerning platform policies and regulations. The protection and use of individuals' personal data have crossed the borders of privacy-focused discussions, growing to encompass an ample range of topics, including competition,

property rights and the conflict with the collective right to access to information. The chapters included in this part provide a selection of analyses and some useful food for thought to identify priorities, find common ground and ponder what regulatory solutions might be elaborated.

Krzysztof Garstka and David Erdos open this second part with an important reflection on the right to be forgotten from search engines, entitled "**Hiding in Plain Sight: Right to be Forgotten & Search Engines in the Context of International Data Protection Frameworks**." The authors note that, in the wake of Google Spain (2014), it has become widely recognised that data protection law within the EU/EEA grants individuals a qualified right to have personal data relating to them de-indexed from search engines. However, this is far from being a uniquely EU/EEA phenomenon. Through an analysis of five major extra-EU/EEA international data protection instruments, Garstka and Erdos illustrate that most of such instruments lend themselves to a reasonable interpretation supporting a Google Spain-like result. In light of the serious threats faced by individuals as a result of the public processing of data relating to themselves, they argue that the time is ripe for a broader process of international discussion and consensus-building on the "right to be forgotten". They also suggest that such an exercise cannot be limited to the traditionally discussed subjects such as search engines, but should also encompass other actors including social networking sites, video-sharing platforms and rating websites.

The following chapter turns to the economic dimension of platform regulation, with Rolf Weber's analysis of the heated (but often misinterpreted) subject of "**Data Ownership in Platform Markets**." Weber points out that, while in the past platform regulations mainly concerned content issues related to accessible information and to provider responsibility, the growing debates about data ownership might also extend the scope of regulatory challenges to the economic analysis of platform markets. Relevant topics are collective ownership and data portability in the legal ownership context, as well as access to data and data sharing in case of an existing factual control about data. Weber opines that these

challenges call for a different design of the regulatory framework for the platform economy, thereby offering the proverbial "low hanging fruit" for future DCPR discussion.

The question of data ownership is further explored by Célia Zolynski in "**What Legal Framework for Data Ownership and Access? The Opinion of the French Digital Council.**" This chapter takes stock of the existing European debate and puts forward the approach of the French Digital Council (Conseil National du Numérique or CNNum). The Chapter is in fact on a CNNum Opinion issued in April 2017 to respond to the public consultation launched by the European Commission on online platforms, exploring various legislative and non-legislative options, including the creation of a property right over non-personal data, to encourage the free flow of data. First, the chapter argues that value creation mostly occurs when data is contextualised and combined with data from other datasets in order to produce new insights. Thus, the issue is not to establish a hypothetical right of data ownership; rather, it is about thinking and designing incentive regimes of data access and exchange between data controllers so as to encourage value creation. Indeed, contrary to a widely-held belief, data ownership does not necessarily facilitate data exchanges - it can actually hinder them. Above all, Zolynski makes the argument that a free flow of data should be envisioned not only between EU member states', but also across online platforms. Importantly, the chapter highlights that these new forms of sharing are essential to the development of a European data economy.

1.3 New Roles Calling for New Solutions

This part scrutinises the conundrum created by the blurring of distinction between private and public spheres in some of the most crucial fields affected by the evolution of digital platforms. By exploring the challenges of regulation, terrorism, terrorism and online payments, this third part highlights the heterogeneity of roles that platforms are undertaking while stressing the need of policy solutions able to seize such diversity and properly addressing the underling challenges.

Marc Tessier, Judith Herzog and Lofred Madzou open this part with their chapter on "**Regulation at the Age of Online Platform-based Economy: Accountability, User Empowerment and Responsiveness**." This paper expresses the views of the French Digital Council (CNNum) on the regulatory challenges associated with the development of the digital platform economy. This chapter is part of a more comprehensive reflection on online platforms policy-related issues developed by CNNum since 2013, when the Council had been assigned the task to organise a consultation with the French plaintiffs involved in the Google Shopping antitrust investigation, and made recommendations on policy issues posed by the rise of online platforms. Then, in 2014, the former Prime Minister asked the Council to organise a national consultation to elaborate France's digital strategy.

In this context, various market actors and civil society organisations reported their concerns about the lack of transparency regarding online platform activities and the asymmetry of power in their relationships with platform operators. To address these legitimate concerns, several recommendations were made; including the need to develop the technical and policy means to assess the accountability and fairness of online platforms. In 2016, following that recommendation, the government entrusted the Council with the task of overseeing the creation of an agency with these capabilities. As part of the preparatory work for that effort, Tessier, Herzog and Madzou discuss the challenges brought by the platform economy to our traditional regulatory tools, offering and a comprehensive policy framework to address them and the possible grounds for intervention of a potential Agency for Trust in the Digital Platform Economy

In her chapter on "**Countering terrorism and violent extremism online: what role for social media platforms?**" Krisztina Huszti-Orban highlights that social media platforms have been facing considerable pressure coming from states, in order to "do more" in the fight against terrorism and violent extremism online. Because of such pressure, many social media companies have set up individual and joint efforts to spot unlawful content in a more effective manner, thereby becoming the de facto regulators of online content and the gatekeepers of freedom of expression

and interlinked rights in cyberspace. However, the author stresses that having corporate entities carry out quasi-executive and quasi-adjudicative tasks, outsourced to them by governments under the banner of self- or co-regulation, raises a series of puzzling questions under human rights law. In this perspective, the chapter outlines the main human rights challenges that are arising in the European context, in relation to EU laws and policies as well as Member State practices. In Europe, the issues of terrorism and violent extremism online have become uppermost in the political agenda and, in such context, the author argues that the lack of internationally agreed definitions of violent extremism and terrorism-related offences raises the risk of excessive measures with potential cross-border human rights implications. Furthermore, Huszti-Orban analyses the problems arising from the attempts to broaden the liability of Internet intermediaries in the counter-terrorism context. Crucially, the paper emphasises the need to provide social media platforms with human rights-compliant guidance with regard to conducting content review, the criteria to be used in this respect and the specialist knowledge required to perform these tasks appropriately. The chapter also stresses the role of transparency, accountability and independent oversight, particularly considering the public interest role that social media platforms play by regulating content to prevent and counter terrorism and violent extremism.

In "**Revenue Chokepoints: Global Regulation by Payment Intermediaries**", Natasha Tusikov argues that payment intermediaries are becoming go-to regulators for governments and, in a recent development, for multinational corporations' intent on protecting their valuable intellectual property rights. More problematically, she stresses that those intermediaries that dominate the online payment industry (namely Visa, MasterCard and PayPal) can enact revenue chokepoints that starve targeted entities of sales revenue or donations and thereby undertake many of these regulatory efforts in the absence of legislation and formal legal orders, in what is commonly termed "voluntary industry regulation." Drawing upon interviews with policy-makers, intermediaries and right-holders, the chapter argues that governments strategically employ the narrative of "voluntary intermediary-led" in order to distance the state from

problematic practices. Further, it contends that payment platforms regulatory efforts are part of a broader effort to shape Internet governance in ways that benefit largely western legal, economic, and security interests, especially those of the United States. The conclusion is, in line with other contributions in this book, that intermediary-facilitated regulation needs some serious thinking and must take place within an appropriate regulatory framework, especially when payment platforms act as private regulators for private actors' material benefit.

It is not a coincidence that the last chapter concludes precisely where the discussion began in the opening chapter: the observation of widespread delegation of regulatory and police functions to private entities without an adequate complement of rights and remedies available to protect the affected individuals. As pointed out by virtually every contributor in this book, that is particularly problematic when platforms are in a position where they effectively decide the meaning, scope and level of protection of fundamental rights. This situation calls for a reflection on the goals for regulatory intervention in a platform society, and the role that private platforms can and should play in ensuring respect for individual rights.

PART I

Exploring the Human Right Dimensions

2 Law of the Land or Law of the Platform? Beware of the Privatisation of Regulation and Police

Luca Belli, Pedro Augusto Francisco **and** ***Nicolo Zingales***

Abstract

This chapter argues that digital platforms are increasingly undertaking regulatory and police functions, which are traditionally considered a matter of public law. The authors emphasise that such functions have been growingly delegated to platforms by public authorities, while at the same time platforms are self-attributing such functions to avoid liability, de facto becoming private cyber-regulators and cyber-police.

After highlighting the tendency towards delegation of public functions to private platforms, we provide concrete examples of such phenomenon. For example, the chapter illustrates three types of delegations of public power: the imposition of open-ended injunctions against innocent intermediaries, typically for content removal or website blocking; the implementation of the right to content delisting against search engines, also known as the "right to be forgotten"; and the enlisting of numerous IT companies into a voluntary scheme to counter "illegal hate speech". We show in all these cases that the amount of discretion conferred on platforms is problematic from the standpoint of the protection of individual rights.

Furthermore, the paper scrutinises the case of the parallel copyright regime developed by YouTube, to emphasise another collateral effect of the privatisation of regulation and police functions: the extraterritorial application of a national legislation – US copyright, in this case – which de facto turns the platform into a private proxy for global application of national regulation. We conclude highlighting some of the challenges and viable solutions for the protection of individual rights in an era of increasing privatisation of regulation and police.

2.1 Introduction

Our analysis departs from the observation that digital platforms[28] are increasingly undertaking regulation and police functions, which have traditionally been considered a matter of public law. In particular, such functions have been growingly delegated to platforms by public regulation[29], while at the same time platforms are self-attributing such functions in order to avoid liability, *de facto* becoming private cyber-regulators and cyber-police. This tendency is exemplified tellingly by a series of cases we discuss in sections 2 and 3, focusing on different kinds of intermediaries, and illustrating their growing role as Internet points of control.

First, we scrutinise three types of delegations of public power: the imposition of open-ended injunctions against innocent intermediaries, typically for content removal; the implementation of the right to content delisting against search engines, also known as the "right to be forgotten"; and the enlisting of a number of intermediaries into a voluntary scheme to counter "illegal hate speech". We show in all these cases that the amount of discretion conferred on platforms is problematic from the standpoint of the protection of individual rights. Second, we review the parallel copyright regime developed by YouTube, which can be deemed as the most utilised content distribution platform. This latter example is particularly useful to emphasise another collateral effect of the privatisation of regulation and police functions, which is the extraterritorial application of a national regulatory regime – in this case, US copyright legislation – *de facto* turning the platform into a private proxy for global application of national regulation.

Lastly, we draw some conclusions, based on the presented case studies, highlighting challenges and possible solutions for the protection of individual rights in an era of increasing privatisation of regulation and police.

---

28 For purposes of this article, we rely on the definition of "platform" laid out in the DCPR Recommendations on Terms of Service and Human Rights, which refers to "any application[] allowing users to seek, impart and receive information or ideas according to the rules defined into a contractual agreement". See Belli, De Filippi and Zingales (2015), Annex 1 (n).

29 Here, the term "regulation" should be considered as encompassing both the activity of issuing rules (rulemaking) and the activity of adjudicating disputes and taking decision (ruling).

2.2 The Rise of Platforms as Points of Control

Public law and international relations are grounded on the assumption the states and international organisation are the only actors having legitimacy to elaborate and implement binding norms. In this sense, Max Weber critically influenced the evolution of domestic public law, arguing that states are the "political enterprises"[30] characterised by "the monopoly of the legitimate use of physical force within a given territory"[31] while Hans Kelsen affirmed the essential unity between state and legal order, thus considering state and law as synonyms[32]. However, these assumptions take a different flavour at the international level, where no entity may claim the monopoly of force or the legitimacy to unilaterally establish binding rules. In this context, private actors have long taken the lead and bridged the gap left by the lack of international public authority, through the institution of private ordering systems. Such systems structure[33] in a very effective fashion a wide range of variegated sectors, spanning from global finance to organised crime[34] and, of course, the online environment.

By nature, the Internet environment and particularly its application layer – which is composed of privately developed and run platforms – lends itself very well to the surge of private authority to provide law and order while avoiding conflicts of jurisdiction. Indeed, the very commercialisation of the Internet was driven by the belief that "the private sector should lead"[35] the expansion of electronic commerce over the Internet on a global basis.

Considering the above, it is not a surprise that the digital platforms that populate cyberspace have long established private mechanisms, which represent a much more efficient and reliable

30 Weber (1919).

31 *Ibid.*

32 Kelsen (1967).

33 Susan Strange's concept of "structural power" (Strange,1988) is useful to describe very well the capability of private entities to shape frameworks within which (natural or legal) persons relate to each other. For a discussion of how such concept can be applied to internet intermediaries, see Horten (2016).

34 Hall and Biersteker (2002).

35 See W J Clinton and Al Gore Jr (1997).

alternative to conflicting and ineffective public institutions in the online world. As such, the ineffectiveness of state coercion – which in the offline world confers public actors a certain degree of authority and leads citizens to respect legislation – has prompted private players to replace it with the contractual rules and technical architecture that establish what behaviours are allowed in the offline world. In this perspective, digital platforms may be considered as cyberspaces in the sense of true virtual territories whose frontiers are defined by their technical architecture[36]. Notably, platform providers concentrate the capacity to unilaterally establish the law of the (cyber)land, enforce it and utilise their self-established rules to adjudicate conflicts between platform users.

First, platforms enjoy the capacity to regulate the behaviour of their users via their Terms of Service (ToS), which unilaterally establish what content users are authorised to access and share, what activities they are allowed to perform, as well as what data will be collected about users and how such data will be processed.[37] One of the salient features of platforms' ToS is that parties do not negotiate them but, on the contrary, the platform provider defines the conditions in a standard fashion – as it happens in all adhesion or boilerplate contracts – and the platform users can only decide to adhere or not to the pre-established terms.[38] In this context, the platform user is an adhering party, whose bargaining power is limited to the choice between "take it or leave it" thus giving to the ToS the force of a "law of the platform," which is established and modifiable uniquely by the platform provider. Furthermore, such quasi-regulatory power may not only be exercised with regard to the definition of substantive provisions enshrined in the platform's ToS but also with regard to the criteria according to which decisions will be taken by the platform when implementing its ToS as well as the procedural and technical tools to be utilised to put into effect the platform's ToS and decisions.

Secondly, differently from legislation and, more generally, from

36 Belli (2016:202, 219).

37 See Belli & Venturini (2016).

38 See Belli & De Filippi (2012); Radin (2012); Kim (2013).

any type of public regulation, platforms' private ordering does not need to be implemented by public executive organs. By contrast, digital platforms can directly implement their self-defined private regulation by designing the platform's technical structure according to the ToS, in a way that only allows users to perform the actions that are permitted by the platform's rules of engagement. Regulation by architecture[39] is also possible in the off-line but the level and scale of control achieved by the digital architectures of online platforms is extremely difficult to achieve even in the most authoritarian regimes of the offline world. Moreover, the algorithms that enable the platform's functionalities – for instance, establishing the order according to which information will be displayed on the platform's timeline – do not need implementation, for they are self-executing norms[40]. Platforms may also independently establish and run alternative dispute resolution and other private remedy mechanisms, as we stress in section 2.b, including by employing individuals who actively monitor users' compliance with the private regulation.[41]

Thirdly, platforms usually include – and frequently impose[42] – alternative dispute resolution mechanisms to solve conflicts amongst users based on the law of the platform. As such, these intermediaries do not simply enjoy a quasi-normative power to establish the ToS and the quasi-executive power to enforce them but they also enjoy the quasi-judicial power to take decision based on the ToS provisions, for instance deliberating what constitutes "obscene" or "harmful" content. However, such private decision-making may frequently lead to erroneous decisions and over-restriction, as has been stressed by Urban, Karaganis and Schofield (2017), with regard to takedowns of

39 In this sense, Lawrence Lessig argues that regulation of real spaces can define the constraints that real space creates and, likewise, the regulation of the cyberspaces' architecture defines constraints on cyberspaces. See Lessig (2006:127-128).

40 Belli (2016:140-144).

41 As an example, Facebook currently employs a team of more than 7,500 "community operators" dedicated to the review "millions of reports" of abusive content that Facebook receives weekly. See Mark Zuckerberg officially announcing the hiring of 3,000 extra operators to cope with the increasing reports of "abuse", on 3 May 2017, supra n. 3.

42 In this regard, a recent study conducted by the Center for Technology and Society at Fundação Getulio Vargas analysed the ToS of 50 digital platforms, demonstrating that 34% of the analysed ToS imposed arbitration as the only method for dispute resolution. See Center for Technology and Society at Fundação Getulio Vargas (2016).

supposedly illicit content.

Although the expansion of private regulation over individuals should not be considered necessarily as a negative phenomenon, the ways in which business actors exercise their "private sovereignty" should be subject to public scrutiny, in order to avoid the emergence of abusive conducts. As pointed out by Chenou and Radu (2017), the rise of private authority in the online context does not necessarily result in a loss of sovereignty and decision-making power for the state, but it rather stimulates a hybridisation of governance. Indeed, it seems that the supposed efficiency of digital platforms' private enforcement is leading public actors to increasingly delegate regulatory functions to private actors. In this perspective, the OECD already stressed in 2011 the pivotal role that Internet intermediaries, such as digital platforms, play in advancing public policy objectives.[43] This consideration is leading an ample range of governments to utilise digital platforms – and Internet intermediaries in general – as proxies in order to reaffirm their national sovereignty online.

However, it should be emphasised that, in their pursuit of efficiency or compliance with national regulation, platforms end up focusing on cost minimisation and avoidance of their potential liability rather than individual rights maximisation. Moreover, the entrustment of platforms with regulatory functions tends to increase their power *vis a vis* market participants which depend on the platform's services, and often entrench already powerful market positions by imposing regulatory burdens on a whole category, to the disadvantage of smaller competitors. Finally, it should not be underestimated that platforms may choose to simply implement domestic legislation at the global level, rather than designing a framework better suited to meet multicultural needs and exceptions, thereby leading to the extraterritorial implementation of a discretionarily chosen regime. In the following sections, we offer some concrete examples, corroborating what we have argued above with evidence and illustrating the rise of platforms as *de facto* private regulators and police of cyberspace.

43 See OECD (2011).

2.3 The Delegation of Regulatory and Police Functions to Private Intermediaries

In recent years, the above-mentioned type of delegation of public functions to online platforms has increased exponentially. As discussed, such transfer of responsibilities is grounded upon the recognition of the instrumentality of Internet intermediaries in advancing public policy objectives. This can be explained by digital platforms' essential role with regard to the circulation of information online, as well as by the inescapable need for any regulatory framework to involve platform in the implementation process, in order to be effective. However, as illustrated below, the varying mechanisms by which such involvement is established are typically lacking in the definition of limits to the platforms' discretion, thus failing to secure due respect for the fundamental rights of the individuals who bear the consequences.

Three prominent examples of this tendency are: (i) the use of injunctions against (innocent) intermediaries to remove illegal content from their properties; (ii) the entrustment of data controllers with the delisting of specific information, implementing the so called "right to be forgotten"; and (iii) the enlisting of a selected number of ICT companies for the countering of "illegal hate speech". These examples vividly illustrate that the tasks assigned to digital platforms as private executors of regulatory objectives can morph into private law-making and adjudication, where platforms not only choose the means of implementation of the delegated functions, but also substantially take part in the definition and interpretation of the rights and obligations of their users.

2.3.1 Injunctions against Innocent Third Parties

The first example concerns a possibility that the European Union has explicitly established in its legislation concerning intellectual property enforcement[44]. Indeed, according to Article 11 of the Intellectual Property Enforcement Directive of 2004, "Member States shall [...] ensure that rightholders are in a position to apply

44 See Husovec (2017).

for an injunction against intermediaries whose services are used by a third party to infringe an intellectual property right" (IPR). The interpretation of this provision as sufficient legal basis to trigger the intermediary's duty to assist rightholders, even in the absence of liability, was confirmed in *L'Oreal v Ebay*[45]. In this trademark-related case, which involved the online marketplace eBay, the European Court of Justice also clarified that such injunctions may entail the prevention of future infringements of the same kind[46]. Worryingly, the Court did not specify what would constitute an infringement of that "kind"; nor did it indicate what specific types of measures that can be imposed through such injunctions[47]. However, it provided an admonition to EU Member States that such measures must strike a "fair balance" between on the one hand, the right to intellectual property and the right to an effective remedy for the IPR holder, and on the other hand, the intermediary's freedom to conduct business and the end users' right to personal data protection, privacy and freedom of expression[48].

In a later case, the Court provided further details on the meaning of this admonition with regard to injunctions imposing website blocking. Conspicuously, such measures shall "at least partially prevent and seriously discourage the access to a targeted website"[49] but without leading to unbearable sacrifices for the intermediary in question[50] and without "unnecessarily depriv[ing] Internet users of the possibility of lawfully accessing the information available"[51]. It also established that any such measures must give the court dealing with enforcement proceedings a possibility to assess their degree of reasonableness; and must provide a possibility for Internet users to assert their rights before a court once the implementing measures taken by the Internet

45 Case C-324/09, *L'Oreal v. eBay*, ECLI:EU:C:2011:474, paras. 137-144.

46 Para. 144.

47 The Court only provided two examples: the suspension of the infringer, and measures that make it easier to identify customers who are operating in the course of trade. See paras. 141- 142.

48 Para. 143.

49 Case C-314/12, *UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH,* ECLI:EU:C:2014:192. Para. 57.

50 Para. 62.

51 Para. 63.

service provider are known[52]. Despite these important caveats, it cannot be neglected that the answers to a number of crucial questions for the effectiveness of fundamental rights protection remain subject to the discretion of the platform – or any other intermediary – implementing the measure.

This is especially problematic considering that the CJEU admitted[53] the possibility for courts to issue injunctions imposing an "obligation of result", as opposed to an obligation to adhere to a prescribed course of conduct ("obligation of conduct[54]"). In practice, such injunctions to obtain a particular result entail a choice between an ample range of measures with different relative impact on fundamental rights. Letting aside doubts about the suitability of such cost-benefit analysis to determining the scope of protection of fundamental rights, it is evident that economic incentives directly impact the effectiveness of protection afforded to individuals. Intermediaries are naturally inclined to err in favour of more restrictive measures, rather than to try and devise more elaborate and costly solutions that accurately balance conflicting rights: restricting access to content exhaust the demands of copyright holders, while affected subjects would need to file a separate claim in order to mitigate its adverse effects.

The trend of granting injunctive relief against innocent third party should not be considered as a European specialty and can also be noticed in other jurisdictions, notably the United States, where a number of orders have been issued requiring domain name registries, Internet service providers, payment intermediaries, search engines and social media to prevent the accessibility of infringing websites.[55] More recently, the trend was also embraced for the first time by the Canadian Supreme Court in *Google v Equustek*[56]. Affirming the lower court's opinion that imposed

52 Para. 57.

53 *Id.*

54 See Conde (1999:102).

55 See, e.g., *Hermes v. Doe*, (SDNY April 30, 2012); *Chanel Inc. v. Does* (D. Nev., Nov. 14, 2011); *ABS-CBN Corporation v Ashby*, Case (Dist. Or. Aug. 8, 2014); *Richemont International SA v Chen*, Case (SDNY Jan. 4, 2013); *Arista Records LLC v. Tkach*, 122 F.Supp.3d 32 at 33-38 (SDNY 2015).

56 *Google Inc. v. Equustek Solutions Inc.*, 2017 SCC 34.

Google to delist certain trademark-infringing websites on a worldwide level, the Canadian Supreme Court found it justified to do so on the basis of its equitable jurisdiction, which among other things allows the issuing of orders against non-parties that facilitate the commission of wrongdoing[57]. Crucially, the Court found "unpersuasive" Google's argument that the order clashes with the right to freedom of expression recognised in other countries, requiring it instead to prove in separate proceedings that any such conflict has actually arisen.

2.3.2 The Right to Be Forgotten and the Rise of Private Remedy Mechanisms

A second example of delegation concerns the implementation of the so called "right to be forgotten" defined by the CJEU in the *Google Spain* case[58]. In that case, the Court affirmed the existence of the right of all individuals to obtain erasure of their personal data from the results of search engines prompted by a search for their name, whenever such information is "inadequate, irrelevant or no longer relevant, or excessive." While the judgment has been primarily criticised for its insufficient consideration of freedom of expression, the most striking implication for our purposes is that it leaves the responsibility of implementing the aforementioned right in the hands of a private entity. Although the result of the private pondering between the accessibility and the elimination of the from the search results under an individual's name may be subsequently appealed by that data subject to the relevant data protection authority, we should stress that this mechanism creates not only one, but potentially multiple regimes of private governance running in parallel to (and possibly afoul of) the domestic legal systems.

Shortly after the ruling, all three major search engines in Europe (Google, Microsoft Bing and Yahoo) acted as *de facto* regulators creating a specific web form that enables users to provide the

57 Para. 31.

58 Case C-131/12, *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González*, ECLI:EU:C:2014:317. For a more in-depth analysis, see Zingales and Janczuck (2017).

relevant information that should be delisted[59], each with their own different requirements. For example, while Google and Yahoo provide a blank space in the form for individuals to explain how the page relates to the data subject and why its content is "unlawful, inaccurate, or outdated",[60] while Microsoft Bing poses a number of additional questions.[61]

Furthermore, although these companies have not yet released any criteria they use to adjudicate conflicting rights, it is likely that significant divergence arises as a result of the open-ended character of the guidelines provided by the Article 29 Working Party[62]. The lack of prescriptions detailing the implementation of those guidelines in accordance with national freedom of expression standards, granting these entities wide discretion in the implementation of the right, is problematic for at least two reasons. First, search engines are not public courts, and thus employees tasked with making these determinations will not have the same competence and standards of professional ethics and independence that bind members of the judiciary[63]. The fact that the relevant DPA and a court may be asked to review such determinations is not sufficient to overcome this concern, as such requests are unlikely to be systematic, and can only be made by the affected data subject (not by the individual or entity who has produced the content whose accessibility is in question). Second,

59 According to press coverage, Google made its form available in June 2014, and Microsoft in July of the same year. It is less clear when the form first appeared on Yahoo!, although it was reported to be already in place on December 1st, 2014. See Schechner (2014); and Griffin (2014).

60 For Google, see <https://www.google.com/webmasters/tools/legal-removal-request?complaint_type=rtbf&visit_id=1-636297647133257433-1626206613&rd=1> [accessed 31 October 2017]; for Yahoo, see <goo.gl/3qUdTe> [accessed 31 October 2017].

61 See <https://www.bing.com/webmaster/tools/eu-privacy-request> [accessed 31 October 2017]. Specifically, claimants must indicate (1) whether they (and presumably anyone on behalf of whom the application is made) are public figures; and (2) whether they have or expect to have a role in the local community or more broadly that involves leadership, trust or safety. Furthermore, claimants are asked to qualify the information that Bing is requested to "block" as (a) inaccurate or false; (b) incomplete or inadequate; (c) out-of-date or no longer relevant; or (d) excessive or otherwise inappropriate. They are also invited to indicate why their "privacy interest" should outweigh the public's interest in free expression and the free availability of information. Last, but not least, they are given the opportunity to upload supporting documentation.

62 Article 29 Working Party, Guidelines on the implementation of the Court of Justice of the European Union Judgment on 'Google Spain and Inc v. Agencia Espanola de Proteccion de Datos (AEPD) and Mario Costeja Gonzales' C-131/12., 14/EN WP 225 (26 November 2014) <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf> [accessed 1 November 2017].

63 Haber (2016).

the nature and depth of balancing users' fundamental rights may be affected by the economic incentives and the interest of those entities to conduct their business in the most efficient and lucrative fashion. For instance, it is clear that a very probing inquiry into the circumstances of each case would impose serious costs on the search engine. Similarly, it runs against the incentives of search engines operators to publish a detailed list of their criteria for decision-making, as the availability of such criteria would make users' claims more sophisticated and more complex to decide. Under these conditions, as a result of the concerns for transparency of the criteria and fairness over their substantive standards, the role of online platforms in giving effect to individual rights becomes at least questionable.

2.3.3 Countering of Illegal Hate Speech

Our third example of public functions delegation relates to the agreement defined by the European Commission in conjunction with Facebook, Microsoft, Twitter and YouTube, with the aim of adopting a specific code of conduct on "countering the spread of illegal hate speech online."[64] Above all, the code of conduct requires such companies to have in place "Rules or Community Guidelines clarifying that they prohibit the promotion of incitement to violence and hateful conduct," and "clear and effective processes to review notifications regarding illegal hate speech on their services so they can remove or disable access to such content", in the majority of cases in less than 24 hours since the reception of a valid notification. It also demands companies to "raise awareness" about their rules and procedures with users and Member States' designated national contact points, and encourages the provision of notice and flagging mechanisms to tackle hate speech with the help of experts from civil society organisations through the creation of a group of "trusted reporters". On its part, the European Commission commits, in coordination with Member States, to promote adherence to the Code to other relevant platforms and social media companies, thereby setting the conditions for this

64 The text of the "Code of Conduct" agreement can be found at <http://ec.europa.eu/justice/fundamental-rights/files/hate_speech_code_of_conduct_en.pdf> [accessed 31 October 2017].

to serve as a basis for promoting greater protection against hate speech in the sector.

As pointed out by Article 19, there are significant problems of overbreadth with the definition of "hate speech" provided by the Code, which derives from the Commission's Framework Decision on Combating Certain Forms and Expressions of Racism and Xenophobia by Means of Criminal Law.[65] Notably, the code of conducts presents an overbroad focus on "incitement to hatred" (as opposed to the ICCPR's "incitement to discrimination, hostility and violence"), a lack of reference to the intent of the speaker and an unspecified threshold of seriousness for the forms of racism and xenophobia to be considered as illegal[66]. Furthermore, as noted by EDRI, the Code effectively creates a framework for privatised law-enforcement by enabling the above-mentioned companies to come up with an own definition of "hate speech" in their rules and to community guidelines, and review removal requests against those rules and guidelines[67]. Finally, there are concrete problems of oversight in the application of the Code, given that there is no direct reporting from the companies adhering to the code, but only "testing" of the reactions received by organisations that volunteered to submit notices in different Member States[68]. As a result of these tests, the review of the practices of these companies one year after the enactment of the Code revealed deficiencies in feedback provided to users submitting notification, corroborating the picture that companies enjoy a large amount of discretion both in the definition of offenses and in enforcement of those prohibitions.[69]

Interestingly, the Commission has also of recent facilitated the adoption of a Common Position of national authorities within the Consumer Protection Cooperation network concerning the

65 Article 19 (2016).

66 *Id.*, pp. 7-8.

67 McNamee (2016).

68 European Commission, 'Code of Conduct on countering illegal hate speech online: First results on implementation' (December 2016), Factsheet, <http://ec.europa.eu/information_society/newsroom/image/document/2016-50/factsheet-code-conduct-8_40573.pdf> [accessed 31 October 2017].

69 European Commission, 'Code of Conduct on countering illegal online hate speech 2nd monitoring', Press Release IP/17/1471, <http://europa.eu/rapid/press-release_MEMO-17-1472_en.htm> [accessed 31 October 2017], at 1 and 5.

protection of consumers on social networks, which seemingly takes issues with the framework created by the Commission through the Code of Conduct[70]. Lamenting the "general and unspecified" nature of the criteria used by social networking platforms to refuse to display or remove content, the Position explains that contract clauses granting "unlimited and discretionary power" without identifying sufficient criteria for the suitability of user-generated content are illegal under consumer law, as they create a significant imbalance *vis à vis* consumers. In addition, the Position proposes the establishment of a standardised communication format between social media and consumer protection authorities including, in the case of requests for removal, information of the action taken and, if no action is taken, the legal and factual reasons for that. While this Position constitutes a significant step towards greater accountability of social networking platforms for their removals and a model exportable to other types of digital platforms, it still does little to fix the problems originated by the vaguely worded delegation that we have described in this Section.

2.4 YouTube and iRegulate

In this Section, we consider a more specific example with regard to content regulation. Specifically, we analyse how YouTube shapes copyright through its own ToS, which are based on US copyright law, thus creating a hybrid public-private regime that is entirely privately implemented. The case of the content industry is particularly interesting, because few are the relations that are not intermediated by a third party and therefore, there is ample margin for platform action. To reach a user, the work created by an author must be fixed in some media – be it physical or digital – and subsequently distributed. In the content industry of the 20th century, these activities were typically performed by intermediaries such as big record companies, publishers and producers. These actors have been remarkably impacted by the popularisation of ICTs and by the digitisation of information. However, although digital technologies have completely changed

70 European Commission, 'The European Commission and Member States consumer authorities ask social media companies to comply with EU consumer rules', Press Release IP/17/631, <http://europa.eu/rapid/press-release_IP-17-631_en.htm> [accessed 31 October 2017].

the industry settings, such impact has not resulted in the extinction of the aforementioned intermediaries, as many thought at the end of the last century.[71] Indeed, differently from what was originally expected, the mid-2000s witnessed the emergence of streaming platforms, shifting intermediation towards the offering of content as a service, rather than as a product.

The historical reality of content industries shows that several actors who were relevant in the past still retain their importance. Although the configurations have changed, the power relations have been maintained as old intermediaries have adapted to the current scenario and big copyright holders continue to influence how copyrighted works can be reproduced and distributed. What is different now is the emergence of a new breed of actors in the content industries: the digital distribution platforms. These platforms can be characterised by their private governance, consisting in privately defined rules along with the provision of an infrastructure designed to allow only the authorised interactions between the involved actors[72]. Their business models depends on the use of information and communication technologies to connect people, organisations and resources, inside ecosystems where value is generated and goods and services are exchanged. Ultimately, the goal of digital distribution platforms is to foster the establishment of agreements between their users and facilitate any type of exchange that can generate value from the distributed material.

Among these digital platforms, one of the most notable is certainly YouTube. Created in 2005 and acquired by Google just over a year later, YouTube is by far the biggest online video streaming platform in the world, with – according to its own website[73] – over a billion users, which would mean almost one-third of all Internet users. The website also states that, In the US, the platform reaches more people between 18 and 49 years old than any cable TV. YouTube has been influencing content consumption in such

71 In this sense, see Parker, Alstyne & Choudary (2016); Evans and Schmalensee (2016); Moazed & Johnson (2016).

72 Rochet & Tirole (2003).

73 See 'YouTube in numbers' <https://www.youtube.com/intl/en-GB/yt/about/press/> [accessed 31 October 2017].

a way that it cannot be perceived as a mere channel between creators and consumers. As a cultural-industry intermediary, Youtube implements its own content governance technologies and imposes on its users the US Digital Millennium Copyright Act (DMCA), a legal regime that should only apply to US users – not users in any country in which a video is watched or uploaded.

YouTube's private copyright protection is enforced through two mechanisms: copyright takedowns and the Content ID system. The copyright takedown mechanism works in accordance with the DMCA. US copyright law determines that online hosting providers shall not be liable for copyright infringement if they do not have actual knowledge of the infringing material on its system, and have designated a DMCA agent to receive notifications of allegedly illegal content. Once received a notice, the online service provider wishing to escape potential liability must expeditiously take that content down. Only subsequently can the content uploader file a counter-notice, in which case Youtbe shall make that content available after 10 to 14 days, unless the original claimant demonstrates to have filed an order in court against the alleged infringer.

As is well known, YouTube is a video-sharing platform which also offers users the ability to create their own channels, where they can stream or simply share with followers their own videos. Any person who believes their copyright-protected work was posted in a channel without authorisation may submit an infringement notice through a dedicated web form.[74] YouTube will remove the allegedly infringing video and the owner of the channel that uploaded it will receive a "copyright strike". According to YouTube's privately established procedure, if a channel receives three copyright strikes, its owner's account will be terminated, all their videos will be removed – importantly, even the ones that were *not* infringing any rights – and the user will not be able to create new accounts. After being notified that the infringing video has been struck, the owner has three possible courses of

74 See 'Submit a Copyright takedown notice' <https://support.google.com/youtube/answer/2807622?hl=en&ref_topic=2778544> [accessed 31 October 2017].

action.[75] First, the notified user can decide to wait for the strike to be removed after 90 days, subject to the condition that the user attends YouTube's "Copyright School." This means that the owner must watch an animated video explaining the functioning of copyright and answer 4 true-or-false questions about the topic to verify the content has been understood correctly.

Despite its friendliness and humour – the Copyright School video consist in a Happy Tree Friends short animation – the video has a strong message about the dangers of using copyright protected materials without authorisation, alerting the audience that infringing copyright can result in economic loss. Even though there is a short mention to the existence of fair use[76] and similar provisions in the US and other countries jurisdictions, the video is emphatic in saying that any misuse or false allegations can result in a court case.[77] The underlying message is to always use original content, despite the fact that the use of third-party content may be legally legitimate in several cases. The second possible action is to contact directly the person who triggered the strike and ask this person to retract the claim, while the third option for the recipient of a strike is to submit a counter-notice through an ad hoc web form.[78] YouTube then forwards the counter-notice to the original claimant, who has 10 days to show proof that he or she has initiated a court action aimed at keeping the content down. Failing that, the platform will put the video back online.

The Content ID System is a more sophisticated tool. Since 2007, in order to legitimise itself as a reliable and law-abiding platform and to consolidate its position as a mainstream distribution medium, YouTube created a new system of digital identification, which can

75 See UN Human Rights Committee.t Act'or the dissemination ofs of EU and national law. See 'Copyright Strike Basics' <https://support.google.com/youtube/answer/2814000?hl=en&ref_topic=2778545> [accessed 31 October 2017].

76 The US Copyright Office defines fair use as the legal doctrine that promotes freedom of expression by permitting the unlicensed use of copyright-protected works in certain circumstances. Section 107 of the US Copyright Act provides the statutory framework for determining whether something is a fair use and identifies certain types of uses—such as criticism, comment, news reporting, teaching, scholarship, and research—as examples of activities that may qualify as fair use. See more at <https://www.copyright.gov/fair-use/more-info.html> [accessed 31 October 2017].

77 See YouTube's 'Copyright School' <https://www.youtube.com/copyright_school> [accessed 31 October 2017].

78 See Youtube's 'Counter Notification Basics' <https://support.google.com/youtube/answer/2807684?hl=en&ref_topic=2778545> [accessed 31 October 2017].

identify copyright protected materials. The system is based on the premise that any video has unique attributes that allows identification of the material even from within a short clip.[79] In this system, any copyright holder can establish a partnership with YouTube, where it uploads its protected material and allows it to become part of a reference database. YouTube can then automatically detect the use of that material in other videos. When the copyright holder establishes this type of partnership, three different actions become available to manage any further material that matches with the uploaded one. The copyright holder can decide to block a whole video from being viewed; to mute a video that contains the copyright protected music; to monetise the video by running ads against it – potentially opting for sharing the revenue with the user that uploaded the material –; and to simply track the video's statistics.[80] This gives record companies the ability to automatically monetise a mashup video that uses even a fraction of one of their owned material, or simply block that content.

In fact, much like in the case of the notice and takedown procedure implemented by YouTube, the biggest problem with the Content ID system is that it does not require the consideration of fair use provisions by copyright holders submitting a claim[81]. Even though the system allows for a Content ID claim dispute, the rights holder may disagree with the uploader's reasoning and request the removal of their video– which means that the potentially "fair" user will end up receiving a copyright strike. Recently, YouTube changed its Content ID policy in order to assuage at least part of these concerns. The main innovation is it will hold advertisement revenues associated with any video in a Content ID dispute, to then disburse the funds to the winning party only once the claim is resolved.[82] However, this is far from solving the problem of overbroad takedowns documented by Urban, Karagnis, Schoefield (2017).

---

79 See Kevin J. Delaney, 'YouTube to Test Software To Ease Licensing Fights', *Wall Street Journal* (12 June 2007) <https://www.wsj.com/articles/SB118161295626932114> [accessed 31 October 2017].

80 See Youtube's'How Content ID Works' <https://support.google.com/youtube/answer/2797370?hl=en&ref_topic=2778544> [accessed 31 October 2017].

81 Note that this is in direct conflict with the Ninth Circuit's ruling in *Lenz v Universal*, which held that §512(c)(3)(A) (v) requires the consideration of fair use before the issuing of takedown requests. See *Lenz v. Universal Music Corp.*, 801 F.3d 1126 (2015).

82 See Goodmann (2016).

Systems like Content ID and copyright strikes are implementations of a private right-management regime embodying a "DMCA-plus" approach – i.e., voluntary, above-and-beyond enforcement measures that are undertaken by intermediaries whose compliance obligations are defined by DMCA safe harbours clauses[83]. Such regimes should not be valid outside of the US but are privately implemented by globally accessible digital platforms. This observation serves to relativise the idea that YouTube is a "global" platform, for in fact its private regulation is based on a very specific American law. Indeed, YouTube's private regulation rarely ensures respect of exceptions and limitations recognized in international copyright regimes and implemented in legislation other than US law. As discussed, although YouTube provides the possibility of a dispute between users – allowing the user that had its content blocked to defend him or herself – the mode of resolution of the conflict and the continue availability of the disputed content are at the mercy of the copyright holder.[84] In the end, through its architecture and ToS, the platform takes a clear choice of reinforcing the imbalance of power between big copyright holders and those small independent creators who depend on YouTube to make and distribute their content.

2.4 Conclusions

The examples discussed above seem to corroborate our initial hypothesis, *i.e.* that the advent of the Internet environment has prompted parallel consolidation of power in the hands of private intermediaries, demonstrating an increasing tendency towards the privatisation of traditionally public functions. In some instances, this tendency is the result of a specific choice taken by policymakers or courts, obliging platforms to implement appropriate responses and mechanisms to avoid liability or to give force to a decision (as in the cases of injunctions against innocent third parties and the implementation of *Google Spain*). In another scenario, the choice to define specific rules or to utilise specific national frameworks globally is "voluntarily"

83 See Bridy (2015).

84 Francisco & Valente (2016).

made (with different degrees of regulatory influence) by the specific platform, as shown in the implementation of the code of conduct on hate speech and in YouTube's approach to copyright exceptions and limitations. These examples illustrate that the lack of adequate constraints to platform power generates collateral damages, such as insufficient commitment to fundamental rights protection and distortion of competition in the market.

Digital platforms have become essential to allow individuals fully enjoy many of their fundamental rights, such as the right to educate themselves, their right to privacy and their freedom of communication and of information. In this sense, in light of the fact that social interactions increasingly depend on digital platforms, it is simply unacceptable for States to throw their hands up and let platform define the content, scope and limitations of fundamental rights without adequate constraints. More specifically, States cannot escape liability for violations of such rights occurring as a result of platform rules created in response to the incentives set up by the legal framework[85], be it for insufficient safeguards or for lack of regulatory intervention. International human rights law is quite clear in this respect, affirming not only "the positive obligations on States Parties to ensure human rights [and protect] individuals against acts committed by private persons or entities"[86] but also that "the obligations of States to respect, protect and promote human rights include the oversight of private companies."[87]

There is a spectrum of responses that States can take to ensure appropriate protection of fundamental rights, ranging from "command and control" regulation to secondary liability regimes, co-regulation, and ultimately self-regulation: thus, the encouragement of platform responsibility through commitment and transparency mechanisms constitutes the least intrusive type of regulatory intervention. Choosing this end of the scale may be preferable in the absence of evident market failures, but can

85 Zingales (2014).

86 See UN Human Rights Committee (2004).

87 See CoE Recommendation CM/Rec (2014)6.

only be effective in conjunction with adequate State supervision designed to ensure the detection and remedy of such failures. Additionally, targeted efforts of promotion of a culture of human rights compliance in the corporate environment may be necessary to ensure that the impacts of platforms on individuals are taken into account at the level of management as well as by shareholders, highlighting the significance of monetary consequences of human rights violations, such as reputational losses and liability under domestically implemented human rights law.

This focus on platforms' self-awareness and acceptance of their own responsibility to respect human rights is in line with the increased recognition of corporations as responsible entities for the upholding of the values of International human rights law, and should imply at a minimum that platforms do not merely devise the most cost-efficient solutions to conflicts between users, but rather strive to ensure effective protection of fundamental rights. States should remain vigilant that this does not remain an aspiration of principle, ensuring that it be given concrete effect through platforms' policies and ToS.

2.5 Bibliography

Article 19 (2016). 'EU: European Commission's Code of Conduct for Countering Illegal Hate Speech Online and the Framework Decision' (Article 19, June 2016) <https://www.article19.org/data/files/medialibrary/38430/EU-Code-of-conduct-analysis-FINAL.pdf> [accessed 31 October 2017].

Article 29 Working Party, 'Guidelines on the implementation of the Court of Justice of the European Union Judgment on 'Google Spain and Inc v. Agencia Espanola de Proteccion de Datos (AEPD) and Mario Costeja Gonzales' C-131/12', 14/EN WP 225 (26 November 2014) <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf> [accessed 1 November 2017].

Belli L (2016). *De la gouvernance à la régulation de l'Interne*t. (Berger-Levrault, 2016).

Belli L, De Filippi P and Zingales N (eds.) (2015). 'Recommendations on terms of service & human rights. Outcome Document n°1; <https://tinyurl.com/toshr2015> [accessed 31 October 2017].

Belli L & Venturini J (2016). 'Private ordering and the rise of terms of service as cyber-regulation' (2016) 5 (4) Internet Policy Review.

Bridy A (2015). 'Copyright's Digital Deputies: DMCA-Plus Enforcement by Internet Intermediaries'. J A Rothchild (ed.), *Research Handbook on Electronic Commerce Law* (Edward Elgar, 2016).

Center for Technology and Society at Fundação Getulio Vargas (2016). 'Terms of Service and Human Rights: An Analysis of Platform Contracts' (Recavan Press, 2016) <http://tinyurl.com/toshr> [accessed 31 October 2017].

Chenou J M and Radu R (2017). 'The "Right to Be Forgotten": Negotiating Public and Private Ordering in the European Union' Business & Society.

Evans D and Schmalensee R (2016). *Matchmakers: The New Economics of Multisided Platforms*. (Harvard Business Review Press, 2016).

European Commission, 'Code of Conduct on countering illegal hate speech online: First results on implementation' (December 2016), Factsheet, <http://ec.europa.eu/information_society/newsroom/image/document/2016-50/factsheet-code-conduct-8_40573.pdf> [accessed 31 October 2017].

European Commission, 'Code of Conduct on countering illegal online hate speech 2nd monitoring', Press Release IP/17/1471 <http://europa.eu/rapid/press-release_MEMO-17-1472_en.htm> [accessed 31 October 2017].

European Commission, 'The European Commission and Member States consumer authorities ask social media companies to comply with EU consumer rules', Press Release IP/17/631 <http://europa.eu/rapid/press-release_IP-17-631_en.htm> [accessed 31 October 2017].

Francisco P and Valente M (2016). *Da Rádio ao Streaming: ECAD, Direito Autoral e Música no Brasil*. (Azougue, 2016).

Griffin A (2014). 'Microsoft's Bing and Yahoo search engines have started to fulfill the controversial requests', *The Independent* (London, 1 December 2014) <http://www.independent.co.uk/life-style/gadgets-and-tech/news/microsoft-and-yahoo-join-google-in-deleting-search-results-under-right-to-be-forgotten-ruling-9896100.html> [accessed 31 October 2017].

Goodmann D (2016). 'YouTube's Content ID Policy Change Now Saves Lost Monetization for Fair Use Videos' (*Washington Journal of Law, Technology and Law Blog*,, 1 December 2016) <https://wjlta.com/2016/12/01/youtubes-content-id-policy-change-now-saves-lost-monetization-for-fair-use-videos/> [accessed 31 October 2017].

Haber E (2016). 'Privatization of the Judiciary' (2016), 40 Seattle University Law Review 115.

Hall RB, and Biersteker TJ (Eds.) (2002). *The emergence of private authority in global governance*. (Cambridge University Press, 2002).

Horten M (2016). *Closing of the Net* (Polity Press, 2016).

Husovec M (2017). *Injunctions against Intermediaries in the European Union*. (Cambridge University Press, 2017).

Kelsen H (1967). *Pure Theory of Law. Translation from the Second German Edition by Max Knight*. (University of California Press, 1967).

Kim NS (2013). *Wrap Contracts: Foundations and Ramifications* (Oxford University Press, 2013).

OECD (2011). *The Role of Internet Intermediaries in Advancing Public Policy Objectives* (OECD Publishing, 2011). <http://dx.doi.org/10.1787/9789264115644-en> [accessed 31 October 2017].

McNamee J (2016). 'Guide to the Code of Conduct on Hate Speech' (*EDRi,*, June 2016) <https://edri.org/guide-code-conduct-hate-speech/> [accessed 31 October 2017].

Moazed A and Johnson N (2016). *Modern Monopolies: What it Takes to Dominate the 21st Century Economy* (St. Martin's Press, 2016).

Parker G, Alstyne M and Choudary S (2016). *Platform Revolution – How Networked Markets Are Transforming the Economy – and How to Make Them Work for You* (W. W. Norton & Company, 2016).

Radin M J (2012). *Boilerplate: The Fine Print, Vanishing Rights, and the Rule of Law* (Princeton University Press, 2012).

Rochet J C and Tirole J (2003). 'Platform Competition in Two-Sided Markets' (2003) 1 (4) Journal of the European Economic Association 990.

Schechner S (2014).'Google Starts Removing Search Results Under Europe's 'Right to be Forgotten'', *Wall Street Journal* (New York, 26 June 2014) <https://www.wsj.com/articles/google-starts-removing-search-results-under-europes-right-to-be-forgotten-1403774023> accessed 31 October 2017].

Strange S (1988). *States and markets* (Continuum, 1988).

UN Human Rights Committee (2004). General Comment 31/2004. Nature of the General Legal Obligation on States Parties to the Covenant. CCPR/C/21/Rev.1/Add.13. http://www.unhcr.org/4963237716.pdf

Urban JM, Karaganis J and Schofield BL (2017). 'Notice and Takedown in Everyday Practice' UC Berkeley Public Law Research Paper No. 2755628. <https://ssrn.com/abstract=2755628> [accessed 31 October 2017].

Weber M (1919). 'Politics as a Vocation'. in H H Gerth and C Wright Mills (eds.) *From Max Weber: Essays in Sociology* (Routledge & Kegan Paul, 1948).

Zingales N (2014). 'Virtues and perils of anonymity: should intermediaries bear the burden? '(2014)' 5 (3) Journal of Intellectual Property, Information Technology and E-commerce 155.

Zingales N and Janczuck A (2017). 'Implementing the Right To Be Forgotten: towards a co-regulatory solution?' e-conférence on the Right to Be Forgotten in Europe and Beyond, May 2017, Blogdroiteuropeen. <http://wp.me/p6OBGR-22t.> [accessed 31 October 2017].

3 Online Platform Responsibility and Human Rights

Emily B. Laidlaw

Abstract

This paper explores the human rights responsibilities of online platforms at the intersection of three areas: human rights, corporate social responsibility (CSR) and regulation (more broadly law). It seeks to untangle the governance problems in framing platform responsibility, focusing in particular on the uneasy relationship between CSR and law, and identifying the difficulties in articulating what it means for a platform to respect human rights. It concludes by examining the future of platform governance, identifying three key challenges in the areas of intermediary liability, the scope of the duty of respect, and the lens through which dispute resolution mechanism should be interrogated.

3.1 Introduction

Online platforms operate in a precarious space for the purpose of Internet governance. They have tremendous power as gatekeepers to control the flow of information online. Given the transnational, instantaneous nature of Internet communications, these platforms also have great capacity to regulate in a situation where a state's powers are more limited. Indeed, platforms are crowd leaders[88], and pressured by governments, both directly and indirectly, and by society to leverage their power and leadership to regulate their services.

At the centre of their gatekeeping function are human rights, in particular the rights to free expression and privacy, and the question is the responsibilities of companies for human rights standards. Conceptualizing this responsibility is problematic for a human rights system which has historically treated human rights as a government responsibility. This is compounded when the goal is to move beyond aspirational guidance to concrete

88 Citron (2010:4).

recommendations on how to embed such responsibilities into a company's governance structure.

When a platform deletes user content because it infringes the Terms of Service, how is this to be framed? Do users have a right to freedom of expression on a private platform, or does the company have a corresponding duty to respect user rights? Should platforms match the approach of governments in delineating limits to these rights, or should it carve out stricter rules on the basis of social responsibility? The law is a blunt tool that is often reserved for the most extreme cases, especially in the area of freedom of expression and privacy.

Thus, under the banner of corporate social responsibility (CSR) platforms are often expected to draw a harder line than what might be legally required. This creates unease because as our exercise of free speech and experiences of privacy are increasingly channelled through online platforms, their regulation of such rights become default human rights laws. State systems of human rights are all well and good, but the day-to-day experience of our digital lives is through the laws of Facebook, Twitter, Snapchat and so on[89], which often more narrowly frame acceptable online behaviour. Should this phenomenon be characterised as platforms living up to their social responsibilities or privatization of human rights?

The issues of responsibilities and rights are compounded by the sheer volume of content these platforms manage. Consider that every minute 400 hours of content are uploaded to YouTube[90] and 1.3 million posts are shared on Facebook[91]. In terms of content complaints, YouTube receives 200,000 flags per day[92] and Facebook receives two million requests for content removal per week[93]. As a result, complaints mechanisms are increasingly automated, raising questions about whether these processes can satisfy the rule of law.

89 Laidlaw (2015); Laidlaw (2017).

90 Daphne Keller, 'Making Google the Censor' *The New York Times* (New York, 12 June 2017). <https://www.nytimes.com/2017/06/12/opinion/making-google-the-censor.html?smid=tw-share&_r=0> [accessed 1 November 2017].

91 Hopkins (2017).

92 United Kingdom Parliament, 'Oral Evidence: Hate Crimes and its Violent Consequences' (2017), Q 409 and Q 411.

93 Rosen (2013).

I suggest that conceptions of governance as it relates to online platforms is at a critical juncture, where major social issues such as fake news, online abuse, and data gathering and sharing, to name a few, often occur in the grey area between the law and CSR. This paper explores governance at the intersection of three fields of study: human rights, regulation (more broadly law) and CSR. While these issues are examined in more detail in this author's earlier work[94], here I wish to canvass the main issues to then identify for readers emerging issues for the future of online platforms and governance. In using the term CSR in this paper, I am describing the umbrella term for the relationship between business and society[95].

3.2 CSR and the Law

A key conceptual problem in analysing the role of online platforms is the relationship between CSR and the law. When an online platform regulates its service, is this purely voluntary, or is there a legal aspect to what it voluntarily undertakes[96]? This is important, because if an online platform commits to a system of responsibility, there is a risk it will be legally responsible for what it might have initially envisioned as an act of corporate citizenship, good business sense or management of its product or services[97].

In conceiving of CSR broadly as the relationship between business and society, it is observable at four levels of governance: international, state, industry and company. International frameworks, such as the United Nations Global Compact[98] or the *OECD Guidelines for Multinational Enterprises99* are more formalized frameworks largely serving a normative function. State level frameworks, such as *a renewed EU Strategy 2011-14 for Corporate Social Responsibility100*, advocate for corporate-

94 See in particular Laidlaw (2015).

95 Laidlaw (2015:67).

96 See Webb (2004).

97 See for example *Choc v Hudbay Minerals Inc*, 2013 ONSC 1414 (Ontario Superior Court).

98 United Nations Global Compact. <https://www.unglobalcompact.org> [accessed 1 November 2017].

99 OECD (2011).

100 Communication from the Commission to the European Parliament, The Council, The European Economic and Social Committee of the Regions, 'A renewed EU strategy 2011-14 for Corporate Social Responsibility' (25 October 2011), COM(2011) 681 final.

led responsibility underpinned by government activity, such as creating an environment, perhaps through legislation, that supports companies in meeting their social responsibilities. Such an approach is evident in the European Commission ICT Sector Guidance[101] on the responsibilities of ICT businesses for human rights.

Industry level initiatives are often more regulatory, as at this level there is capacity to create enforcement powers. A mixed approach is evident with the Global Network Initiative, which among other things, provides a framework to guide companies using international standards, and accountability through periodic independent audits[102]. As Dorothee Baumann-Pauly *et al.* argue, industry level initiatives are advantageous compared to broader efforts, because they can more easily walk the line between voluntary and mandatory frameworks, and industry is well-positioned to create and maintain standards[103]. Company-level CSR is where all roads lead, where companies determine their social responsibility in light of the social, political and legal context.

While CSR is framed as social responsibility above and beyond the law, the tendency is to now focus on ways that this responsibility can be facilitated through regulation, such as reporting requirements in, for example, a company's annual reports. See, by way of example, the *Occupational Pension Schemes (Investment, and Assignment, Forfeiture, Bankruptcy etc.) Amendments Regulation*, 1999; and the reporting of supply chain management concerning trafficking and slavery in the *California Transparency in Supply Chains Act* and *Modern Slavery Act*). This is described in regulatory literature as meta-regulation[104]. To put it another way, "how is it possible for the *law* to make companies accountable for going *beyond the law*?"[105] Based on the above, CSR begins to look less voluntary and more like a collaborator in a system of governance. Peter Utting describes

101 European Commission 'ICT Sector Guidance on Implementing the UN Guiding Principles on Business and Human Rights'. https://ec.europa.eu/anti-trafficking/sites/antitrafficking/files/information_and_communication_technology_0.pdf.

102 See <https://www.globalnetworkinitiative.org/> [accessed 1 November 2017].

103 Baumann-Pauly (2015:11-13).

104 Parker (2007:210).

105 Parker (2007:207).

such hardening as "ratcheting-up of voluntary initiatives"[106], where increasingly it is about accountability characterise ed by codes of conduct, monitoring schemes and so on.

Given the grey area in which many issues of human rights are decided and the uncertainty this creates for both platforms and users, discussions of Internet regulation should be broadened to better account for the role of CSR. CSR is outward-looking and aligns with the role of human rights in mobilizing and responding to social change. Regulation, in contrast, is more targeted and instrumental. Certainly, CSR can be deployed through regulation, such as self or industry regulation, and in my view, this is CSR operating at its best. However, unlike regulation its core function is effecting social responsibility although tolerating various approaches and uncertain outcomes.

However, there are significant disadvantages to CSR. Namely, these kinds of corporate regulation aren't great for standard setting. For example, the dispute resolution mechanisms of platforms vary wildly. They can range from innovative, to existing but lacking in transparency or sophistication, to non-existent. An innovative example is Wikipedia's developed ODR system, which provides users with a range of scalable options, from information to formalized mediation and arbitration[107].

The lack of standard setting means that principles of good regulation that one normally expects of public institutions aren't normally present. Such principles include that regulations are transparent, accountable, proportionate, consistent, and accessible[108]. Indeed, Ranking Digital Rights, a project led by Rebecca McKinnon, published a Corporate Accountability Index of 16 Internet companies, including Facebook and Twitter. Among other things, it found that, concerning private requests for content removal, the major intermediaries provided minimal information:

> Disclosure about private and self-regulatory processes is minimal and ambiguous at best, and

106 Utting (2005:6).

107 Katsh & Rabinovich-Einy (2017:122-125).

108 Laidlaw (2015:258).

> often non-existent. Few companies disclose data about private third-party requests to remove or restrict content or to share user information – even when those requests come with a court order or subpoena, or are made in accordance with established legal processes such as a copyright "notice-and-takedown" system. Even fewer companies disclose any information about whether – let alone how – they receive or respond to private or informal requests. Further, **no companies in the Index disclose any information about actions they have taken to enforce their terms of service**. [emphasis added][109].

This lack of transparency is concerning, because of the pseudo-judicial role these platforms undertake. At a more fundamental level, the voluntary nature of these types of CSR frameworks, set down through contractual arrangements with users, is problematic. In earlier work, I summarized some of the issues in a wider human rights context:

> Pure-CSR codes simply lack the standard-setting appeal and oversight necessary to the structure of a free speech system. Such codes are too reliant on the whims or commitments of management; they are thus susceptible to change over time and unreliable as a public signal of the expectations of company conduct. A change in management, for example, can lead to a change in the business's human rights policies or, more insidiously, lead to no change in policy, but a change in the seriousness with which human rights matters are treated. The work of the Private Sector and Human Rights Project found that the commitment of particular leaders in a company was the 'dominant driver for engaging with human rights'. The finding was particularly the case for companies that operated outside the public sector and industry regulation, which would be the case for

109 Ranking Digital Rights (2015:6).

> most macro-[Internet information gatekeepers] such as ISPs and search engines. The problem inherent in this situation is exacerbated by the fact that IT companies, in terms of their democratic impact, are changeable, and the Internet environment is unstable. This leaves the public hopelessly confused and offers none of the characteristics of due process needed to be a governance framework. Most important, it makes it more difficult to establish and sustain human rights standards[110].

The narrower question about CSR is how it can be used to complement other efforts to achieve a desired objective? In order to better understand the role of online platforms and human rights, the United Nations Guiding Principles (GP) are explored.

3.3 The Guiding Principles

The Guiding Principles have played a key role in transforming the debate about business and human rights[111]. They are the global reference point on the responsibilities of businesses for human rights[112], having been endorsed by the Human Rights Council[113], and influencing multiple global standards (such as the OECD Guidelines and ISO 2600 Guidance on social responsibility). The Guiding Principles are not universally embraced, and efforts continue for a legally binding treaty[114].

The Guiding Principles comprise three pillars: (1) a state's duty is to protect human rights, which reflects traditional state legal obligations for human rights; (2) a business's duty is to respect human rights, rooted in social expectation and systems of due diligence; and (3) a right of aggrieved to a remedial mechanism to make a complaint and have it resolved[115]. This chapter does not

110 Laidlaw (2015:246-247).

111 Ruggie (2011).

112 Ruggie (2013:101-102).

113 Human Rights Council (2011). 'Human Rights and transnational corporations and other business enterprises'. A/HRC/RES/17/4.

114 See University of Notre Dame London Gateway (2017).

115 Ruggie (2011).

discuss in detail the interpretation of each element of the Guiding Principles, but rather focuses on key issues in relation to online platforms, namely related the second and third pillars.

In some ways, the duty to respect helps articulate what the baseline is for corporate responsibility for human rights. It bridges the gap between proponents of direct duties under human rights laws and voluntariness, and has a weight of authority that is missing from the pure-CSR focus. The duty to respect is based on social expectation, focusing on accountability mechanisms rather than legal duties. This accountability is effected through a system of due diligence, namely assessing, monitoring and acting on their human rights impact, and communicating with the public. A typical form of due diligence would be audits[116].

Criticisms of the duty to respect resonate for online platforms, and parallel some of the criticisms of CSR. Namely, 'social expectation' is arguably too weak for human rights duties, not providing effective guidance for companies[117], especially because soft laws are most effective as complements to hard laws[118]. It is also difficult to move from blanket commitments to concrete guidance in a way that is instructive to companies. This can be seen concerning the scope of the duty to respect. Many online platforms narrowly view the duty to respect as related to government interferences with user rights[119]. This explains the narrow focus of the Global Network Initiative and the lack of transparency concerning enforcement of Terms of Service. While industry initiatives like the GNI are potentially an effective way to implement the duty to respect[120], the problem of the scope of the duty endures.

The third pillar requiring access to a forum of remediation envisions three types: judicial (traditional courts), state-based non-judicial (such as National Human Rights Institutions) and non-state-based (such as the kinds of industry or company-

116 Ruggie (2011).

117 Bilchitz (2013).

118 Nolan (2013).

119 See interviews in Jørgensen (2017).

120 Baumann-Pauly (2015: 3-4).

level mechanisms explored in this paper)[121]. Non-state-based mechanisms are particularly relevant for online platforms. Most major platforms have a remedial mechanism. Some frameworks are highly innovative, such as eBay and Wikipedia's online dispute resolution systems. Riot Games, for example, in response to online abuse on League of Legends, assembled a 'player behavior team' to study user profiles, comprised of psychology, cognitive science and neuroscience professionals, and revised their approach to responding to complaints based on their findings[122]. Social networking platforms are trialing innovative approaches to resolution, with mixed success, such as Facebook's "compassion team" to innovate resolution of interpersonal disputes and its use of social reporting[123], or Twitter's mute, block and report strategy[124].

However innovative these approaches are, it is unclear what qualifies as a legitimate non-state-mechanism under the Guiding Principles. To put it another way: when is a company deemed successful under the third pillar? Seven criteria are articulated, namely that a mechanism is legitimate, accessible, predictable, equitable, transparent, rights-compatible and a source of continuous learning[125]. Some online dispute resolution systems reflect these principles, but most social networking platforms do not. Thus, for interpersonal disputes does Facebook's report abuse button or Twitter's block feature qualify as a legitimate non-state-based process? To satisfy the third pillar does the process need to replicate due process requirements such as a right to make a case and hear the case against you?

What is evident is that remedial mechanisms deployed through the platforms provides an opportunity for innovation as they are tied to the communities involved. However, they succumb to many of the issues identified concerning CSR, and a question pursuant to the Guiding Principles is whether a state's duties require it to provide or enable such forums of remediation. As Katsh and

121 Ruggie (2011), paras. 25-30.

122 Katsh & Rabinovich-Einy (2017:129-130).

123 Katsh & Rabinovich-Einy (2017:113).

124 Twitter Help Centre. Learn How to Control Your Twitter Experience. Retrieved from <https://support.twitter.com/articles/20170134> [accessed 1 November 2017].

125 Ruggie (2011), para. 31.

Rabinovich-Einy remind, "[o]ne of the oldest maxims of law is that "there is no right without a remedy"[126]. States are beginning to address access to justice hurdles to resolving online disputes. For example, Europe's Directive on alternative dispute resolution (ADR)[127] creates an online dispute resolution platform to enable users to connect with a private ADR provider to resolve low-value e-commerce disputes[128]. One can imagine a similar service for content-related disputes that raise issues of freedom of expression and privacy[129]. Arguably a state enabling these alternative forums of remediation might fulfil its duty to enable access to a forum of remediation, even if the providers are privately run.

3.4 Areas for future research

In earlier work, I advocated that the duty to protect human rights is that of the state, and outsourcing human rights through encouragement of corporate governance without more fails to fulfil that duty[130]. However, direct legal obligations are not effective to address some of the issues that arise online, and what is needed is bridging of human rights and regulatory traditions. In short, the goal should be to approach governance of human rights as a system and seek to build complementarity and synergy between various systems of regulation[131].

My solution, while not explored in detail here, is what I termed the "Internet Rights Governance Model"[132], offered as a blueprint for company-level assessment of responsibilities and a model for state-based non-judicial and non-state-based bodies. The complementarity focuses on a common policy framework and complementary dispute resolution mechanisms:

126 Katsh & Rabinovich-Einy (2017:15).

127 Directive 2013/11/EU on alternative dispute resolution for consumer disputes and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC. OJ L 165 (18.6.2013), p. 63–79.

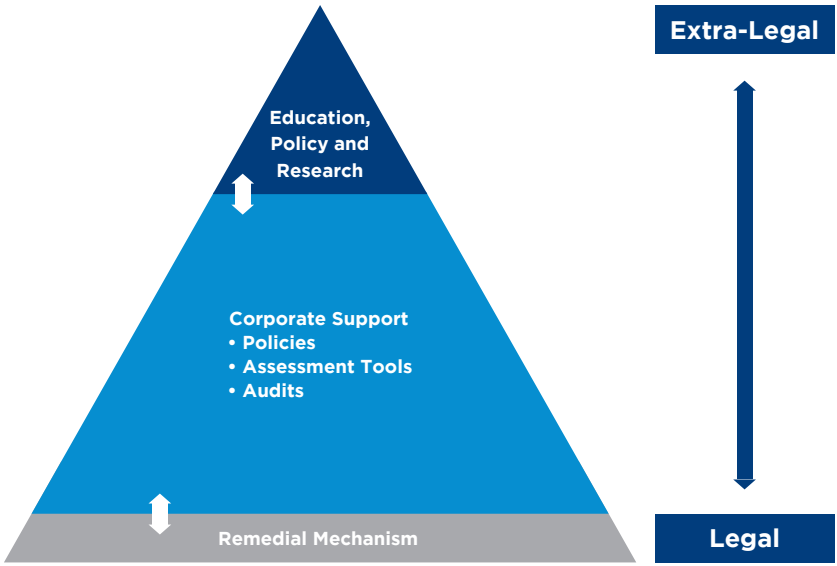
128 See the ODR Platform at. <https://ec.europa.eu/consumers/odr/main/index.cfm?event=main.home.show&lng=EN> [accessed 1 November 2017].

129 In a defamation context, see Laidlaw (2017).

130 Laidlaw (2015), chapter 6.

131 Laidlaw (2015: 233-234); Utting (2005).

132 Laidlaw (2015:259).



Source: *Laidlaw (2015:259)*

What I want to tease out here is that the solutions to the human rights problems we face online, and the role of platform providers, is often less about "old school" strategies of command and control regulation, and more about systems of governance, which involve both legal and non-legal elements.

Moving forward I see three challenges requiring further research. First, the scope of the duty to respect needs to be untangled in the context of online platforms. Specifically, does the duty to respect require respect for all interferences for human rights, including by private parties? While I have advocated that to be the case in earlier work, there is a disconnect between my views and the approach of companies that should be further explored[133]. For example, if a Facebook "friend" posts content that reveals intimate, embarrassing information about me, does Facebook have a duty to respect my privacy (as a separate duty to any arising from the Terms and Conditions)? Or, is Facebook's duty restricted to a government interference with my right to privacy?

133 See Jørgensen (2017).

While the duty to respect is grounded in social expectation, clarification as to its scope would guide platforms on how to design their spaces to manage content problems, although admittedly those platforms that would heed such guidance likely are already influenced by human rights principles. Rogue platforms would likely be unaffected by such guidance. Where the clarification is powerful is in bringing home the duty to provide access to a remedial mechanism. Most platform mechanisms to resolve disputes resemble little the legitimate non-state-based models envisioned in the Guiding Principles.

Second, we need to continue to examine the baseline of intermediary liability. Is harmonization possible? A significant amount of research has been undertaken on this issue revealing starkly different visions for intermediary liability models. Two influential human rights-based models are *Marco Civil da Internet*[134] and the *Manila Principles on Intermediary Liability*[135]. The *Manila Principles* draws significantly from the Guiding Principles to create "baseline safeguards and best practices"[136].

At the same time, there are calls for greater platforms responsibility to remove illegal content, in particular content that is harmful to children, terrorism or copyright infringing. Organisations such as the National Society for the Prevention of Cruelty to Children argue for greater responsibility on intermediaries to proactively remove illegal content[137]. Similar calls have been made by the United Kingdom and French governments to combat online radicalization, advocating fines against technology companies that fail to remove extremist content[138].

At an international level, the Human Rights Council stated that restrictions on access to online content must comply with the right to freedom of expression under Article 19 of the Universal

134 Marco Civil da Internet. English translation retrieved from <http://sflc.in/wp-content/uploads/2014/05/APPROVED-MARCO-CIVIL-MAY-2014.pdf> [accessed 1 November 2017].

135 Manila Principles, supra n. 16.

136 *Ibid.*, introduction.

137 Fossi (2015).

138 Elgot (2017).

Declaration of Human Rights[139]. The four special rapporteurs, in a joint declaration on freedom of expression and the Internet, expressed concern with imposing liability on intermediaries:

> Intermediary Liability
>
> **1** No one who simply provides technical Internet services such as providing access, or searching for, or transmission or caching of information, should be liable for content generated by others, which is disseminated using those services, as long as they do not specifically intervene in that content or refuse to obey a court order to remove that content, where they have the capacity to do so ('mere conduit principle').
>
> **2** Consideration should be given to insulating fully other intermediaries, including those mentioned in the preamble, from liability for content generated by others under the same conditions as in paragraph 2(a). At a minimum, intermediaries should not be required to monitor user-generated content and should not be subject to extrajudicial content takedown rules which fail to provide sufficient protection for freedom of expression (which is the case with many of the 'notice and takedown' rules currently being applied). (United Nations Special Rapporteur, para. 2).

The former (Frank La Rue) and current (David Kaye) United Nations special rapporteur on the promotion and protection of the right to freedom of opinion and expression, published reports cautioning against excessing intermediary liability[140].

In the area of reform of defamation law, with my co-author Hilary Young, we recommended to the Law Commission of Ontario a notice-and-notice-plus system[141] modelled on three principles: the

139 Human Right Council (2011). 'General Comment No. 34. Article 19: Freedoms of opinion and expression'. CCPR/C/GC/34, para. 43.

140 La Rue (2011); Kaye (2016).

141 Laidlaw and Young (2017:93-107).

rules should be human-rights based; should enable innovation; and should serve to encourage corporate social responsibility. Our conclusion is that intermediaries should not be held liable as publishers for third party content, but should remove defamatory content in narrow circumstances (if a user disputes the allegations, the intermediary is not required to remove the content). The risk to the intermediary for failure to comply with the procedures would not be liability for the underlying defamatory content, but rather a risk of a fine, similar to Canada's notice-and-notice system in copyright law[142].

Third, what makes a good dispute resolution system under the Guiding Principles third pillar requires a significant amount of research. There is a need here to synergize different areas of law and policy. While I have examined it through the lens of human rights, regulation and CSR, another angle I suggest would add value: the potential intersection of ADR, legal innovation and human rights.

A significant body of scholarly work and practical output is evident in the field of legal innovation and ADR[143]. The future of law is at a time of transformation, and the systems of resolving disputes are being innovated in response. Resolving disputes is no longer contained to simple dispute resolution, but is broadened to include avoidance and containment of the dispute[144]. As discussed, the European Union identified issues in high-volume, low-value disputes in the e-commerce sector, prompting the ADR Directive[145]. The time has come for similar attention to content-related disputes and online platforms. The United Kingdom is developing an Online Court, and British Columbia is operating an online tribunal (Civil Resolution Tribunal) for small claims and condominium disputes. Currently, most research is in silos with access to justice and innovation informing dispute resolution,

142 Copyright Act, RSC 1985, c C-42., ss. 41.25-41.27

143 See Hörnle (2009); Susskind (2017) (among his other books); Thompson (2014); Wang (2009).

144 Online Dispute Resolution Advisory Group (2015). 'Online Dispute Resolution for Low Value Civil Claims'. *Civil Justice Council* (February 2015) <https://www.judiciary.gov.uk/wp-content/uploads/2015/02/Online-Dispute-Resolution-Final-Web-Version1.pdf> [accessed 1 November 2017].

145 Directive 2013/11/EU on alternative dispute resolution for consumer disputes and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC,. OJ [2013] L 165, p. 63–79.

and human rights informing international governance. I suggest more finely connecting ADR and innovation with human rights will provide key guidance to governance of online platforms.

3.5 Conclusion

This paper sought to canvass the big picture challenges in platform responsibility by unpacking the tension between CSR, regulation and human rights. Platforms operate in a precarious space having both great power and responsibility over the flow of information online. This paper sought to broaden understanding of governance of such platforms, focusing on ways to build synergy between various systems of regulation, including CSR. Through this exercise, three emerging challenges for the future of platform governance were identified. First, is the need to untangle the scope of the duty to respect under the second pillar of the Guiding Principles, namely whether it extends or should extend to private interferences with rights. Second, is the enduring question of potential harmonization of intermediary liability frameworks. While largely out of reach, this paper suggests shifting the focus to building complementarity between governance strategies. Third, is the question of what makes a good remedial mechanism under the third pillar of the Guiding Principles. There is great potential to draw from the body of work in legal innovation and ADR to inform Internet governance and human rights strategies.

3.6 Bibliography

Baumann-Pauly D et al (2015). 'Industry-Specific Multi-Stakeholder Initiatives that Govern Corporate Human Rights Standards – Legitimacy Assessments of the Fair Labour Association and the Global Network Initiative' (2015) 143 (4) Journal of Business Ethics 771.

Bilchitz, D (2013). 'A Chasm between "Is" and "Ought"? A Critique of the Normative Foundations of the SRSG's Framework and Guiding Principles'. In S Deva and D Bilchitz (Eds.), *Human Rights Obligations of Business: Beyond the Corporate Responsibility to Respect* (Cambridge University Press, 2013).

Citron D K (2010). 'Civil Rights in Our Information Age'. In S Levmore and MC Nussbaum (Eds.), *The Offensive Internet* (Harvard University Press, 2010).

Elgot J (2017). 'May and Macron plan joint crackdown on online terror', *The Guardian* (London, 12 June 2017) <https://www.theguardian.com/politics/2017/jun/12/may-macron-online-terror-radicalisation> [accessed 1 November 2017].

European Commission (2013). 'ICT Sector Guidance on Implementing the UN Guiding Principles on Business and Human Rights'. <https://ec.europa.eu/anti-trafficking/sites/antitrafficking/files/information_and_communication_technology_0.pdf> [accessed 1 November 2017].

Fossi J (2015). 'Are social networking sites doing enough to keep children safe. London School of Economics blog Parenting for a Digital Future', (*LSE Parenting for a Digital Future blog*, 10 June 2015). <http://blogs.lse.ac.uk/parenting4digitalfuture/2015/06/10/are-social-networking-sites-doing-enough-to-keep-children-safe/> [accessed 1 November 2017].

Hopkins N (2017). 'Revealed: Facebook's internal rulebook on sex, terrorism and violence',*The Guardian* (London, 21 May 2017). <https://www.theguardian.com/news/2017/may/21/revealed-facebook-internal-rulebook-sex-terrorism-violence> [accessed 1 November 2017].

Hörnle J (2009). *Cross-border Internet Dispute Resolution* (Cambridge University Press, 2009).

Human Rights Council (2011). 'Human Rights and transnational corporations and other business enterprises'. A/HRC/RES/17/4.

Human Right Council (2011). 'General Comment No. 34. Article 19: Freedoms of opinion and expression'. CCPR/C/GC/34.

Human Rights Council (2014). 'Elaboration of an international legally binding instrument on transnational corporations and other business enterprises with respect to human rights'. A/HRC/26/L.22.

ISO 26000. 'Guidance on Social Responsibility' <https://www.iso.org/standard/42546.html> [accessed 1 November 2017].

Jørgensen R (2017). 'Framing human rights: exploring storytelling within Internet companies' (2017) Information, Communication & Society, 1-16.

Katsh E & Rabinovich-Einy O (2017). *Digital Justice: Technology and the Internet of Disputes* (Oxford University Press, 2017).

Kaye D (2016). 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression'. A/HRC/32/38.

Keller D (2017). 'Making Google the Censor' *The New York Times* (New York, 12 June 2017). <https://www.nytimes.com/2017/06/12/opinion/making-google-the-censor.html?smid=tw-share&_r=0> [accessed 1 November 2017].

Laidlaw E (2017). 'Are we asking too much from defamation law? Reputation systems, ADR, Industry Regulation and other Extra-Judicial Possibilities for Protecting Reputation in the Internet Age: Proposal for Reform', Law Commission of Ontario (July 2017). <http://www.lco-cdo.org/wp-content/uploads/2017/07/DIA-Commissioned-Paper-Laidlaw.pdf> [accessed 1 November 2017].

Laidlaw E & Young H (2017). 'Internet Intermediary Liability in Defamation: Proposals for Statutory Reform'. Law Commission of Ontario (July 2017). <http://www.lco-cdo.org/wp-content/uploads/2017/07/DIA-Commissioned-Paper-Laidlaw-and-Young.pdf> [accessed 1 November 2017].

Laidlaw E (2017). 'What is a joke? Mapping the path of a speech complaint on social networks'. In D. Mangan and L.E. Gillies (Eds.), *The Legal Challenges of Social Media* (Edward Elgar, 2017).

Laidlaw E (2015). *Regulating Speech in Cyberspace: Gatekeepers, Human Rights and Corporate Responsibility* (Cambridge University Press, 2015).

La Rue F (2011). 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression'. A/HRC/17/27.

Nolan J (2013). 'The Corporate Responsibility to Respect Human Rights: Soft Law or Not Law?' In S Deva and D Bilchitz (Eds.), *Human Rights Obligations of Business: Beyond the Corporate Responsibility to Respect* (Cambridge University Press, 2013).

Organization for Economic Cooperation and Development (2011) *OECD Guidelines for Multinational Enterprises*. <http://www.oecd.org/daf/inv/mne/48004323.pdf> [accessed 1 November 2017].

Parker C (2007). Meta-Regulation: Legal Accountability for Corporate Social Responsibility. In D. McBarnet et al (Eds.), *The New Corporate Accountability: Corporate Social Responsibility and the Law* (Cambridge University Press, 2017).

Ranking Digital Rights (2015). '2015 Corporate Accountability Index' <https://rankingdigitalrights.org/index2015/assets/static/download/RDR-4pager.pdf> [1 November 2017].

Rosen J (2013). The Delete Squad. The New Republic. Retrieved from www.newrepublic.com/article/113045/free-speech-internet-silicon-valley-making-rules.

Ruggie J (2011). 'Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework'. A/HRC/17/31. <https://business-humanrights.org/sites/default/files/media/documents/ruggie/ruggie-guiding-principles-21-mar-2011.pdf> [accessed 1 November 2017].

Ruggie J (2013). *Just Business: Multinational Corporations and Human Rights* (W.W. Norton & Company, 2013).

Susskind R. (2017). *Tomorrow's Lawyers: An Introduction to Your Future* (Oxford University Press, 2017).

United Kingdom Parliament, House of Commons, Home Affairs Committee. (2017). Oral Evidence: Hate Crime and its Violent Consequences (Chair: Yvette Cooper).

United Nations Global Compact. <https://www.unglobalcompact.org> [accessed 1 November 2017].

University of Notre Dame London Gateway (2017). 'Expert Round Table on Elements of a Possible Binding International Instrument on Business and Human Rights', Summary Report (11 July 2017) <https://business-humanrights.org/sites/default/files/documents/May%2016%202017%20rtable%20sum%20rep%20final.pdf> [accessed 1 November 2017].

The United Nations Special Rapporteur on Freedom of Opinion and Expression, et al. (2017). 'Joint Declaration on Freedom of Expression and the Internet'. <https://www.article19.org/data/files/pdfs/press/international-mechanisms-for-promoting-freedom-of-expression.pdf> [accessed 1 November 2017].

Thompson D (2014). 'The Growth of Online Dispute Resolution and Its Use in British Columbia'. Continuing Legal Education Society of British Columbia, March 2014 <http://www.cle.bc.ca/practicepoints/LIT/14-GrowthODR.pdf> [accessed 1 November 2017].

Utting P (2005). 'Rethinking business regulation: from self-regulation to social control'. Technology, Business and Society Programme Paper Number 15, United Nations Research Institute for Social Development (2005).

Wang F (2009). *Online Dispute Resolution: Technology, Management and Legal Practice from an International Perspective*. (Chandos, 2009).

Webb K (2004) (Eds.), *Voluntary Codes: Private Governance, the Public Interest and Innovation* (Carleton Research Unit for Innovation, Science and the Environment, 2004).

4 Regulation *by* Platforms: the Impact on Fundamental Rights

Orla Lynskey

Abstract

Increasing regulatory and doctrinal attention is focused on the problem of 'platform power'. Digital platforms often exercise this power in conjunction with States, for instance in the field of security and law enforcement, and this power is regulated by States through legal instruments such as competition law and rules governing intermediary liability. However, in addition to this regulation of private online platforms, this paper suggests that we are also regulated by private platforms and that this 'private ordering', facilitated by technological code, has implications for economic, social, cultural and political dimensions of our lives. In particular, this paper argues that platforms influence the extent to which we can exercise our rights and the effectiveness of those rights both directly and indirectly. Furthermore, it suggests that these implications are exacerbated when the platform concerned is in a position of power, for instance because of the number of individuals that use the platform. This paper shall illustrate this point by reference to two examples, and will then briefly identify some of the options open to policy-makers to tackle these issues, and the challenges they may face in so doing.

4.1 Introduction

When John Perry Barlow penned the 'Declaration of the Independence of Cyberspace'[146] it was governments, 'weary giants of flesh and steel', rather than private actors that threatened to jeopardise emerging governance structures in 'cyberspace'. Twenty years later, the State increasingly operates in tandem with online private actors in security and law enforcement, in the provision of public goods and even to adjudicate what is in the 'public interest'.[147] Digital platforms are key players in this picture. While

146 Barlow (1996).

147 This follows from the ECJ ruling in Case C-131/12 *Google Spain SL v AEPD* (EU:C:2014:317). See further, Powles (2017).

what constitutes a 'digital platform' is contested, a digital platform is defined here as an 'undertaking operating in two (or multi)-sided markets, which uses the Internet to enable interactions between two or more distinct but interdependent groups of users so as to generate value for at least one of the groups'.[148] Digital platform is therefore a broad category encompassing familiar services such as content-sharing site YouTube, micro-blogging service Twitter, shopping site Amazon, and general and specialized search services, such as Google Search and Skyscanner, amongst many other others.

What is critical about a platform for the purpose of this paper is that it acts as a type of digital middleman, intermediating the activities of individuals in the digital sphere. Private platforms are already subject to various forms of regulation: for instance, they are beneficiaries of private law rights, and subject to private law liabilities.[149] They also benefit from a presumption of neutrality, which exempts them from liability, when they or 'cache' or 'host' content originating from third parties.[150] Thus, for instance, a platform like Facebook will not be held liable for defamatory content originating from third parties if it can demonstrate that it did not have actual or constructive knowledge that the content it was hosting was defamatory, and that it acted expeditiously to remove the content upon becoming aware of its existence.[151]

However, in addition to this regulation *of* private online platforms, this paper suggests that we are also regulated *by* private platforms and that this 'private ordering'[152], facilitated by technological code, has implications for economic, social, cultural and political dimensions of our lives.[153]

148 European Commission, 'Public Consultation on the regulatory environment for platforms, online intermediaries, data and cloud computing and the collaborative economy' (September 2015): 5. <https://ec.europa.eu/digital-agenda/en/news/public-consultation-regulatory-environment-platforms-onlineintermediaries-data-and-cloud> [accessed 1 November 2017].

149 Lemley (2006); Hartzog (2011).

150 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (E-Commerce Directive) [2000] OJ L178/1.

151 E-Commerce Directive, Article 14. The application of this provision has, however, not always been straightforward in practice. See, most recently, *CG v Facebook* [2016] NICA 54.

152 One way in which such private ordering operates, not discussed in this paper, is through terms and conditions. See further, Belli & Venturini (2016).

153 Gillespie (2017).

This paper argues, in particular, that platforms influence the extent to which we can exercise our rights, and the effectiveness of those rights, in a direct and indirect way. These implications are exacerbated when the platform concerned is in a position of power, for instance because of the number of individuals that use the platform. This paper shall illustrate this point by reference to two examples, and will then briefly identify some of the options open to policy-makers to tackle these issues, and the challenges they may face in so doing.

4.2 Regulation by Platforms: the Direct Impact on the Exercise of Fundamental Rights

According to Article 10 ECHR, the freedom of expression includes the freedom to 'receive and impart information and ideas without interference'. Powerful platforms, such as Facebook with its privileged access to 1.86 billion monthly active users[154], control information flows, and shape the relationship between these users[155], on one side of the market, and providers of information and content, on the other side of the market. Whether or not a platform such as Facebook is in a 'dominant' position, or a position of 'significant market power' for competition law purposes is contestable and will ultimately depend on the definition of the relevant market and an empirical assessment of power on that market. Nevertheless, the position of these platforms as chokepoints, or gatekeepers[156], in the digital information sphere is implicit in the fact that they are co-opted by the State in order to police certain content, for instance child abuse images.[157]

154 Facebook, 'Newsroom: Stats'. <http://newsroom.fb.com/company-info> [accessed 1 November 2017].

155 Individuals who register with Facebook and thus create a user profile are deemed to be Facebook users. It is nevertheless important to bear in mind that these users are themselves also content providers (or producers, hence the label 'prosumers' coined by Brown and Marsden: see Brown and Marsden (2017).

156 Barzilai-Nahon (2008).

157 For instance, in the UK the Internet Watch Foundation helps the State to combat the dissemination of child abuse images For further information on the activities of the Internet Watch Foundation visit: <https://www.iwf.org.uk/> [accessed 1 November 2017].

Thus, it is possible to say that in the online world, platforms have primary responsibility for enabling, or disabling, our access to and dissemination of information. Indeed, this power has attracted considerable media attention following the British referendum on Brexit and the election of Donald Trump in the US, where the victors claim that political micro-targeting made possible by the processing of extensive user data was critical to their success at the ballot box.[158] Digital platforms also determine the terms and conditions on which this access to information and dissemination occurs. In practice therefore platforms determine the extent to which individuals can enjoy the benefits of established rights and freedoms, such as the right to freedom of expression. This power to include or exclude certain content from a platform, or to rank it, is a significant power. For instance, in its most recent annual report on Digital News Oxford's Reuters Institute reports that of the 50,000 individuals it surveyed across 26 countries, 12% say social media is their main source of news while in the US, for instance, the percentage of people who use social media as a news source is now 46%, almost doubling since 2013.[159]

This issue has gained prominence recently as a result of increased media and political scrutiny of the role of platforms in disseminating 'fake news'.[160] However, this power of platforms over opinion formation has always been present. Such power is also present in other forms of media, most notably traditional print media and television and radio broadcasts. The critical distinction between these other forms of media and digital platforms is that the former fall within the scope of media law and regulation while digital platforms, such as Facebook for instance, vehemently contest that they constitute 'media' companies and have not been treated as such for legal purposes.

158 See, BBC Panorama, 'What Facebook Knows About You', aired on 8 May 2017; [accessed 1 November 2017]. Cadwalladr (2017).

159 Reuters Institute for the Study of Journalism (2016:7-8).

160 House of Commons - Culture, Media and Sport Committee, 'Fake news' inquiry (closed 3 March 2017) which queried, inter alia, whether 'changes in the selling and placing of advertising encouraged the growth of fake news, for example, by making it profitable to use fake news to attract more hits to websites, and thus more income from advertisers'. <https://www.parliament.uk/business/committees/committees-a-z/commons-select/culture-media-and-sport-committee/inquiries/parliament-2015/inquiry2/> [accessed 8 March 2016].

Ranking in the search engine context is inevitable, as not all search results can appear at the top of the results, or even on the first page. Nevertheless, it appears that search is a 'credence good'[161], and that users therefore trust that the results that are produced in response to a search query, and the order in which these results are produced, is based on objective criteria. This results in what has been labelled a 'search engine manipulation effect' (SEME).[162] SEME does not suggest that search engines deliberately manipulate individuals but rather that individuals fail to consider critically the veracity of search results. Similarly, the suggestions offered by 'autocomplete' tools by platforms arguably influence individual perceptions. As Mansell suggests, search engines have the 'power to ensure that certain public impressions become permanent, while others remain fleeting'.[163]

Consider the controversy in the UK when it was reported that Google search engine's failure to offer a suggested 'autocomplete' search term when individuals entered the words 'Conservatives are' in the search engine yet offered several autocomplete suggestions when terms relating to rival political parties (for instance, 'Labour are') were entered into the search engine.[164] Google's secret sauce – its ranking algorithm – is zealously guarded as a commercial secret with Google revealing only that its algorithm relies on 200 or so signals to glean the search intention of the user. Relevant factors here certainly include geographic location, the 'freshness' of website content etc.[165]

161 In this context, a market for credence goods is understood as a market where 'even when the success of performing the service is observable, customers often cannot determine the extent of the service that was needed and how much was actually performed'. There is therefore an information asymmetry between the service users and those providing the service that prevents the service user from evaluating, amongst other things, the quality of the service received. See, for instance, Wolinsky (1994).

162 Epstein and Robertson (2015).

163 Pasquale (2015:14).

164 The New Statesman, 'Why doesn't Google autocomplete "Conservatives are..."?', 3 February 2016. <http://www.newstatesman.com/politics/media/2016/02/why-doesn-t-google-autocomplete-conservatives-are> [accessed 8 March 2016].

165 Google, 'How Google Search Works': <https://support.google.com/webmasters/answer/70897?hl=en> [accessed 1 November 2017].

Critical attention has however focused on the extent to which this ranking should, or can, be neutral.[166] It is important to highlight that while is an established, and necessary part of the service offered by search engines, ranking and prioritization is a more general feature of many digital platforms. For instance, Facebook does not allow users to adjust their news feeds on a permanent basis to show content in a chronological order. Rather, the news feed of users is governed by Facebook's algorithm: Facebook's 'whole mission is to show people content that we think that they find meaningful', according to its News Feed Product Management Director.[167]

Platforms can also have a significant direct impact on freedom of expression by blocking the route between individuals and providers. Pasquale provides the example of Apple's exclusion of the 'Drone +' application from its App Store.[168] The Drone + application provided users with real-time alerts of drone strikes reported in the media. In this way, users of the application who wished to gain access to publicly available information about under-reported military drone strikes could obtain it in a user-friendly format. The application was rejected from the App Store twice: first on the grounds that it was 'not useful' and subsequently on the basis that it was 'objectionable and crude'.[169] The exclusion of the application is just one illustration of the way in which the actions of gatekeepers can have an impact on opinion formation and the autonomy of Internet users.[170] It also illustrates that gatekeeper transparency is critical.[171]

166 For instance, the European Commission continues to investigate Google for an alleged abuse of dominance on the grounds that it 'systematically favours its comparison shopping services in its search results pages'. The Commission therefore appears to assume an obligation of non-discrimination on Google's part. See European Commission, 'Commission takes further steps in investigations alleging Google's comparison shopping and advertising-related practices breach EU rules', Press Release (14 July 2016). For comment see Daly (2014).

167 Luckerson (2015).

168 Pasquale (2015:62).

169 Pasquale (2015:62).

170 Competition lawyers reject the suggestion made by some authors that Google could be likened to public utilities (such as rail or electricity providers) or essential facilities. See, for instance, Marina Lao (2013).

171 The recent controversy following the 'revelation' that Facebook uses human curators in order to shape the 'Facebook trends' feature also illustrates the opacity of the operations of gatekeepers and the consequent lack of understanding of these operations. See Sam Thielman (2016); Deepa Seetharaman (2016).

It might be argued that other sources of this information remained available, and that all editorial decision-making, including by traditional media outlets such as newspapers, necessarily implies the exclusion of some information. This is true. However, as noted above, decisions in the context of traditional media distribution are subject to media regulation and thus, for instance, rules might apply about the truthfulness of materials broadcast by a newspaper in the run-up to a referendum. Such rules do not apply to digital intermediaries. Moreover, a further difference in the context of this example is the role of Apple's architecture (or code) in the decision-making context.

Apple devices are automatically, and necessarily, routed through the Apple App Store 'walled garden'.[172] Apple's choices are therefore the choices of the user, and the user should be aware of the factors informing Apple's decisions to include and exclude applications/products from its App Store. Apple's role is highlighted here as the 'Drone +' application' was removed from its App Store. However, Google exercises a similar power through its Android Operating System (as discussed below) and it might be argued that the existing duopoly of Apple OS and Android OS in the market for operating systems exacerbates this problem. These operating systems have the power to include and to exclude from their platforms however, as Mansell suggests, 'citizens cannot choose to view what they are not aware of or to protest about the absence of content which they cannot discover'.[173]

4.3 Regulation by Platforms: the Indirect Impact on Fundamental Rights

Platforms may also have an indirect effect on fundamental rights as a result of their position of power vis-à-vis content and service providers. In the data protection and privacy context, this is evident when one considers the role of platforms in setting the benchmark

172 A 'walled garden' is a closed environment (for instance, an operating system) where the operator controls access to the applications, content and services that can be accessed. By only allowing approved apps into the Apple App Store, Apple seeks to ensure better interoperability, synching and security however this closed system may also limit user autonomy. Brian Meyer, 'Why is iOS a Walled Garden?' (*Apple Gazette*,13 November 2013) <http://www.applegazette.com/opinion/why-does-apple-hide-ios-in-a-walled-garden/> [accessed 1 November 2017].

173 Mansell (2015:28).

for data use conditions for all providers wishing to distribute their content or services on the platform. For instance, the UK Competition and Markets Authority (CMA) noted that operating systems (such as Google's Android, or the Apple OS) are:

> responsible for the Application Programming Interfaces (APIs) which dictate how the software and hardware interact – including what information the app can access. APIs control the release of information according to the privacy controls in place at the [operating system] level.[174]

The operating system therefore determines to what extent key data protection principles are promoted. Reports suggest that platforms are doing little to promote key data protection principles, such as data minimisation,[175] amongst application providers. For example, a 2014 survey conducted by the Global Privacy Enforcement Network (GPEN) discovered that one third of all applications requested an excessive number of permissions to access additional personal information.[176] Moreover, the US Federal Trade Commission (FTC) has taken actions against applications such as Brightest Flashlight and Snapchat in recent years for misrepresenting how the personal data they gather is used.[177]

This is not to say that platforms are entirely inactive when it comes to promoting privacy and data protection. Google has, for instance, recently announced that, in addition to accepting the privacy policy of the Android App Store (Google Play), applications must also have their own privacy policy.[178] Reports suggest that Google Play culled applications from its platform on the basis of privacy

174 CMA (2015).

175 Article 6(1)(c) of the Data Protection Directive (European Parliament and Council Directive 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 L281/23) states that personal data must be 'not excessive in relation to the purposes for which they are collected and/or further processed'.

176 CMA (2015:123).

177 CMA (2015:123-124).

178 Charlie Osborne, 'Google plans purge of Play Store apps without privacy policies' (*ZDNet*, 9 February 2017) <http://www.zdnet.com/article/google-plans-purge-of-play-store-apps-without-privacy-policies/> [accessed 1 November 2017].

and data protection concerns.[179] However, their ostensible 'lowest common denominator' approach to these rights influences the extent to which these rights can be enjoyed their users. Indeed, Google Play's cull appeared only to remove egregious violators of rights from the App store (for example, applications requesting sensitive permissions – such as unnecessary data from cameras or microphones – and that did not comply with the basic principles set out in the Play Store privacy policy).

In addition to determining the terms on which applications can operate (and process data), platforms can also demand that applications provide them with access to customer data. For instance, it is well documented that the Financial Times withdrew its application from the Apple App store when it was forced to provide Apple with its consumer data. The news provider went on to launch a Web-based version of its mobile app in a bid to retain reader interest.[180] Smaller news outlets have chosen not to provide an app in a bid to retain custody of their user data.[181]

A complaint filed with the European Commission by the provider of a privacy enhancing technology (PET) provides a further illustration of how platforms can indirectly influence the extent to which individuals can exercise their rights. Disconnect complained to the Commission that Google had excluded one its applications from Android's Google Play application store thereby abusing its position of market power on the market for mobile handset operating systems.[182] Disconnect argued that the exclusion of its application from the Google Play App store unfairly discriminated against its application and gave Google's own rival software a competitive advantage. The Disconnect application in question prevents third parties from tracking Android users when they browse the web or use applications on their devices.

179 Eric Abent, 'Google Play prepares to remove apps over missing privacy policies', (*Slashgear*, 9 February 2017) <https://www.slashgear.com/google-play-prepares-to-remove-apps-over-missing-privacy-policies-09474464/> [accessed 1 November 2017].

180 Reuters, 'Financial Times pulls its apps from Apple Store', (*Reuters,* 31 August 2011) <http://www.reuters.com/article/us-apple-ft-idUSTRE77U1O0020110831>.

181 Helberger et al. (2015:50, 56).

182 Barr (2015).

This tracking is used to gather data to improve the targeting of advertising but can also facilitate the installation of malware on devices. Google responded informally by highlighting that it applies its policies consistently to all applications and that it has 'long prohibited apps that interfere with other apps – such as altering their functionality, or removing their way of making money'.[183] It also emphasised that there are over 200 privacy applications available in Google Play that comply with its policies. This example again illustrates the indirect impact that gatekeepers can have on the exercise of rights: by blocking a PET – a technology designed to enhance privacy – a platform can make it more cumbersome for an individual to exercise privacy and data protection rights. While the impact on rights might be minimal given the availability of competing PETs, it highlights that in the absence of an objective and transparently applied policy for the inclusion of applications on a software platform, the platform can have an impact on the rights of individuals leading to a 'lowest common denominator' approach to their protection.

4.4 Regulatory Options for the Road Ahead

The examples set out above seek to illustrate that private platforms are having a direct and an indirect influence on the extent to which individuals can exercise their fundamental rights, and the effectiveness of these rights in practice. Nevertheless, a regulatory 'solution' to deal with these fundamental rights implications is not obvious.

The issue of 'platform power' has been the subject of increasing doctrinal[184] and media attention.[185] For instance, Cohen has argued that successful state regulation of the information economy will, amongst other things, require an 'analytically sound conception of *platform power*' and 'coherent and publicly accountable methods for identifying, describing and responding to systemic threats'.[186]

183 Chee (2015).

184 See, most notably, Daly (2016).

185 Kennedy (2015); Fairless (2015).

186 Cohen (2016: 369-414). Julie Cohen defines 'platform power' as the 'power to link facially separate markets and/or to constrain participation in markets by using technical protocols.'

'Platform power' is also becoming a prominent feature on public policy and regulatory agendas, particularly across Europe.[187] The European Union (EU) pinpointed this issue for further attention in a 2015 Communication setting out its strategy for a Digital Single Market for Europe. It noted that:

> Some online platforms have evolved to become players competing in many sectors of the economy and the way they use their market power raises a number of issues that warrant further analysis beyond the application of competition law in specific cases.[188]

This marks a turning point as, to date, regulators have assumed that the application of ex post competition law (or antitrust) rules, designed to ensure that companies with market power will not exclude equally efficient competitors or engage in exploitation, negates the need for the *ex ante* regulation of platforms. It is for this reason that competition authorities have, in recent years, dedicated increasing attention to how competition law tools apply to digital markets, and markets involving big data processing in particular.[189]

However, it is suggested in this paper that competition law is the wrong tool to address these harms for several reasons. For instance, the concept of power is 'market power' and is a term of art identified on the basis of economic analysis of substitutability patters. These tests do not reflect power in all its guises. Indeed, markets that are experienced by consumers as monopolistic (for instance, social networking services) may not be classified as relevant markets or may be deemed competitive.

This is not to say that the definition of the 'relevant market' for competition law purposes should reflect consumer perceptions (as opposed to consumer preferences, which should be reflected).

---

187 Conseil National du Numerique (CNNum) (2014:6)..The French *CNNum* acknowledge the ability of internet platforms 'to create great value from the data retrieved from users', it also states that the use of this data must ensure respect for the 'data rights' of users and that individuals 'maintain sole control over the repercussions resulting from the use thereof' and 'benefit from the use of their data'. It concludes that 'recent events have illustrated that current practices do not make it possible to reach these goals'.

188 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 'A Digital Single Market Strategy for Europe' COM (2015) 192 final, 12.

189 For instance, see Autorité de la Concurrence and Bundeskartellamt (2016).

Rather, it is to suggest that 'market power' focuses solely on economic power, defined as the power to act independently of competitors and consumers. Therefore certain areas of activity of digital platforms (such as the offering of 'free' services to end-users) may be overlooked as 'non-economic'. Similarly, other types of power, for example 'data power' (the power to profile and to exacerbate asymmetries of information) and 'media power' (the power to influence opinion formation and autonomous decision-making) may also be overlooked.

Perhaps more significantly, the harms that competition law seeks to remedy are economic harms. This is manifest, for instance, through its focus on consumer welfare.[190] However, the harms at stake here are fundamental rights harms, with civic and social ramifications. This issue should not therefore be viewed solely from a competition law perspective, or from the lens of economic regulation. Indeed, it may be argued that by facilitating further consolidations of power, without any regard for these non-economic implications, competition law should rather be viewed as part of the problem rather than part of the solution.[191]

This is not to say however that the task of regulating powerful platforms is a necessary or an easy one. As a starting point, the harms outlined, even in the context above, are relatively distinct – power over opinion formation; encouraging low standards of data protection, leading to this de facto reality; and, preventing the emergence of technologies that would facilitate 'informational self-determination' and data protection rights, yet harm the bottom line of other application providers. It is thus clear that, if regulation is appropriate to tackle these implications, a single overarching regulatory framework is not the obvious solution. Moreover, as Cohen suggests, as 'threatened future harms have become more abstract, diffuse, and technologically complex, disputes about the appropriate regulatory response have become struggles for

190 According to the European Commission in its Guidance on Article 102 TFEU consumer welfare means that consumers 'benefit from competition through lower prices, better quality and a wider choice of new or improved goods and services'. European Commission, Guidance on the Commission's enforcement priorities in applying Article 82 of the EC Treaty to abusive exclusionary conduct by dominant undertakings OJ [2009] C 45/7, [5].

191 Case COMP/M.7217, *Facebook/Whatsapp*, Commission Decision, [2014] OJ L24/1.

control over the modelling and representation of systemic threats and the burden of proof required to justify regulatory action'[192]

It is also difficult to delimit the target of such regulation: would it simply be 'powerful' platforms? This begs the question of how we might identify, and delimit, these regulatory targets in an objective way. While GAFA (Google-Amazon-Facebook-Apple) might come to mind, it is immediately apparent that the operations of each is distinct and thus may or may not have fundamental rights implications. A harms-focused approach is thus potentially to be preferred, although this may need to take into account the challenge identified by Cohen and to incorporate a lower burden of proof to justify regulatory action.

A further difficulty is that regulation would involve extending the logic of fundamental rights to private operators. Pursuant to international human rights instruments, such as the ECHR, rights can only be exercised vis-à-vis public authorities. However the ECtHR has accepted that in some circumstances a positive obligation exists for the State to protect this right. For instance, in deciding whether such an obligation exists in the freedom of expression context, several factors should be taken into account including: the kind of expression at stake; the capability of that expression to contribute to public debates; the natural and scope of the restrictions on expression rights; the availability of alternative venues for expression; and, the countervailing rights of others or of the public.[193] Others, such as Jean Thomas, have proposed models to enable the enforcement of these public law rights vis-a-vis private actors, justifying this approach by emphasizing the common objectives of descriptive, normative and constitutional theories of rights and the gaps in rights protection that would ensue in the absence of such an extension.[194]

Given these challenges in regulating, it may well be necessary to resort to other non-legal 'modalities of regulation'[195], for instance norm changing or technological fixes, in order to adjust to the influence that private platforms are now having on fundamental rights.

192 Cohen (2016), supra n. 186.

193 *Appleby and Others v. the United Kingdom*, (2003) 37 EHRR 783 paras [42]-[43] and [47]-[49].

194 Thomas (2015).

195 Lessig (2006).

4.5 Bibliography

Abent E (2017). 'Google Play prepares to remove apps over missing privacy policies', (*Slashgear*, 9 February 2017) <https://www.slashgear.com/google-play-prepares-to-remove-apps-over-missing-privacy-policies-09474464/> [accessed 1 November 2017].

Autorité de la Concurrence and Bundeskartellamt (2016). 'Competition Law and Data' Joint Report (10 May 2016) <http://www.autoritedelaconcurrence.fr/doc/reportcompetitionlawanddatafinal.pdf> [accessed 1 November 2017].

Barlow J P (1996). 'A Declaration of the Independence of Cyberspace' (8 February 1996) <https://www.eff.org/cyberspace-independence> [accessed 1 November 2017]

Belli L & Venturini J (2016). 'Private ordering and the rise of terms of service as cyber-regulation' (2016) 5(4) Internet Policy Review.

Brown I and Marsden C (2013). 'Regulating Code: Towards Prosumer Law?' (February 25, 2013). <https://ssrn.com/abstract=2224263> [accessed 1 November 2017].

Barzilai-Nahon K (2008). 'Toward a theory of network gatekeepeing: A framework for exploring information control' (2008) 59(9) Journal of the American Society for Information Science and Technology 1493.

Barr A (2015). 'App Maker Files EU Complaint Against Google, Alleging Abuse of Android Dominance', *Wall Street Journal* (1 June 2015) <http://www.wsj.com/articles/app-maker-files-eu-complaint-against-google-alleging-abuse-of-android-dominance-1433204706#:mdP9UlcFB3W9ZA> [accessed 1 November 2017].

Cadwalladr C (2017). 'The great British Brexit robbery: how our democracy was hijacked', *The Guardian* (7 May 2017) https://www.theguardian.com/technology/2017/may/07/the-great-british-brexit-robbery-hijacked-democracy [accessed 1 November 2017].

Chee F Y (2015). 'Privacy app maker files EU antitrust complaint against Google', (*Reuters*, 2 June 2015). <http://www.reuters.com/article/us-eu-google-antitrust-idUSKBN0OI1Z220150602> [accessed 1 November 2017].

Competition and Market Authority (2015). 'Commercial use of consumer data: Report on the CMA's call for information' (June 2015) <https://gov.uk/government/consultations/commercial-use-of-consumer-data [accessed 1 November 2017].

Conseil National du Numerique (2014). 'Platform Neutrality: Building an open and sustainable digital environment', CNNum (May 2014) https://cnnumerique.fr/platform-neutrality-builduing-an-open-and-sustainable-digital-environment [accessed 1 November 2017].

Daly A (2016). *Private Power, Online Information Flows and EU Law: Mind the Gap* (Hart Publishing, 2016).

Daly A (2014). 'Dominating search: Google before the law' in R Konig & M Rasch (Eds.) INC Reader #9 Society of the Query: Reflections on Web Search (Institute of Network Cultures, 2014), 86-104.

Epstein R & Robertson R E (2015). 'The search engine manipulation effect (SEME) and its possible impact on the outcomes of elections' (2015) 112 Proceedings of the National Academy of Sciences of the United States of America (PNAS). <http://www.pnas.org/content/112/33/E4512.abstract> [accessed 1 November 2017].

European Commission, 'Guidance on the Commission's enforcement priorities in applying Article 82 of the EC Treaty to abusive exclusionary conduct by dominant undertakings'. OJ [2009] C 45/7.

European Commission, 'Public Consultation on the regulatory environment for platforms, online intermediaries, data and cloud computing and the collaborative economy' (September 2015) <https://ec.europa.eu/digital-single-market/en/news/public-consultation-regulatory-environment-platforms-online-intermediaries-data-and-cloud> [accessed 1 November 2017].

European Commission, 'Commission takes further steps in investigations alleging Google's comparison shopping and advertising-related practices breach EU rules', Press Release (14 July 2016) <http://europa.eu/rapid/press-release_IP-16-2532_en.htm> [accessed 1 November 2017].

Fairless T (2015). 'EU Digital Chief Urges Regulation to Nurture European Internet Platforms', *The Wall Street Journal* (14 April 2015) <http://www.wsj.com/articles/eu-digital-chief-urges-regulation-to-nurture-european-internet-platforms-1429009201> [accessed 1 November 2017].

Gillespie T (2017). 'Governance of and by platforms' in J Burgess, T Poell, and A Marwick (eds) *SAGE Handbook of Social Media* (Sage Publishing, 2017).

Hartzog W (2011). 'Website Design as Contract' (2011) 60 American University Law Review 1635.

Helberger N, Kleinen-von Königslöw K and van der Noll R (2015). 'Regulating the new information intermediaries as gatekeepers of information diversity' (2015) 17(6) Info 50.

Kennedy J (2015). 'Don't regulate internet platforms, embrace them', *EurActiv* (14 November 2015) http://www.euractiv.com/section/digital/opinion/don-t-regulate-internet-platforms-embrace-them/ [accessed 1 November 2017].

Lao M (2013). 'Search, Essential Facilities and the Antitrust Duty to Deal' (2013) 11 (5) Northwestern Journal of Technology and Intellectual Property 275.

Lemley M A (2006). 'Terms of Use' (2006) 91 (2) Minnesota Law Review 459.

Lessig L (2006). *Code and Other Laws of Cyberspace*, *Version 2.0* (Basic Books, 2006).

Luckerson V (2015). 'Here's Why Facebook Won't Put Your News Feed in Chronological Order', *TIME* (9 July 2015) <http://time.com/3951337/facebook-chronological-order/> [accessed 1 November 2017].

Mansell R (2015). 'Platforms of power' (2015) 43(1) Intermedia 20.

Meyer B, 'Why is iOS a Walled Garden?' (*Apple Gazette*, 13 November 2013) <http://www.applegazette.com/opinion/why-does-apple-hide-ios-in-a-walled-garden/> [accessed 1 November 2017].

Osborne C (2017). 'Google plans purge of Play Store apps without privacy policies' (*ZDNet*, 9 February 2017) <http://www.zdnet.com/article/google-plans-purge-of-play-store-apps-without-privacy-policies/> [accessed 1 November 2017].

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

Powles J (2015). 'The Case That Won't be Forgotten' (2015) 47 (2) Loyola University Chicago Law Journal 583.

Reuters Institute for the Study of Journalism (2016). 'Reuters Institute Digital News Report 2016' http://reutersinstitute.politics.ox.ac.uk/sites/default/files/Digital%20News%20Report%202016.pdf.

Reuters, 'Financial Times pulls its apps from Apple Store', 31 August 2011 <http://www.reuters.com/article/us-apple-ft-idUSTRE77U1O020110831> [accessed 1 November 2017].

Seetharaman D (2016). 'Facebook's Curators Shape 'Trending' News Feature' *Wall Street Journal* (12 May 2016). <http://www.wsj.com/articles/facebooks-curators-shape-trending-news-feature-1463095472> [accessed 1 November 2017].

The New Statesman, 'Why doesn't Google autocomplete "Conservatives are..."?' (3 February 2016). <http://www.newstatesman.com/politics/media/2016/02/why-doesn-t-google-autocomplete-conservatives-are> [accessed 1 November 2017].

Thielman S (2016). 'Facebook news selection is in hands of editors not algorithms, documents show', *The Guardian* (London, 12 May 2016) <https://www.theguardian.com/technology/2016/may/12/facebook-trending-news-leaked-documents-editor-guidelines> [accessed 1 November 2017].

Thomas J (2015). *Public Rights, Private Relations* (Oxford University Press, 2015).

Wolinsky A (1994). 'Competition in Markets for Credence Goods', Discussion Paper No 1099, July 1994. <https://www.kellogg.northwestern.edu/research/math/papers/1099.pdf> [accessed 1 November 2017].

5 Fundamental Rights and Digital Platforms in the European Union: a Suggested Way Forward

Joe McNamee **and** ***Maryant Fernández Pérez***[196]

Abstract

This chapter analyses the debate regarding digital platforms and fundamental rights in the European Union. First, the paper argues that, when referring to "digital platforms", it may be counterproductive to categorise players as different as AirBnB, Google News and YouTube, as the same type of business. In this sense, the chapter suggests five categories of platforms based on the existence of a relationship with consumers or businesses and based on the transactional nature of the relationship. Furthermore, this paper notes that standard content guidelines of digital platforms do not necessarily respect the principle of legality or comply with fundamental human rights. In this regard, so called "community guidelines" often prohibit content, which is lawful and/or protected by European human rights law. We offer several examples of bad practices to corroborate our thesis and to conclude that, worryingly, neither governments nor Internet intermediaries appear to feel morally or legally responsible/accountable for assessing the durability or potential counterproductive effects that can be deployed by the measures that they implement. As a conclusion, the paper recommends the essential elements that future platform policies should incorporate in order to abide fully to the obligations prescribed by the Charter of Fundamental Rights of the European Union.

5.1 Introduction

5.1.1 Digital Platforms: Which Platforms?

It is important to understand which actors we are addressing when referring to "digital platforms". As stated in EDRi's response to the European Commission's public consultation on online platforms in

196 This paper is based on EDRi's initial comments to the questions asked by the European Commission in preparation for its Workshop on Fundamental Rights and Digital Platforms that took place on 12 June 2017.

2015[197], "it is not useful to have AirBnB, Google News and YouTube categorised as being the same type of business" – to name but a few examples. In this sense, this paper suggests five classifications of platforms (P) based on the relationship with consumers (C) or businesses (B) and based on the transactional nature of the relationship:

- Transaction[198]-based platform to consumer (P2C) platforms, such as Netflix or Spotify. These platforms utilise content licensed by rightholders to platforms. Therefore, transactions occur on the various sides of the platform, *i.e.* between platform and rightholders and between platform and its users.
- Non-transaction-based P2C platforms, such as Google news and other news aggregators or review services like Yelp. In these platforms, content is freely available online, with no P2B transaction. Hence, there is no transaction on either side of platform.
- Zero consumer value P2B services, such as promoted content on social media companies like Twitter. In this type of platforms, the transaction happens on the business side of platform.
- Transaction-based consumer or business to consumer (C2C & B2C) platforms. Examples of this type of platform include companies like Ebay and AirBnB. In these platforms, transactions take place between businesses and the platform, and between consumers and businesses (B2P & C2B transactions).
- Non-transaction-based consumer to consumer (C2C) platforms. These include UGC, blogging, micro-blogging, etc.

When referring to digital platforms, big players like Google or Facebook often come to mind. However, small and medium companies need to be taken into account. Big players and SME have different needs and, frequently, the same obligations cannot be applied to both because they would represent excessive burden for start-ups and SMEs in general, thus stifling competition and reducing opportunities for freedom of expression.

197 See EDRI's answering guide to the European Commission's platform consultation, available at <https://edri.org/files/platforms.html> [accessed 1 November 2017].

198 Transaction means "Financial transaction". The business model may be based on harvesting/ reuse of personal data (non-financial) to some degree.

For the purposes of this paper, when referring to "digital platforms", we will mostly refer to non-transaction-based consumer-to-consumer platform companies unless indicated otherwise.

5.1.2 What Fundamental Rights are at Stake?

The activities of digital platforms may have many implications on individuals' capacity to enjoy their human rights and fundamental freedoms, such as the right to privacy, protection of personal data, freedom of expression, freedom of thought, conscience and religion, freedom of assembly and association, freedom of the arts and sciences, right to an effective remedy, among others. Hence, it is important to consider the different implications and capabilities of digital platforms from a wider perspective in order to understand the complexity of the debate. This paper, however, will focus only on the impact of digital platforms on freedom of expression and opinion when restricting access to online content.

5.1.3 What Is Happening in the European Union?

In the European Union, references to the need to fight against illegal and "harmful" online content are constantly and incoherently being made.[199] In this perspective, it should be noted that the term "harmful" is exceedingly vague and, for this reason, cannot form the basis for lawful restrictions on freedom of expression under European human rights law. Indeed, when the decision on what is harmful or not is left to the free will of companies, such entities may not necessarily comply with the legality principle.[200]

As a matter of law, however, the obligation to only restrict speech in compliance with the legality principle, as established by the European Charter of Fundamental Rights, only applies to legal

199 See, for instance: Maryant Fernández Pérez, 'Audiovisual Media Services Directive reform: Document pool' (*EDRi*, 15 May 2017) <https://edri.org/avmsd-reform-document-pool/> [accessed 1 November 2017]; Maryant Fernández Pérez, 'EU Parliament to vote on contentious anti-radicalisation Resolution' (EDRi, 18 November 2017) <https://edri.org/eu-parliament-vote-antiradicalisation-resolution/> [accessed 1 November 2017]; Communication from the Commission and the European Parliament, The Council, the European Economic and Social Committee and the Committee of the Regions 'Online Platforms and the Digital Single Market Opportunities and Challenges for Europe' (22 May 2016), COM(2016) 288 final<http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016DC0288> [accessed 1 November 2017].

200 See, for instance, Joe McNamee, 'FAQ: EU Code of Conduct on illegal hate speech' (*EDRi*, 18 November 2017) <https://edri.org/faq-code-conduct-illegal-hate-speech/> [accessed 1 November 2017].

instruments adopted by the EU. Companies remain free to remove "harmful content" under their terms and conditions, even if this may be sometimes unjustified. In the latter case, it seems appropriate that the companies be publicly criticised, when imposing undue restrictions. As a bare minimum, companies' community guidelines should be in line with international and European standards on freedom of expression.

As stated in Articles 12 to 15 of the E-Commerce Directive and described in our response to aforementioned public consultation,

> "where an intermediary is not hosting the content (acting as a mere conduit, an access provider or a search engine), it should have no liability for this content, nor should it have any obligations with regards to the removal or filtering of this content as an access provider, it should have neither liability nor obligations with respect to content;
>
> where an intermediary acts as a hosting provider, its liability with respect to the content hosted should be restricted to its lack of compliance with a court order to take down this content.
>
> Intermediaries should have no obligation to monitor content." [201]

The E-Commerce Directive is the European legislative instrument that applies horizontally to all laws regarding the provision of relevant information society services. This means that the liability provisions for all types of infringing content are the same for all companies covered by those provisions. Nonetheless, such horizontal legislation is being changed by vertical legislation[202] (legislation that sets specific types of infringing content), such as the Copyright Directive reform,[203] the Audiovisual Media Services

201 See supra n. 197.

202 Joe McNamee, 'ENDitorial: Commissioners' oath – a broken promise on fundamental rights', EDRI (14 December 2015). <https://edri.org/enditorial-commissioners-oath-a-broken-promise-on-fundamental-rights/> [accessed 1 November 2017].

203 Diego Naranjo, 'Copyright reform: Document pool' (*EDRi*, 12 December 2016) <https://edri. org/copyright-reform-document-pool/> [accessed 1 November 2017].

Directive (AVMSD) revision[204] as well as by the encouragement of "voluntary" arrangements, such as the EU Code of Conduct on Hate Speech.

If encouraged by public entities, including the European Commission, "voluntary measures" are not truly voluntary or "self-regulatory" but rather necessary to avoid liability, maintain good public relations or avoid political costs. It is clear, therefore, that both the European Commission and Member States should stop misrepresenting the aforementioned measures as such. On the other hand, a procedural best practice is the European Commission's decision to sign the "follow the money" agreement, thereby having the courage to stand behind the agreement both legally and politically. Even if the arrangement is not exempted from critiques from a substantial perspective, this is a meaningful step in the right direction, from a procedural standpoint.

States have positive and negative obligations with regard to human rights obligations, including in the digital environment. However, companies do not have these obligations and ensuring that voluntary measures are "in full respect of fundamental rights" is close to impossible. From a legal perspective, companies are not bound by the Charter of Fundamental Rights of the European Union. In this context, the legally, but not ethically or politically, grey zone between state responsibilities for fundamental rights and the rights and responsibilities of companies is being exploited in ways that border on cynicism.

According to the UN Special Rapporteur on freedom of opinion and expression, corporations have a responsibility to respect fundamental rights, even if enforcement instruments are lacking. However, companies are getting more and more pressure from public authorities to "do more", to remove and restrict access to certain content online, without the need to conduct a legality assessment, without any counterbalancing obligations for companies to respect human rights and fundamental freedoms. This is what we call "privatised law enforcement" or "privatised

204 Maryant Fernández Pérez, 'Audiovisual Media Services Directive reform: Document pool' (*EDRi*, 15 May 2017) <https://edri. org/avmsd-document-pool/> [accessed 1 November 2017].

censorship". This phenomenon, however, should be seen in the context of states positive and negative obligations. Restrictions, imposed by states directly or indirectly, on fundamental rights must be provided for by law, be necessary and proportionate to the aims pursued. Hence, EU member states must take measures to ensure respect of fundamental rights in any notice and action mechanism.

In its 2016 Communication on platforms, the European Commission stated that the EU will "only address clearly identified problems related to a specific type or activity of online platforms" and that "such problem-driven approach should begin with an evaluation of whether the existing framework is still appropriate." This statement, together with the procedural precautions, the call for checks and balances as well as transparency in the notice-and-action process highlighted in the 2017 Communication, are very welcome. Moreover, the Commission has correctly pointed out the need for minimum procedural requirements for notice and action procedures. This should be done in the form of a combination of EU and national legislation. In view of advancing the Digital Single Market in the EU, a Directive seems to be the most suitable mechanism for this.

5.2 What Are the Key Questions to Be Considered?

This section answers key questions regarding fundamental rights, raised by the European Commission in its consultation on digital platforms. The brief analysis of these questions will allow to understand the background and reasons why further guidance on notice and action is needed in the EU.

5.2.1. Gathering Evidence

In this section, we provide evidence supporting the claim that freedom of expression can be undermined by voluntary measures taken by digital platforms.

First, it should be noted that standard content guidelines of digital platforms do not necessarily follow the law or respect fundamental human rights. Community guidelines often ban content, which is lawful and/or protected by European human rights law, often in an

arbitrary and unpredictable way. Many examples of bad practice can be offered in this regard, including:

- The outcomes of the Multatuli Project, conducted by Bits of Freedom in 2004 and 2012.[205] EDRi-member Bits of Freedom wanted to test how Dutch Internet Service Providers (ISPs) dealt with notice and action procedures. They invented a customer who had uploaded a text from the author Multatuli (Eduard Douwes Dekker), which clearly belongs to the public domain (the date of publication was prominently displayed) and whose publication was obviously legal. They invented a copyright holder and created a fake legal representative. They issued transparently unjustified complaints to ten Dutch ISPs. Most of the ISPs deleted the content despite the fact that even a cursory assessment would have made clear that the complaints had no merit;
- The EU Code of Conduct on Hate Speech does not require cooperation between private actors and public authorities or any legality assessment;[206]
- Censorship of an iconic Vietnam War picture, for nudity, by Facebook in September 2016.[207] The picture was restored only because of intense public pressure due to the emergence of a worldwide debate on the matter. This is an example of the negative impact and uncertainty produced by leaving the power to decide what is licit and what is not to private companies. These entities respond to government, shareholder or public relations pressure. Such pressure, together with business motives (avoiding bad publicity in the aforementioned case), plays a considerable a role in whether content is removed or restored by online platforms.

205 Sjoera Nas, 'The Multatuli Project. ISP Notice & take down' (*Bits of Freedom*, 1 October 2004) <https://www-old.bof.nl/docs/researchpaperSANE.pdf> [accessed 1 November 2017]; Janneke Sloëtjes, 'Unpredictable and unclear: Hosting policy removal policy' (*Bits of Freedom*, 21 December 2012) <https://bof.nl/2012/12/21/onvoorspelbaar-en-onduidelijk-het-verwijderingsbeleid-van-hostingproviders/> [accessed 1 November 2017]; 'Overgeleverd Aan Willekeur' (*Bits of Freedom site*, 22 December 2012) <https://bof.nl/wp-content/uploads/20120401-overgeleverd-aan-willekeur-rapport.pdf> [accessed 1 November 2017].

206 See Joe McNamee, supra n. 200; Maryant Fernández Pérez, 'New documents reveal the truth behind the Hate Speech Code' (*EDRi*, 7 September 2016) <https://edri.org/new-documents-reveal-truth-behind-hate-speech-code/> [accessed 1 November 2017].

207 Mark Scott and Mike Isaac, 'Facebook Restores Iconic Vietnam War Photo It Censored for Nudity', *New York Times* (9 September 2016) <https://www.nytimes.com/2016/09/10/technology/facebook-vietnam-war-photo-nudity.html?_r=0> [accessed 1 November 2017].

Furthermore, a variety of sources have provided increasing evidence demonstrating that private ordering designed and implemented by digital platforms can have harmful effects on users' rights. To mention a few examples, Dr. Sally Broughton Micova analysed the terms set by Facebook, YouTube and Snapchat. The researcher concluded that there are serious gaps and disparities in the terms of service.[208] In the same vein, the Center for Technology & Society at Fundação Getúlio Vargas Rio de Janeiro Law School conducted a study on Terms of Service and Human Rights in partnership with the Council of Europe, demonstrating that, frequently, platforms' terms of service do not comply with international human rights law, regarding freedom of expression, privacy and due process.[209]

Several documentaries have also exposed in detail the influence of companies on people's rights. As an instance, the documentary "The Moderators" shows evidence of some of the flaws of content removals in online platforms.[210] The documentary "Facebookistan"[211] also provides useful insight on the social network practices, exposing an interview with a Facebook content reviewer.

In May 2017, the Guardian leaked the guidelines given to the Facebook officers when dealing with nudity in art[212] and, according to some of them, they do not help a lot. The situation becomes worse when dealing with cyber bullying and sextortion.[213] The impact of companies like Facebook is not only tangible in the European Union, but also across the globe. The OnlineCensorship portal[214] provides several examples of "what content is taken

208 Cf. Broughton Micova (2017:3)

209 Center for Technology and Society (2016).

210 Andy Greenberg, 'Watch People Learn Filter Obscene and Violent Photos from Dating Sites', *Wired Magazine* (14 April 2017) <https://www.wired.com/2017/04/watch-people-learn-filter-awfulness-dating-sites/> [accessed 1 November 2017]; Colin Lechner, 'A new documentary goes inside the bleak world of content moderation' *The Verge* (16 April 2017) <https://www.theverge.com/2017/4/16/15305562/the-moderators-documentary> [accessed 1 November 2017].

211 See <http://facebookistan.org/> [accessed 1 November 2017].

212 Sex and nudity in art: Facebook's rules', *The Guardian* (London, 22 May 2017) <https://www.theguardian.com/news/gallery/2017/may/22/sex-and-nudity-in-art-see-facebooks-rules> [accessed 1 November 2017].

213 Jamie Grierson, "No grey areas': experts urge Facebook to change moderation policies', *The Guardian* (London, 22 May 2017) <https://www.theguardian.com/news/2017/may/22/no-grey-areas-experts-urge-facebook-to-change-moderation-policies> [accessed 1 November 2017].

214 See <https://onlinecensorship.org/> [accessed 1 November 2017].

down, why companies make certain decisions about content, and how content takedowns are affecting communities of users around the world."[215] Just to cite an example, the prohibition of the word "*kalar*" in social networks, in Myanmar, led to a wide range of unintended consequences, the term being used both as a racist term referring to Muslims and as an innocuous adjective referring to "lentil bean" or a variety of chili.[216]

Finally, it is worth pointing out that EU legislation may also encourage potentially damaging practices. For instance, Article 4.1. m) of the Europol Regulation[217] foresees the "voluntary" removal of content on the basis of terms of service, with no mention of illegality. Worse still, there is no indication that the European Commission devotes any effort whatsoever to ensuring that the provision is implemented in line with the Charter.[218]

5.2.2 Legal Impact of Fundamental Rights on Digital Intermediaries' Operation

The Fundamental Rights Charter is only legally binding for the EU and for Member States (Article 51). Private companies such as digital platforms are not directly bound to comply with them and could legally limit the content that they made available according to their own terms and conditions.

However, EU Member States are required to assure that private entities comply with the law, including human rights law. This is not happening when dealing with online companies as they are often pressured to adopt restrictions to freedom of expression on a "voluntary" basis, without necessarily complying with the rule of law and the necessity and proportionality principles.

215 For more information, please see Anderson et al. (2016).

216 Thant Sin, 'Facebook Bans Racist Word 'Kalar' in Myanmar, Triggers Collateral Censorship' (*Advox*, 2 June 2016) <https://advox.globalvoices.org/2017/06/02/facebook-bans-racist-word-kalar-in-myanmar-triggers-collateral-censorship/> [accessed 1 November 2017].

217 Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA. OJ L 135, 24.5.2016, 53–114

218 See EDRi, 'Europol: Non-transparent cooperation with IT companies' (18 May 2016) <https://edri.org/europol-non-transparent-cooperation-with-it-companies/> [acccessed 1 November 2017]. See also 'Oversight of the new Europol regulation likely to remain superficial', *EDRi* <https://edri.org/oversight-new-europol-regulation-likely-remain-superficial/> [acccessed 1 November 2017].

Unfortunately, even if the UN Guiding principles on business and human rights have been adopted by many Member States and companies, it seems its implementation is not really working.[219] The same applies to other non-legally binding principles. One of the ways in which Member States can impose direct obligations on companies to respect fundamental rights is by adopting laws like *e.g.* data protection laws. Since one of the critical shortfalls of social media companies concerns due process and lack of effective remedies for wrongful removal of content, there is an argument to be made that at the very least States should provide an avenue of appeal once social media companies' internal mechanisms have been exhausted. This view appears to be supported by the CJEU in the Telekabel ruling.[220] However, this must not be taken as meaning that any amount of privatised enforcement is acceptable, as long as there is a theoretical appeals process.

5.2.3 Corporate Responsibility of Digital Intermediaries in Relation to Fundamental Rights

Beyond legal responsibility, reports from the UN and the Council of Europe have suggested that companies providing online services have a corporate responsibility to respect human rights. On this topic, the former UN Special Rapporteur on Freedom of Expression, Frank LaRue, recommended intermediaries to:

a only implement restrictions to the rights of freedom of expression and privacy after judicial intervention;
b be transparent about the measures taken;
c minimise impact of measures taken strictly to the content involved;
d notify users before implementing restrictions;
e put in place effective remedies for affected users;
f establish clear and unambiguous terms of service.

However, digital platforms may face some problems when they take up their responsibility of respecting and promoting Fundamental

219 See Jorgensen (2017).

220 See Case C-314/12, *UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH*, ECLI:EU:C:2014:192. Elements of this judgement are discussed in the next section.

Rights. Digital intermediaries are asked to act expeditiously to remove illegal content but to not interfere with the transmission (*i.e.* not to be involved in processes which would give effective knowledge of the potential illegality of the content) in order to benefit from safe-harbour provisions provided by the E-commerce Directive.[221]

Digital intermediaries make a distinction between terms of service violations and external requests made by governments and Law Enforcement Agencies (LEAs). In the latter case, they would need to check the legal basis for a request and its compliance with human rights standards, in order to guarantee the right to freedom of expression of their users. This does not happen when they have to deal with their internal rules (or community guidelines), which are not framed as a freedom of expression issue. For example, Google only includes external requests in its transparency report.[222]

With regard to privacy, some intermediaries (*e.g.* Facebook and Google) do not seem to fully consider the implications of privacy, when dealing with massive exploitation of their users' data.[223] The view appears to be that, once the user is in control, however nebulous this control might be, of its privacy settings, the problem is solved, regardless of how unpredictable/incomprehensible these settings may be. In reality, the user must have meaningful control of how her/his data are shared, analysed and on how they are collected.[224]

To promote fundamental rights, digital platforms are putting in place several efforts and commitments. Some of them are part of the Global Network Initiative (GNI), created in 2008 and engage in the work of the Freedom Online Coalition. However, evidence shows that very little progress is made for the protection of fundamental rights and for the right to privacy and freedom of expression in particular. Some insight in this regard is provided

221 See Jorgensen et al. (2017).

222 Jorgensen (2017:10-11).

223 Jorgensen (2017:6). See also <http://www.beuc.eu/publications/beuc-x-2017-083-google-privacy-policy_facebook-emotional-ad-targeting.pdf> [accessed 1 November 2017] and <http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083> [accessed 1 November 2017].

224 Jorgensen (2017:12).

by the Ranking Digital Rights Corporate Accountability Index[225], which is based on publicly available material.

As an example, Facebook improved the interface that let users decide what kind of data they share in order to use applications.[226] However, these features are not turned on by default, are very difficult to find and no meaningful information is provided to users. With regard to freedom of expression, Internet companies seem to prefer to restrict access to online content on the basis of terms of service in order to avoid liability. This leads to errors and legal content restrictions that have a negative impact on users.[227]

Worryingly, nobody, whether governments or intermediaries, appears to feel morally or legally responsible/accountable for assessing the durability or potential counterproductive effects – including for the ostensible public policy goal – of any measures that are implemented. This lacuna is quite clear in, for example, the Commission's 2017 Digital Single Market (DSM) Communication.

5.2.4 The Role of the EU in Relation to Corporate Responsibility

Member States and the EU institutions have positive and negative obligations to respect human rights. Exerting pressure on companies to achieve public policy objectives without a counterbalancing obligation for the companies to respect fundamental rights (nor obligations for states to foresee review mechanisms) does not seem the best possible approach. In 2012, the European Commission launched an initiative on Notice and Action procedures "to set up a horizontal European framework to combat illegality on the Internet, and to ensure the transparency, effectiveness, and proportionality of the employed procedures, as well as compliance with fundamental rights."[228] The aim of this initiative by DG CNECT should be to lead to concrete results and deliver a Directive on Notice and Action, as already requested by EDRi in the past.[229] Any such initiative should

225 See https://rankingdigitalrights.org/ [accessed 1 November 2017].

226 Jorgensen (2017:10).

227 Onlinecensorship.org offers a wide variety of examples.

228 Jorgensen et al. (2017:17).

229 See for example <https://edri.org/files/EDRi_ecommerceresponse_101105.pdf> [accessed 1 November 2017].

take a holistic approach and include provisions on diligence such as the role of the state in terms of accountability for the processes put in place, playing its role in dealing with serious illegal content, review mechanisms that look at the overall impact on the public policy objective(s) being pursued and ensuring that counterproductive impacts for both fundamental rights and the public policy objective being pursued are minimised.

Digital platforms have *de facto* a role as gatekeepers in our society, and while they provide huge benefits, they are also in a position of power with the potential for censorship or control over the capacity of users to express themselves. In this context, the EU and the EU Member States should start by controlling that the legislation, non-binding initiatives and activities they are adopting or encouraging respect fundamental rights and freedoms. As EDRi wrote in its expert paper for the Council of Europe (2014)[230]:

> "States have the primary obligation to ensure that their legal systems provide adequate and effective guarantees of freedom of expression, which can be properly enforced." In the Telekabel ruling, the Court of Justice of the European Union, assumed that pressures put on the company via an injunction were counterbalanced by unspecified other obligations to uphold users' fundamental rights. If the Telekabel assumption is incorrect [and such safeguards do not exist], the legal framework needs to be updated. It is dangerous to leave it to the private sector to decide over the proper balance between fundamental rights, as this may lead to arbitrary decisions, most particularly when the incentives are imbalanced. It is also questionable whether intermediaries can reasonably be asked to make an arbitrary ruling of (il)legality with regard to statements made by third parties before anyone even contested them."

230 European Digital Rights (EDRi), 'Human Rights Violations Online', Report for the Council of Europe (4 December 2014), DGI(2014) 31 <https://edri.org/files/EDRI_CoE.pdf> [accessed 1 November 2017].

Unfortunately, as seen *e.g.* in the ongoing Copyright debate, the EU often puts itself in a position that undermines fundamental rights, such as freedom of expression when they ask platforms to use technical means to restrict content.[231]

The Treaties offer Member States, the European Parliament and the Commission possibilities to request for a legal opinion from the CJEU. This could be an interesting avenue to explore. If the Commission follows EDRi's recommendation on adopting a Notice and Action Directive,[232] meaningful action can be brought against companies that fail to respect binding commitments.

Furthermore, it should be stressed that freedom of expression is not the only fundamental right at stake.[233] In the context of notice and action procedures, the Commission may want to pay particular attention at the contributions of the European Data Protection Supervisor (EDPS) in relation to the implications for the rights to privacy and data protection.[234] For example, the EDPS has identified issues in relation to the confidentiality of the notice provider and other relevant actors concerned by notice and action procedures; how personal data are handled; transparency of the process; how companies cooperate with law enforcement authorities, among others.[235]

---

231 See <https://edri.org/files/copyright/copyright_proposal_article13.pdf> [accessed 1 November 2017]; EDRi, 'Civil society urges EU institutions to stop the "censorship machine" in the copyright proposal' (EDRi site, 13 March 2017) <https://edri.org/civil-society-urges-eu-institutions-to-stop-the-censorship-machine-in-the-copyright-proposal/> [accessed 1 November 2017].

232 See the conclusion of this chapter.

233 Other fundamental rights such as freedom of thought, conscience and religion, freedom of assembly and association, freedom of the arts and sciences, the right to an effective remedy and right to a fair trial, should be considered, among others.

234 See for example:EDPS, 'EDPS formal comments on DG MARKT's public consultation on procedures for notifying and acting on illegal content hosted by online intermediaries' (13 September 2012) <https://edps.europa.eu/sites/edp/files/publication/12-09-13_comments_dg_markt_en.pdf> [accessed 1 November 2017]; EDPS, 'EDPS Opinion on the proposal for a Directive of the European Parliament and of the Council on combating the sexual abuse, sexual exploitation of children and child pornography, repealing Framework Decision 2004/68/JHA'. <https://edps.europa.eu/sites/edp/files/publication/10-05-10_child_abuse_en.pdf> [accessed 1 November 2017]. EDPS, 'Opinion of the European Data Protection Supervisor on the current negotiations by the European Union of an Anti-Counterfeiting Trade Agreement (ACTA) (2010/C 147/01)', OJ C 147, 5.6.2010, p. 1. <https://edps.europa.eu/sites/edp/files/publication/10-02-22_acta_en.pdf> [accessed 1 November 2017].

235 See EDPS, 'EDPS formal comments on DG MARKT's public consultation on procedures for notifying and acting on illegal content hosted by online intermediaries', *Ibid.*

5.2.5 Fundamental Rights and Formal Notice-and-action Procedures

To ensure respect of Fundamental Rights in a predictable way, it seems also important that digital platforms explain the reasons for content restrictions and inform the user in a meaningful way (not with vague, standard notifications) on how to appeal the decision and the timeframe available for doing that. A variety of Fundamental Rights could be affected by formal notice-and-action procedures. In particular, freedom of expression can be affected when the decision regarding the removal of specific content is delegated to the platforms (see, *e.g.* the Facebook guidelines above, on nudity in art), even when following a notice-and-action procedure. For example, a politician could flag a harsh comment as defamatory to censor dissidents. Therefore, it is crucial that digital platforms follow binding legal criteria to ensure a balanced judgement. This can be achieved by a good Notice and Action Directive, as we stress in the conclusion of this paper.

Many rights must be balanced in the digital environment, such as the right to conduct a business (for ISP), freedom of expression, the right to privacy, etc. The guide for balancing should be Article 10(2) ECHR. Digital platforms should not arbitrarily restrict one right in favour for another when the solution is not clear. In this case, it is important to have at least a way to redress the decision.

It is important to note that restrictions to Fundamental Rights may be justified in specific circumstances. According to Article 10(2) ECHR and Article 52 of the Charter, restrictions must be provided for by law, be necessary and proportionate to the aim pursued. There are cases, like child abuse material (sometimes referred to as "child pornography"), when a restriction of fundamental rights can be justified. This is clear because the publication of child pornography cannot be included under the umbrella of the freedom of expression, because it is an element of a serious crime and is prohibited by international law instruments ratified by virtually every country on the planet (such as the UN Child Rights Convention, ratified by every country except the USA, and the Optional Protocol on the sale of children, child prostitution and child pornography, which was ratified, *inter alia*, by the USA).

However, as the UN Special Rapporteur on the Promotion of Freedom of Expression said, these restrictions are possible only when "the national law is sufficiently precise and there are effective safeguards against abuse or misuse."[236] It is important to point out that the Rapporteur refers to "the law". This means that a code of conduct is not sufficient alone to justify the removal of content. It is also crucial, when dealing with serious crimes against people, that everybody play their role. It is not acceptable to have codes of conduct for removal of, for example, child abuse material without state authorities having specific obligations to support that action with investigations and prosecutions.

5.2.6 Cross-jurisdiction Issues

Digital platforms work in several Member States and have to face and comply with several jurisdictions. Some of the national laws they are asked to comply with fail to respect human rights law, especially when talking about online content restrictions.[237]

In addition, problems can arise in circumstances where the substantive law on a free speech issue, *e.g.* holocaust denial, differs from country to country across the EU. If a German national posts a Holocaust denial comment on the Facebook page of a British one, what law should apply? In practice, these difficulties are often solved by social media companies' application of their Terms and Conditions. Since companies tend to err on the side of caution, they often set lower free speech standards.

In this context, three issues main arise related to a) content which is illegal or criminal in the relevant jurisdictions; b) content that is illegal in some jurisdictions but not in others and; c) content that is illegal, but subject to different definitions in different jurisdictions.

---

236 Jorgensen et al. (2017:20).

237 See for example the German bill on Network Enforcement Law NetzDG: Maryant Fernández Pérez, 'EU action needed: German NetzDG draft threatens freedom of expression' (*EDRi*, 23 May 2017) <https://edri.org/eu-action-needed-german-netzdg-draft-threatens-freedomofexpression/> [accessed 1 November 2017]. Joe McNamee, 'German Social Media law – sharp criticism from leading legal expert', EDRi site (19 April 2017) <https://edri.org/german-social-media-law-sharp-criticism-from-leading-legal-expert/> [accessed 1 November 2017]; 'Germany: Draft Bill on Social Networks raises serious free expression concerns', (***Article 19***, 26 April 2017) <https://www.article19.org/resources.php/resource/38723/en/germany:-draft-bill-on-social-networks-raises-serious-free-expression-concerns> [accessed 1 November 2017].

a For content that is illegal in relevant jurisdictions, diligent procedures, as described above should be implemented. With regard to serious crimes, such as child abuse material, the obligations of all relevant parties, including states, should be clearly defined.

b For content that is subject to diverse implementations and definitions, efforts should be made, at least on an EU level, to adopt a more harmonised and predictable approach. The lack of harmonisation produced by the Framework Decision on combating various forms of racism and xenophobia is a good example of a problem that could be minimised with an appropriate amount of political will.[238]

c For content that is illegal in some jurisdictions, but not in others, a deeper reflection is needed on to respect principles of democracy and ECtHR case law.

5.3 Conclusion: A Suggested Way Forward

This paper argues that the European Commission should propose a new Directive that serves to bring activities in this area rigorously into line with the Charter of Fundamental Rights – especially with regard to predictability. This can provide more legal certainty and precision for the E-commerce Directive and the vertical legislation that has recently been proposed (such as the AVMSD[239] and the Copyright reform[240]) and "voluntary" frameworks that have resulted from undue political pressure.[241] The current framework is unclear and greatly interferes with fundamental rights and freedoms.[242] This approach was supported by a letter sent by 24 MEPs[243] to Vice-President Ansip recently and has been supported by the European Data Protection Supervisor (EDPS) already in 2012.

238 See Estelle De Marco (ed.), 'Mandola. Monitoring and Detecting Online Hate Speech Intermediate Report' (31 March 2016). <http://mandola-project.eu/m/filer_public/7b/8f/7b8f3f88-2270-47ed-8791-8fbfb320b755/mandola-d21.pdf> [accessed 1 November 2017].

239 See supra n. 204.

240 See supra n. 203.

241 By way of example, see supra n. 200.

242 See supra n. 202.

243 See Marietje Schaake et al., 'MEPs want notice and action directive' (9 May 2017) <https://marietjeschaake.eu/en/meps-want-notice-and-action-directive> [accessed 1 November 2017].

The guidance announced in the European Commission's background paper should result into a legislative proposal, based on a balanced, open consultation process and rigorous evidence-gathering. The Commission has produced several principles and guidance in this field.[244] There is also an urgent need to move away from a short-sighted obsession to "someone doing something" about one aspect of serious crimes (availability online) to taking a more meaningful approach to addressing the entire problem.

In order to fulfil with the European Commission's obligations under the Charter of Fundamental Rights, this paper recommends that any follow-up action incorporates the elements highlighted in section below.

5.3.1 General Requirements

- **Problem identification**: what are the public policy objectives that are being addressed by "voluntary" arrangements? Where are the review processes? What predictability is ensured by the process? Where is the accountability? Where are the correction mechanisms if the outcome proves to be suboptimal?
- **Solutions adapted to the problems identified: impact assessment needed**. The implications of, for example, terrorism and illegal hate speech are different. The implications of copyright infringements and child abuse material are different. The implicit logic of the DSM Communication that the political, legal and practical responses to these different problems can be identical strategies. There is not a one-fits-all solution. As stated by the EDPS,[245] not all categories of illegal content have the same weight. There are certain categories of illegal content that should be notified to data protection authorities (*e.g*. data processing infringement), others to law enforcement authorities (*e.g.* when criminal offences are involved, such as child pornography), *etc.*

244 See *e.g.* European Commission, 'Principles for Better Self- and Co-Regulation and Establishment of a Community of Practice', Press Release (11 February 2013) <https://ec.europa.eu/digital-single-market/en/news/principles-better-self-and-co-regulation-and-establishment-community-practice> [accessed 1 November 2017].

245 See *supra* n. 235.

- **Multistakeholder mapping:**
  - Identify a comprehensive scope for stakeholder involvement. It is current practice of the Commission to propose legislation[246] or codes of conduct[247] considering only an incomplete spectrum of interests, frequently benefiting big players rather than considering the views and issues faced by SMEs and citizens.
  - Specify what type of "digital platforms" the Directive would cover and the differences this implies. As stated above, we suggest five classifications of platforms (P) based on the relationship with consumer (C) or business (B) and based on the transactional nature of the relationship, as follows:
    - Transaction-based platform to consumer (P2C) platforms, such as Netflix or Spotify (content licensed to platform by rightsholder) (transactions on both sides of platform)
    - Non-transaction-based P2C (e.g. Google news and other news aggregators or review services, such as Yelp) (content freely available online, no P2B transaction) (no transaction on either side of platform)
    - Zero consumer value P2B services (promoted content on Twitter, etc) (transaction on business side of platform)
    - Transaction-based consumer/business to consumer (C2C & B2C) platform (Ebay, AirBnB (B2P & C2B transactions)
    - Non-transaction-based consumer to consumer (C2C) platform (UGC, blogging, micro-blogging, *etc.*)
  - Identify the relevant competent authorities dealing with diverse types of content and potential sanctions
- **Funding allocation**: identify which actors would need money to solve the problem, assessing progress and analysing the results

246 E.g. Joe McNamee, 'EU is now giving Google new monopolies to the detriment of European citizens and Internet companies' (*The European Sting*, 16 September 2016) <https://europeansting.com/2016/09/16/eu-is-giving-now-google-new-monopolies-to-the-detriment-of-european-citizens-and-internet-companies/> [accessed 1 November 2017].

247 E.g. *supra* n. 200.

- The promise of the better regulation agenda of "**well-targeted, evidence-based and simply written"**[248] legislation should finally be fulfilled in this policy area.
- **Fundamental rights focus**. For example, the Commission should aim at achieving full compliance of the principle of legality, thereby avoiding removal of legal content, not just "over-removal."
- **User focus**: usually, these discussions focus on the commercial and political implications.[249] Any action taken by the Commission on notice and action needs to have the user at its core.
- **(Illegal) content removal at source following a court order should be the preferred scheme**. Law enforcement authorities (*i.e.* administrative authorities), companies, trusted reporters (*e.g*. NGOs) or users cannot be arbiters of illegality or harm.
- When complementary mechanisms are in place, **safeguards** must be in place.
- Law enforcement agencies should not be able to issue **notice and take down requests** when do not have the power to do so, particularly if they do not assert that the content is illegal. If that power is attributed to LEAs, it should come with appropriate safeguards. Avoiding explicitly using the power to order the take down material means that the LEA is, deliberately or not, circumventing human rights safeguards.
- **Define the type of mechanism chosen**. As we have stated in the past,[250] practices such as "notice and stay down" or, in some circumstances, "notice and notice" do not appear to better protect fundamental rights than the "notice and take down" scheme. "Notice and stay down" implies in addition a monitoring obligation and algorithmic decision-making from Internet intermediaries, to ensure that the content does not appear elsewhere or reappear online. This is entirely unacceptable. "Notice and notice" is more

248 See Communication from the Commission to the European Parliament, the European Council and the Council 'Better Regulation: Delivering better results for a stronger Union', 14.9.2016, COM(2016) 615 final. <https://ec.europa.eu/info/sites/info/files/better-regulation-delivering-better-results-stronger-union_sept_2016_en.pdf> [accessed 1 November 2017].

249 See Paul Bernal, 'Self-regulation of internet intermediaries: public duty versus private responsibility', LSE Media Policy Project Blog (30 May 2017) <http://blogs.lse.ac.uk/mediapolicyproject/2017/05/30/self-regulation-of-internet-intermediaries-public-duty-versus-private-responsibility/> [accessed 1 November 2017].

250 See supra n. 229.

sympathetic to freedom of expression, since it does not involve any content removal by the Internet intermediary, can lead to a chilling effect, to an even greater extent than "notice and action."

If notice and action is chosen, this paper proposes that the Directive incorporates the requirements specified in the following section.

5.4.2 Specific Requirements

- **Quality criteria for notices**: there is evidence showing that companies receive notices which do not fulfil minimum quality criteria.
- **Counter-notice procedures**: it would be useful to agree on clear procedures to ensure due process. For instance, EDRi-member Bits of Freedom proposed a model back in 2012.[251] While the model fits better in cases of possible copyright infringement, it can serve of inspiration in other areas.
- **Third-party consultation mechanism:**
  - Publication of criteria and methodology. If we take the European Commission's Code of Conduct against Illegal Hate Speech as an example, we can see that the Commission states that a methodology was agreed, but the methodology under which organisations, including public bodies, send notices to the signatories of the Code has not been disclosed. Publishing it would enable accountability and would contribute to better legitimacy of the process.
  - Notice of allegedly illegal content only. In this respect, EDRi has received informal confirmation that some trusted reporters are referring legal content to companies that they do not believe to be illegal.
  - Lawyer-review requirement. It is important that the trusted flaggers or the authority referring the content are lawyers specialised in the matter at hand. This will not solve all the issues, but will bring better safeguards for fundamental rights, including freedom of expression and opinion.

251 See Janneke Sloëtjes, 'Questionnaire on procedures for notifying and acting on illegal content hosted by online intermediaries', (Bits of Freedom, 4 September 2012) <https://bof.nl/wp-content/uploads/040912-response-to-consultation-BitsofFreedom-def-includingannexes.pdf> [accessed 1 November 2017].

- Interaction between the trusted reporter and companies and public authorities needs to be defined.
- Independent oversight, in particular to ensure due process and predictability.
- Automatic reporting to public authorities in serious cases (criminal offences), with state authorities obliged to be transparent with regard to their subsequent enforcement measures.

- **The right to remedy and a fair, independent and accessible dispute resolution system, considering:**
  - Due process
  - Establishment of minimum requirements for predictability
- **Counterproductive effects assessment**. What are unintended consequences for fundamental rights when restricting online content? What are the possible counterproductive effects for the public policy objective being pursued? How durable is the process? What are the rights and freedoms concerned? Is the process sufficiently flexible to adapt to countermeasures being taken by criminals in order to circumvent the measures being taken?
- **Transparency reporting obligations for all parties involved**, *e.g.* companies, NGOs, public authorities, including the European Commission.
  - Reports must be timely and transparent and include accurate, thorough, consistent and comparable statistics over time. Stopline.at provides a good example of best practice with regards to consistency.[252]
  - Reporting must be clear, consistent. Minimum requirements should be put forward.
  - Follow-up with national authorities is needed.
  - We suggest the Commission to assess consumer contract law (including unfair contract terms) and the provisions related to transparency reporting. If the current instruments are not serving their purpose, they should be reformed.

252 See <https://www.stopline.at/ueberuns/statistiken/> [accessed 1 November 2017].

- **Independent oversight.**
  - Monitoring and enforcement of the Directive must be inclusive and transparent. For example, the EU Code of Conduct on Hate Speech monitoring would not comply with this requirement.
  - Development of a methodology in a transparent and inclusive way, including different actors, such as digital rights organisations;
  - Set specific deadlines and key performance indicators;
  - A thorough, credible human rights and fundamental freedoms assessment after two years (with the deadline being rigorously respected, unlike, for example, in the case of the Data Retention Directive). *E.g*. Something similar as what has been proposed in the Terrorism Directive, but in a shorter time frame.

As emphasised above, this paper is based on EDRi's initial comments to the questions asked by the European Commission in preparation for its Workshop on Fundamental Rights and Digital Platforms that took place on 12 June 2017. There are other relevant questions that are worth discussing in relation to digital platforms, such as the meaningful solutions that the EU policy-makers are ready to consider or the legal opinion of the European Commission about the German law on Enforcement on Social Networks "NetzDG". This is work in progress and this paper should be seen as a concrete example of the authors' commitment to keep working to achieve a better situation than the current one.

5.5 Bibliography

Anderson J, et al. (2016). 'UNFRIENDING CENSORSHIP. Insights from four months of crowdsourced data on social media censorship', Onlinecensorship.org (31 March 2016). <https://s3-us-west1.amazonaws.com/onlinecensorship/posts/pdfs/000/000/044/original/Onlinecensorship.org_Report_-_31_March_2016.pdf?1459452553> [accessed 1 November 2017].

Article 29 Data Protection Working Party, 'Working document on data protection issues related to intellectual property rights', WP 104 (18 January 2005). <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2005/wp104_en.pdf> [accessed 1 November 2017].

Bernal P (2017). 'Self-regulation of internet intermediaries: public duty versus private responsibility', LSE Media Policy Project Blog (30 May 2017) <http://blogs.lse.ac.uk/mediapolicyproject/2017/05/30/self-regulation-of-internet-intermediaries-public-duty-versus-private-responsibility/> [accessed 1 November 2017].

Bits of Freedom, 'Overgeleverd Aan Willekeur' (*Bits of Freedom,* 2012) <https://bof.nl/wp-content/uploads/20120401-overgeleverd-aan-willekeur-rapport.pdf> [accessed 1 November 2017].

Center for Technology and Society at Fundação Getulio Vargas (2016). 'Terms of Service and Human Rights: An Analysis of Platform Contracts' (Recavan Press, 2016) <http://tinyurl.com/toshr> [accessed 1 November 2017].

EDRi, EDRi submission to UN Special Rapporteur David Kaye's call on freedom of expression and the private sector in the digital age <https://edri.org/ les/privatisedenf/DavidKaye_callICT_EDRi.pdf> [accessed 1 November 2017].

EDRi, EDRi-gram newsletter - Number 10.18 (26 September 2012) <http://history.edri.org/edrigram/number10.18> [accessed 1 November 2017].

EDRi, 'Human Rights and privatised law enforcement' (February 2014) <https://edri.org/wp-content/uploads/2014/02/EDRi_HumanRights_and_PrivLaw_web.pdf> [accessed 1 November 2017].

EDRi, 'The Code. Effective Open Voluntarism: Good design principles for self- and coregulation and other multistakeholder actions', Draft (May 2012) <https://edri.org/files/EC_code_final.pdf> [accessed 1 November 2017] .

EDRi, 'The slide from "self-regulation" to corporate censorship', EDRi Discussion Paper (January 2011) <https://edri.org/wp-content/uploads/2010/01/selfregualation_paper_20110925_web.pdf> [accessed 1 November 2017].

European Commission, 'Principles for Better Self- and Co-Regulation and Establishment of a Community of Practice' (February 2013) <https://ec.europa.eu/digital-single-market/en/news/principles-better-self-and-co-regulation-and-establishment-community-practice> [accessed 1 November 2017].

European Commission, 'Summary of the results of the Public Consultation on the future of electronic commerce in the Internal Market and the implementation of the Directive on electronic commerce' (2000/31/EC) (2010) <http://ec.europa.eu/internal_market/consultations/docs/2010/e-commerce/summary_report_en.pdf>[accessed 1 November 2017].

European Data Protection Supervisor, 'Opinion of the European Data Protection Supervisor on the current negotiations by the European Union of an Anti-Counterfeiting Trade Agreement' (2010) <https://edps.europa.eu/sites/edp/files/publication/10-02-22_acta_en.pdf> [accessed 1 November 2017].

European Data Protection Supervisor, 'EDPS formal comments on DG MARKT's public consultation on procedures for notifying and acting on illegal content hosted by online intermediaries' (2013) <https://edps.europa.eu/sites/edp/files/publication/12-09-13_comments_dg_markt_en.pdf> [accessed 1 November 2017].

Jorgensen R F (2017). 'Framing human rights: exploring storytelling within internet companies' (2017) Information, Communication & Society,1-16 (REP1).

Jorgensen R F, Moller Pedersen A, Benedek W and Nindler R (2017). 'Case Study on ICT and Human Rights (Policies of EU), Fostering Human Rights among European Policies', Large-Scale FP7 Collaborative Project GA No. 320000, European Commission (REP2).

Jourová V, 'Code of Conduct on countering illegal hate speech online: First results on implementation' (December 2016). Factsheet <http://ec.europa.eu/information_society/newsroom/image/document/2016-50/factsheet-code-conduct-8_40573.pdf> [accessed 1 November 2017].

Jourová V, 'Code of Conduct–Illegal online hate speech. Questions and answers' (2016) <http://ec.europa.eu/justice/fundamental-rights/files/code_of_conduct_hate_speech_en.pdf> [accessed 1 November 2017].

McNamee J, 'Internet Blocking', EDRi Booklet (September 2010) <https://edri.org/files/blocking_booklet.pdf> [accessed 1 November 2017].

Mivoca S B (2017). 'Key issues in the AVMSD revision debates: Video-sharing platforms and regulator independence', *CERRE Issue Paper* (17 March 2017) <http://www.cerre.eu/sites/cerre/files/170322_CERRE_AVMSRevision_IssuePaper_final.pdf> [accessed 1 November 2017].

Nas S, 'The Multatuli Project. ISP Notice & take down' (*Bits of Freedom*, 1 October 2004) <https://www-old.bof.nl/docs/researchpaperSANE.pdf> [accessed 1 November 2017].

Sloëtjes J, 'Unpredictable and unclear: Hosting policy removal policy' (*Bits of Freedom*, 21 December 2012) https://bof.nl/2012/12/21/onvoorspelbaar-en-onduidelijk-het-verwijderingsbeleid-van-hostingproviders/ [accessed 1 November 2017].

Sloëtjes J, 'Questionnaire on procedures for notifying and acting on illegal content hosted by online intermediaries' (*Bits of Freedom*, 4 September 2012) <https://bof.nl/wp-content/uploads/040912-response-to-consultation-BitsofFreedom-def-includingannexes.pdf> [accessed 1 November 2017].

PART II

Data Governance

6 Hiding in Plain Sight: Right to be Forgotten and Search Engines in the Context of International Data Protection Frameworks

Krzysztof Garstka **and** ***David Erdos***

Abstract

In the wake of the Google Spain (2014) and debate on the "right to be forgotten", now included in the new General Data Protection Regulation (GDPR), it has become widely recognised that data protection law within the EU/EEA grants individuals a qualified right to have personal data relating to them deindexed from search engines. At the same time, however, this outcome has at times been conceptualised as a uniquely EU/EEA phenomena, perhaps even resulting from one idiosyncratic CJEU judgment. This paper questions such a conceptualisation. Through an analysis of five major extra-EU/EEA international data protection instruments, it argues that most of these could on a reasonable interpretation be read as supporting a Google Spain-like result. Further, and in light of the serious threats faced by individuals as a result of the public processing of data relating to them, it argues that the time is ripe for a broader process of international discussion and consensus-building on the "right to be forgotten". Such an exercise should not be limited to generalised search engines (which undoubtedly raise some uniquely challenging interpretative conundrums within data protection), but should also encompass other actors including social networking sites, video-sharing platforms and rating websites.

6.1 Introduction

For the online platform operators, one of the most critical and growing challenges is how to navigate in the maze of obligations various jurisdictions place on them in the field of online content regulation. The bigger an online platform is, the more likely it is to encounter situations where one jurisdiction requires them, for example, to take a certain type of content down, in a specific period of time, after a defined assessment of legality; while another jurisdiction places a different set of requirements on the platform

or may even grant it a complete immunity from such obligations. This fissiparous situation is not helped by the fact that it is difficult to specify a perfectly clear set of online content regulation requirements even within particular and comparatively mature legal frameworks. Moreover, in the area of data protection, such inconsistency and uncertainty is liable to seriously detract from efforts to ameliorate the very serious threats to individual's privacy and other rights that can emanate from the public processing of personal data relating to them online.

When the Court of Justice of the European Union (CJEU) handed down its decision in Case C-131/12 *Google Spain*,[253] mandating that conditional, nominative deindexing on the basis of the EU's data protection laws, some perceived it as an isolated extension of this branch of law-making, an embodiment of the right to be forgotten that is limited to the EU and the Google Search engine.[254] This paper seeks to challenge such perceptions by exploring whether other international data protection frameworks could potentially support legal interpretations (within the non-EU/EEA jurisdictions) which would place the operators of online search engines under *Google Spain*-like obligations. Realising the extent to which this could be possible is one of the key initial steps of regulatory initiatives aimed at ameliorating the maze of obligations described in the introductory paragraph, as well as providing genuine and effective protection for data subjects within a fast changing and ever more globalised environment.

In order to achieve its aims, the paper embraces the following structure. Section two starts by introducing and clarifying the concept of the right to be forgotten, which in recent years was oftentimes narrowly construed as describing a specific legal right, as opposed to a broader principle and valid regulatory aim. Section three outlines the CJEU decision in *Google Spain* and extracts from it the two key elements of legal interpretation which

253 Case C-131/12, *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González*, ECLI:EU:C:2014:317.

254 See, e.g., Danny Sullivan, 'How Google's New "Right To Be Forgotten" Form Works: An Explainer' (*SearchEngineLand*, 30 May 2014) <http://searchengineland.com/google-right-to-be-forgotten-form-192837>, or the Wikipedia entry <https://en.wikipedia.org/wiki/Right_to_be_forgotten>, which identifies the right to be forgotten as a mainly EU/Argentinian phenomenon. [accessed 26 September 2017].

led to the establishment of a specific takedown regime. Section four moves onward to explore the presence and character of those two elements within a selected set of international data protection frameworks.[255] Finally, section five concludes by outlining the resulting panorama of international regulation in the studied area and proposing a path towards a suitable, international initiative in this field.

6.2 Right to Be Forgotten: Misguided Label or Useful Principle?

One of the key needs of an effective and fruitful debate on the emerging branches of law is the presence of precise terms which can then help to undergird regulatory will in a clear and unequivocal manner. Unfortunately, looking back at the last three years of the debate surrounding the right to be forgotten, it is difficult to point at this right as achieving this desirable outcome. The term "right to be forgotten" came to be used for multiple ends; among them to describe a specific, enforceable legal right, as well as the broader, socio-philosophical concept underlying this and related rights. Furthermore, the discussed term was often conjoined with the multiple other terms, with the aim of clarifying its meaning(s). Hence, it is worth starting by exploring these definitional aspects, so that the use of the term in this paper is clear and visibly justified.

Unsurprisingly, the majority of the conceptual debate outlined above took place after the *Google Spain* decision. The term "right to be forgotten" became a buzzword, one often used in the public media and general debates to (mistakenly) claim that the CJEU created a new, unequivocal right for personal data to be removed from the Internet, period.[256] It is perhaps this development which prompted some scholars, like Lynskey, to criticise the use of the term "right to be forgotten" and suggest that it should be abandoned.[257] Others – like Gryffroy - argued that the term in

255 For a broad and interesting study of the right to be forgotten's presence in national frameworks, see Voss & Castets-Renard (2016).

256 See Moran (2014). 'Things to remember about Google and the right to be forgotten' (*The Guardian*, 03 July 2014), <https://www.theguardian.com/technology/2014/jul/03/google-remember-right-to-be-forgotten> [accessed 26 September 2017].

257 Lynskey (2015).

question denotes the right to remove the content at its source, while the CJEU established a "right to delist", focused on the removal of indexing information.[258]

Moving onwards, Ambrose and Ausloos suggested that the right to be forgotten came to be an umbrella term for the right to oblivion (grounded in the right to privacy and the tradition of *droit à l'oubli*, a right based on the individual's desire to hide certain information from the public eye)[259] and the right to erasure (a more "mechanical" right, focused - according to the cited writers - on the removal of passively disclosed data).[260] Finally, the controversy and complexity of the discussed term is perfectly visible in the very text of the EU General Data Protection Regulation (GDPR),[261] which labels one of its provisions (article 17) as the "right to erasure", with the sub-label "right to be forgotten" added right after, in timid brackets, a witness to many years of rather tortured discussion.[262]

Against this background, the following approach is adopted in this paper. The term "right to be forgotten" is not abandoned, as it has become a lodestar for a regulatory and philosophical goals which may be thought to underline many aspects of data protection law, including fair processing and data limitation in particular over time. However, the term is interpreted not as a specific legal right, but as a concept permeating a number of specific legal rights and provisions, which is further not tied specifically to search engines or to a single judgement of the CJEU. Seen in this manner, the right to be forgotten denotes the idea that individuals should be able to restrict access to information identifying them (in order to prevent actual or potential damage), provided there are no overriding, legitimate reasons to oppose such a removal. The

258 Gryffroy (2016:150).

259 Ambrose & Ausloos (2013:14).

260 See Ambrose & Ausloos.

261 Regulation (EU) 2016/679 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 and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) <http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=FR> [accessed 26 September 2017].

262 For further discussion of the taxonomy surrounding the term "right to be forgotten", see Voss & Castets-Renard (2016:284).

drive to achieve this is especially aimed at preventing, as Mayer-Schönberger described it, the world filled with "lives shattered (or at least dented) by perfect recall of trivial past deeds", by a "strangely unforgiving public."[263]

6.3 The CJEU Decision in *Google Spain*

Taking on board this understanding of the right to be forgotten, the paper can proceed to the analysis of the legal reasoning behind *Google Spain*. This preliminary reference to the CJEU came from Spain, and centred around the question of whether search results appearing on Google's search engine as a result of typing in an individual's name and leading to content containing personal data, can be ordered to be removed on the basis of the right to erasure (art. 12 (b)) and the right to objection (art. 14(a)) of the Data Protection Directive,[264] even if the content in question was lawfully published.[265] The claimant on behalf of whom the Spanish data protection authority demanded the removal of such indexing information was a man whose home repossession notice (drawn for non-payment of social security) from over ten years previously kept appearing in Google's search results (tied to the claimant's name), as a part of an official notice still found in an online version of the La Vanguardia newspaper.

The Court answered the referred question affirmatively, stating that "the operator of a search engine is obliged to remove from the list of results displayed following a search made on the basis of a person's name links to web pages, published by third parties and containing information relating to that person, also in a case where that name or information is not erased beforehand or simultaneously from those web pages, and even, as the case may be, when its publication in itself on those pages is lawful".[266]

263 Mayer-Schönberger (2009:197).

264 Directive 95/46/EC of the European Parliament and of the Council 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.

265 Case C-131/12, *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González*, ECLI:EU:C:2014:317, at [20].

266 Case C-131/12, Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González, ECLI:EU:C:2014:317, at [88].

A specific set of legal elements had to be present in order for the Court to reach this decision. While the judgement is a complex one, for the purposes of this paper, the focus will result on two key elements enabling the described outcome – the presence of *ex post* rights implementing the concept of the right to be forgotten, as well as a suitably formed and interpreted definition of a data controller. They are described in the following paragraphs, in the form they took in the Data Protection Directive (binding at the time of the judgement; hereafter referred to as the DPD); without dismissing the importance of the EU General Data Protection Regulation (GDPR), which will replace the Data Protection Directive on the 25th May 2018.

6.3.1 Presence of a Right Implementing the Concept of the Right to Be Forgotten

In *Google Spain*, the CJEU relied primarily on both art. 12(b) of the DPD (right to erasure), which states that "Member States shall guarantee every data subject the right to obtain from the controller (…) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data" and art. 14(b) (the right to object) which enables the data subject (at least when processing is based on the legitimate interests of the controller) to "object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him … Where there is a justified objection, the processing instigated by the controller may no longer involve those data".[267]

Each of these provisions are replicated in modified form in the new GDPR. Thus, the former finds a mirror in art. 17(1), which provides that under specified circumstances, "the data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall

267 The Court was also inspired by the inclusion of data protection, as well as the more traditional right to respect for private life, in articles 8 and 7 of the *EU Charter of Fundamental Rights*. Nevertheless, the ultimate rationale for the Court's findings were firmly based on the codified secondary legislation of the DPD. Given this, it is notable that even Google has taken *Google Spain* to be binding in the three associated European Economic Area (EEA) jurisdictions of Iceland, Liechtenstein and Norway, which are subject to the DPD but not formally to the *EU Charter*.

have the obligation to erase personal data without undue delay". Meanwhile, the latter is reflected in art. 21 which, with a similar scope to art. 14(b), states that once a subject has objected "on grounds relating to his or her particular situation", it will be for the controller to demonstrate "compelling legitimate grounds for the processing" or to cease such activity.

6.3.2 Search Engine as the Data Controller

The definition of a data controller was one of the key interpretative challenges in the *Google Spain* judgement. The definition in question is laid out in art. 2(d) of the DPD, which states that the term "controller" denotes "the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data (…)". "Personal data" is defined as "any information relating to an identifiable or identifiable natural person (data subject)" (art. 2 (a)), whilst "processing" refers to "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as *collection*, *recording*, *organization*, *storage*, *adaptation* or *alteration*, *retrieval*, *consultation*, *use*, *disclosure by transmission*, *dissemination* or otherwise *making available*, *alignment* or *combination*, *blocking*, *erasure* or *destruction*" (art. 2(b)).[268]

The CJEU started by considering whether nominative indexing by a search engine ought to be classified as processing of personal data. After referring to its earlier judgement in *Lindqvist269* (which stated that loading personal data on an unstructured webpage counts as such processing[270]), the Court answered this question affirmatively, and its justification is, given the scope of this paper, worthy of being cited in full. It was found that "in exploring the Internet automatically, constantly and systematically in search of the information which is published there, the operator of a search engine *'collects'* such data which it subsequently *'retrieves'*, *'records'* and *'organises'* within the framework of its indexing programmes, *'stores'* on its servers and,

268 Emphasis added.

269 Case C-101/01 *Bodil Lindqvist* [2003].

270 See Case C-101/01 *Bodil Lindqvist* [2003], at [25].

as the case may be, *'discloses'* and *'makes available'* to its users in the form of lists of search results."[271]

Following this finding, the CJEU approached the issue of whether the operator of a search engine can be seen as the data controller of the described processing of personal data. The Court found affirmatively in relation to this question as well,[272] an answer which remained unaffected by the operator's lack of control over the source platforms,[273] the fact that operators of the said platforms may have the option of setting up their websites so that they are not indexed by Google Search [274] and the fact that the search engine may not distinguish between "personal data" and "other types of information".[275] In sum, it emphasised that it was the search engine itself which was determining both the "purposes and means" of its own services and, as such, it fell within the "clear wording" of the term "controller".[276] Furthermore, in relation to nominative indexing specifically, the judgment emphasised that search engines play "a decisive role in the overall dissemination"[277] of personal data and also provide "a structured overview of the information relating to that individual".[278] Therefore, unless search engines were caught by this term, data protection's core purposes of ensuring "effective and complete protection of data subject" would be contradicted.[279]

6.4 Search Engine-oriented Right to Be Forgotten within the Non-EU International Data Protection Frameworks

The full exegesis of the legal "right to be forgotten" applied to search engines within EU/EEA data protection law is a matter of profound complexity. Indeed, this issue is returning to the CJEU with a new reference,[280] and Member States' courts are still in the

271 See Case C-131/12 *Google Spain v Gonzalez* [2014], at [28], (emphasis added).

272 See Case C-131/12 *Google Spain v Gonzalez* [2014], at [33].

273 See Case C-131/12 *Google Spain v Gonzalez* [2014], at [34].

274 See Case C-131/12 *Google Spain v Gonzalez* [2014], at [39].

275 See Case C-131/12 *Google Spain v Gonzalez* [2014], at [28].

276 See Case C-131/12 *Google Spain v Gonzalez* [2014], at [33]-[34].

277 See Case C-131/12 *Google Spain v Gonzalez* [2014], at [36].

278 See Case C-131/12 *Google Spain v Gonzalez* [2014], at [37].

279 See Case C-131/12 *Google Spain v Gonzalez* [2014], at [34].

280 See Conseil d'État, 'Right to be delisted' (*Conseil d'État*, 24 February 2017) <http://english.conseil-etat.fr/Activities/Press-releases/Right-to-be-delisted> [accessed 26 September 2017].

process of developing cohesive guidance on the scope of the rights which can be claimed in *Google Spain*-type situations[281] and when should such claims give way to the public interest in maintaining access to the contested information. Nevertheless (as it was earlier mentioned), for the purposes of this exploratory, time and space-limited paper, two discrete yet core elements of the EU/EEA legal framework as interpreted in *Google Spain* will be focused upon and compared with other international instruments.

Firstly, the presence of a specific, *ex post* right to stop publication-related processing which violates core data protection principles, at least if there is no continuing public interest in this processing. Secondly, the presence of a data controller concept, which could be interpreted to encompass search engines' nominative indexing of personal data on the web. They are the central pillars of the outcome which emerged from the CJEU decision and hence, it is sensible to start by looking for their presence or absence in other international data protection frameworks.

6.4.1 Convention 108 – Council of Europe (CoE)

Council of Europe's Data Protection Convention (No. 108)[282] was, as Greenleaf notes, the first binding international data privacy agreement at the time of its introduction in 1981.[283] Since then, the Convention has been supplemented with an additional protocol in 2001,[284] agreed in order to achieve greater consistency between the Convention and the latter provisions of the DPD. In any case,

281 The Court in *Google Spain* only obliquely considered the important questions of whether a search engine's responsibilities were confined to *ex post* measures and whether deindexing could be demanded other than in relation to nominative searches. In sum, it stated at para. 38 that such a search engine would (at the very least) acquire controller duties when it was "liable to affect significantly, and additionally compared with that of publishers of websites, the fundamental rights to privacy and to the protection of personal data" and that it "must ensure, within the framework of its responsibilities, powers and capabilities" that substantive data protection guarantees were safeguarded. The reasoning of this paragraph undoubtedly requires further specification and raises many questions including, most notably, the relationship between data protection and the general framework for e-commerce. Given that this paper focuses only on the core holding of *Google Spain*, consideration of these difficulties including in relation to the other international instruments lies largely outside its scope.

282 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981) Council of Europe, European Treaty Series – No. 108.

283 Greenleaf (2012:2).

284 Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows (2001) Council of Europe, European Treaty Series – No. 181.

out of the instruments explored in this paper, the CoE's Convention is most likely the closest one to the DPD and the GDPR, both geographically and spiritually; indeed, the DPD acknowledges this directly by stating that it aims to "give substance to, and amplify" the principles found in the Convention.[285] Nevertheless, the Convention does not possess the depth and level of prescriptiveness existing in the Directive, let alone the Regulation. This might, however, change somewhat should the currently ongoing revision of the Convention come to fruition.[286]

Within the CoE's DP Convention, the closest provision to the DPD's rights to erasure and objection is art. 8(c) which states that "any person shall be enabled (…) to obtain, as the case may be, rectification or erasure of such data if these have been processed contrary to the provisions of domestic law giving effect to the basic principles set out in Articles 5 and 6 of this Convention." While the indicated basic principles largely reflect those found in both the Directive and the Regulation, it is beyond the scope of this paper to compare those principles in depth. What can be said, however, is that similarly to the EU/EEA regime, Convention 108 does set out an *ex post* right to *remove* content on the basis of its incompatibility with the data protection law, including its core principles.

Regarding the definition of the data controller, the Convention currently uses the term "controller of the file", which by virtue of art. 2(d) denotes "the natural or legal person, public authority, agency or any other body who is competent according to the national law to decide what should be the purpose of the automated data file, which categories of personal data should be stored and which operations should be applied to them". An automated data file is meant to indicate "any set of data undergoing automatic processing",[287] and automatic processing "includes the following operations if carried out in whole or in part by automated means: storage of data,

285 See Directive 95/46/EC of the European Parliament and of the Council 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, rec. 11.

286 See <https://www.coe.int/en/web/data-protection/modernisation-convention108> [accessed 1 November 2017].

287 See Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981) Council of Europe, European Treaty Series – No. 108, art. 2(b).

carrying out of logical and/or arithmetical operations on those data, their alteration, erasure, retrieval or dissemination".[288]

Looking back to the CJEU decision, it seems clear that search engines' indexing does fall within the concept of "automatic processing". The act of "storing" is present in both frameworks' definitions of processing - and "carrying out of logical and/or arithmetical operations" can very well be understood to encompass retrieving, recording and organising of data (terms which also appeared in the CJEU's judgement). Finally, "dissemination" present in art. 2 of the Convention 108, can also be seen as synonymous to the acts of disclosure and making available.

As for the definition of the "controller of the file" aka data controller, the DPD's reference to determining "the purposes and means of processing" can be seen as reflected directly in Convention's matching reference to deciding on the purposes of processing, as well as in the indirect, yet very strong correlation between deciding on the "means of processing" and on "operations (which) should be applied" to personal data. Moreover, since a private search engine necessarily does maintain control over its own indexing operations and so must be judged "competent according to national law" to do so, the CoE DP Convention would appear very able to accommodate the two key pillars of the *Google Spain* judgement.

6.4.2 Privacy Guidelines – Organisation for Economic Cooperation and Development (OECD)

The Organisation for Economic Cooperation and Development was established in 1961 and comprises of thirty-five members, namely Australia, Austria, Belgium, Canada, Chile, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Israel, Italy, Japan, Korea, Latvia, Luxembourg, Mexico, Netherlands, New Zealand, Norway, Poland, Portugal, Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, UK, and USA.

The key OECD instrument of interest for this paper are the Guidelines Governing the Protection of Privacy and Transborder

288 See Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981) Council of Europe, European Treaty Series – No. 108, art. 1(c).

Flows of Personal Data (Privacy Guidelines), which appeared first in 1980 (after being developed alongside the Council of Europe's Convention 108), and were subject to limited revisions in 2013.[289] The Guidelines took the form of a Recommendation of the Council and as such, are not a binding legal instrument like the Convention 108, let alone the DPD or the directly applicable GDPR. On the other hand, they reach out across multiple continents, and as such, deserve this paper's attention.

The key right of interest in the Guidelines is present in art. 13(d), which states that "(i)ndividuals should have the right (...) to challenge data relating to them and, if the challenge is successful to have the data erased, rectified, completed or amended." While the possibility of data's erasure is reminiscent of the provision which stood behind *Google Spain*, the right present in the Guidelines is very timid when it comes to explaining what can be the basis of the challenge, and under what circumstances would a challenge be successful and trigger erasure. A certain indication lies, however in art. 14 of the Guidelines, which provides that "a data controller should be accountable for complying with measures which give effect to the principles stated above". The location of processing which does not comply with the indicated principles (and is not subject to a justified exception[290]) seems sufficient to make an art.13(d) challenge successful. Consequently, it can be stated that the Guidelines do possess a specific right which, under at least a plausible interpretation, could form the basis of a *Google Spain*-like implementation of the right to be forgotten.

Moving onto the second studied element, that is whether a search engine could be classified as a data controller, we encounter art. 1(a), which defines the latter as one "who, according to national law, is competent to decide about the contents and use of personal data regardless of whether or not such data are *collected*, *stored*, *processed* or *disseminated* by that party or by an agent on its

289 OECD, Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (1980), C(80)58/FINAL, as amended on 11 July 2013 by C(2013)79].

290 See Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (1980) OECD, C(80)58/FINAL, as amended on 11 July 2013 by C(2013)79], art. 3.

behalf".[291] In this instrument, the definitions of a data controller and data processing are collated into the cited provision.

When comparing the activities listed in art. 1(a) of the Guidelines with those from art. 2(b) of the DPD which the CJEU relied on, similarities arise. Collection and storage appear expressly in both art. 1(a) and the CJEU judgement, while processing is reflected indirectly in retrieval, recording and organisation of data. Additionally, "dissemination" present in art. 1(a) is – just as in the case of Convention 108 – indirectly reflected in the acts of disclosure and making available. Consequently, it seems that the Guidelines' definition of data processing would be perfectly capable of accommodating the activity of a search engine.

As for the definition of a data controller, it is not limited to the mere function of deciding on the means and purposes of data processing, it requires the party to be "according to national law (…) *competent* to decide about the *contents* and *use* of personal data".[292] As regards competency in national law, for similar reasons to the CoE Convention discussed above, it would seem necessarily the case that a private search engine will ordinarily be legally competent over its own processing. On the other hand, "contents and use" appears at first sight rather different than the DPD's "means and purposes". Search engines do exercise decision-making over "the contents" of personal data on their service but this is clearly limited.[293] However, by deciding to collect, retrieve, store and disclose information, they could very well be judged to have exercised decision-making over the *use* of all information within the service. Hence, if the CJEU's finding that it does not matter whether the search engine was choosing to index personal data specifically was to be maintained, *Google Spain*'s core holdings could be manifested within the OECD Guidelines as well – though in a less straight-forward manner than in the case of Convention 108.

291 See Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (1980) OECD, C(80)58/FINAL, as amended on 11 July 2013 by C(2013)79], art. 1(a).

292 Emphasis added.

293 For example, search engines may remove manifestly problematic content, such as child pornography or which is aimed at the perpetration of fraud.

6.4.3 Privacy Framework - Asia-Pacific Economic Cooperation (APEC)

The Asia-Pacific Economic Cooperation (APEC) was established in 1989 and contains twenty-one members, namely Australia, Brunei Darussalam, Canada, Chile, People's Republic of China, Hong Kong, Indonesia, Japan, Republic of Korea, Malaysia, Mexico, New Zealand, Papua New Guinea, Peru, Philippines, Russia, Singapore, Chinese Taipei, Thailand, USA, and Vietnam.

In 2005, the countries of this organisation signed the APEC Privacy Framework, a non-binding agreement which became dubbed "OECD-lite", due in part to its conceptual and express references to the OECD Guidelines. Indeed, para. 5 of the Framework's preamble states that it "is consistent with the core values of the OECD's 1980 Guidelines on the Protection of Privacy and Trans-Border Flows of Personal Data". Nevertheless, the Framework (which was updated in 2016[294]) can be seen as a notable agreement on its own – for example, in Greenleaf's paper from 2012, the Framework was described as the "only significant international attempt to break the influence of the EU Directive".[295]

The closest specific right to that on which the decision in *Google Spain* was based can be found in para. 23 of the Framework, which states that "individuals should be able to: (...) challenge the accuracy of information relating to them and, if possible and as appropriate, have the information rectified, completed, amended or deleted." As it can be seen, despite the possibility of erasure, this is a more modest emanation of the right to be forgotten, one much more focused on the notion of accuracy than granting an independent right to remove personal data due to the potential or actual harm it may cause.

While the right from paragraph 23 would be able to accommodate the removal of personal data which appeared online in an incorrect form, it does not seem to be suitable for the removal of even some of the most egregious types of personal data, such as *e.g.* revenge pornography. However, even if an express subjective right to prevent or limit processing is absent, the Framework as a whole tends to replicate most of the core data protection principles found

294 Updates to the APEC Privacy Framework (2016) APEC, 2016/CSOM/012app17.

295 See Greenleaf (2012).

in the DPD and the Regulation. Further, para. 38 requires APEC members to ensure that their "systems of privacy protections" include "an appropriate array of remedies for privacy protection violations". It may be, therefore, that the basic substantive duties coupled with this broad remedial principle point to an implicit broader right for the data subjects.

In any case, there is still analytical value in considering the Framework's definition of the data controller. Para. 10 of this instrument states that "(p)ersonal information controller means a person or organization who controls the collection, holding, processing or use of personal information (...)". Without a competency factor present in the CoE Convention or OECD Guidelines, holding control over the collection, holding (which could be read as storage), processing or use, provides a definition sufficiently proximate to the one on which the CJEU relied on. However, the fact remains that in order for a *Google Spain*-like interpretation of the Framework to appear, a specific right - independent of the notion of accuracy - would have to be established first.

6.4.4 Supplementary Act on Personal Data Protection – Economic Community of West African States (ECOWAS)

The Economic Community of West African States (ECOWAS) was created in 1975, and fosters cooperation between the countries of the region, namely Benin, Burkina Faso, Cape Verde, Cote d' Ivoire, The Gambia, Ghana, Guinea, Guinea Bissau, Liberia, Mali, Niger, Nigeria, Sierra Leone, Senegal and Togo.

The key instrument of ECOWAS which is of interest to this paper is the Supplementary Act on Personal Data Protection, adopted in 2010.[296] In contrast to the OECD Guidelines and APEC Framework, the Supplementary Act is a binding legal agreement; though its mechanisms for enforcement lag far behind the EU DPD and, still less, the GDPR.

The Supplementary Act includes a cognate to both the DPD's rights to objection and erasure. Thus, under art. 40 (right to object) an individual "is entitled, for legitimate reasons, to object to processing of personal data of which he is the data subject". Meanwhile, as

296 Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS (2010) ECOWAS.

per art. 41 (right to rectification and destruction) if personal data is "inaccurate, incomplete, questionable, outdated or prohibited from collection, use, disclosure or preservation", the data subject has the right to request from the data controller that such data be "rectified, supplemented, updated, blocked or destroyed, as appropriate." Both these rights appear broadly defined. Thus, the concept of raising objection for "legitimate reasons", as well as erasure/destruction of data which is outdated or prohibited from collection, use, disclosure or preservation, do both severally and cumulatively add up to a default subjective right to stop processing which is incompatible with the core data protection principles.

As for the definition of a data controller, it can be found in art. 1 of the Supplementary Act, which states that the concept in question "means any public or private individual or legal entity, body or association who, alone or jointly with others, *decides* to *collect and process personal data* and determines the purposes for which such data are processed".[297] The concept of processing is defined extremely broadly within the same article as "any operation or set of operations carried out or not, with the assistance of processes that may or may not be automated, and applied to data, such as *obtaining*, *using*, *recording*, *organisation*, *preservation*, *adaptation*, *alteration*, *retrieval*, *saving*, *copying*, *consultation*, *utilisation*, *disclosure by transmission*, *dissemination* or *otherwise making available*, *alignment* or *combination*, as well as *blocking*, *encryption*, *erasure* or *destruction* of personal data."[298]

Against this list of activities, the CJEU could have produced an at least as convincing finding of search engine activities falling within the concept of data processing as in the *Google Spain*, drawing on terms such as "alignment" or "combination". As for the definition of the data controller, if the phrase "decides to collect and process personal data" is interpreted as accommodating a situation where a party decides to collect and process both personal and non-personal data indiscriminately, then the ECOWAS framework would be primed for the interpretation of the law akin to that set out in *Google Spain*.

297 Emphasis added.

298 See Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS (2010) ECOWAS, art. 1.

6.4.5 Framework on Personal Data Protection - Association of Southeast Asian Nations (ASEAN)

The Association of Southeast Asian Nations (ASEAN) was created in 1967 and is currently composed of ten member countries: Brunei Darussalam, Cambodia, Indonesia, Laos, Malaysia, Myanmar, Philippines, Singapore, Thailand, and Vietnam.

ASEAN's key data protection instrument is Framework on Personal Data Protection, and is the most recent framework covered by this paper, having been established in 2016.[299] It is a non-binding instrument, as strongly underlined in the preamble, which affirms that the ASEAN Framework "serves only as a record of the Participants' intentions and does not constitute or create, and is not intended to constitute or create, obligations under domestic or international law."[300]

The key provision of interest for this paper is present in section 6(e)(ii), under the label of "Access and Correction". According to its text, "upon request by an individual, an organisation should (...) correct an error or omission in his personal data, unless domestic laws and regulations require or authorise the organisation not to provide access or correct the personal data in the particular circumstances." Similarly to the APEC's Privacy Framework, the focus here is on the accuracy of the data (there has to be an error or omission), but the provision strays even further away from the DPD's right to erasure, in offering only correction, as opposed to removal, of the contested information. Moreover, in significant contrast to APEC, the substantive principles included in the ASEAN framework are very limited and there is also no general requirement to ensure appropriate redress. Furthermore, the ASEAN framework does not possess a separate definition of a data controller or data processing. Nevertheless, throughout the text, references appear to a set of "collection, use or disclosure"[301] of personal data. While rather concise, this list of activities could allow for an interpretation of relevantly caught actor which would encompass search engines indexing content. Nevertheless, aside from inaccurate or misleading data, neither the specific right laid out in section 6(e)(ii) nor the ASEAN Framework as a whole would appear capable of underpinning the type of substantive remedy provided for in *Google Spain*.

299 Framework on Personal Data Protection (2016) ASEAN.

300 See Framework on Personal Data Protection (2016) ASEAN, preamble.

301 For example, in arts. 6(a)(i) and (ii), 6(b) and 6(d).

6.5 Conclusions and Further Development

This paper has examined five international data protection frameworks, in order to explore whether – upon a reasonable interpretation – they could support the presence of a subjective right to deindexing vis-à-vis search engines, akin to that found in the *Google Spain* decision of the CJEU. The undertaken analysis has shown that such a regime could be well supported within the CoE, OECD, ECOWAS instruments and even by the APEC Framework, should the need for effective redress for violation of core data protection principles ground subjective rights beyond that explicitly identified therein. Only the ASEAN Framework, with its exclusive focus on redress against inaccurate or incomplete date, clearly lacks features necessary to underpin a *Google Spain* type result.

Given this, it is argued that the time is ripe for more explicit international discussion and consensus building around the 'right to be forgotten'. Corresponding action could not only help mitigate the dangers of a fissiparous result but, as importantly, help provide some real and effective protection for data subjects against the very real threats described in section 2. In our view, the obvious initial forum to take this forward would be the International Conference of Data Protection and Privacy Commissioners (ICDPPC). With work dating back to 1979, the ICDPPC now brings together over one hundred privacy and data protection authorities through an annual conference, executive committee and secretariat.[302] As a specialist transnational body, it has a self-avowed mission to "provide leadership at international level in data protection and privacy" and "[t]o connect and support efforts at domestic and regional level, and in other international forums, to enable authorities better to protect and promote privacy and data protection".[303]

One of its mechanisms for achieving this has been through the adoption of resolutions on specific topics. Indeed, the Conference has already adopted a number of related resolutions including one

302 See <https://icdppc.org/> [accessed 26 September 2017].

303 International Conference of Data Protection & Privacy Commissioners, 'Mission and Vision', <https://icdppc.org/the-conference-and-executive-committee/strategic-direction-mission-and-vision/> [accessed 26 September 2017].

from 2008, focused on social network services.[304] The Conference should, therefore, begin work with a view to producing a resolution on the 'right to be forgotten' or, should this nomenclature prove too controversial after all, the right to object to public, online processing of personal data. Although this paper and indeed *Google Spain* focused only on search engines, such a resolution should not be solely focused on these actors. Indeed, other entities including social networking sites, video-sharing platforms and rating websites also play a crucial role in structuring the public spread of personal data, but the status of these actors as data controllers is less a matter of controversy than is the case as regards search engines.

The aim of such a resolution must necessarily remain relatively abstract. For example, whilst there is a broad agreement in this context that there should be an overriding public interest derogation from compliance even *ex post* with at least the detailed rules set down in many national data protection laws, the document could not be expected to exhaustively define the parameters of this. Instead, the aim should be to build high-level consensus around the value of such an *ex post* right in today's challenging digital context.

Once a resolution has been adopted, ICDPPC regulators should be expected to practically implement this at the national level, save only when this would not be compatible with their local legal frameworks. As with other initiatives of the Conference, a Working Group could be established to report on progress. Beyond such directly practical results, the Resolution and publicity given to it could hopefully prompt more political debate on actualizing this aspect of data protection. For example, the issue could be referred to bodies attached to those formal transnational instruments which are more institutionalized such as the Council of Europe Data Protection Convention's Consultative Committee. In time, this could lead to a more formal outcome here; for example, in the Council of Europe context, the adoption of a Recommendation by the Committee of Ministers.

Ultimately, any international progress on the 'right to be forgotten' could only be both incremental and partial – and a myriad of issues

304 30th International Conference of Data Protection & Privacy Commissioners, 'Resolution on Privacy Protection in Social Network Services'(*International Conference of Data Protection & Privacy Commissioners*, 17 October 2018) <https://icdppc.org/wp-content/uploads/2015/02/Resolution-on-Privacy-Protection-in-Social-Network-Services.pdf> [accessed 26 September 2017].

remain to be explored and worked through. Nevertheless, this paper has argued that good deal of international consensus on this issue may already be "hiding in plain sight" within the structures of most, though not all, transnational data protection instruments. Given this, it would be profitable if this issue came out of its international hiding and moved towards the agendas of relevant actors engaged in structured discussion and hopefully consensus-building. Only through such, admittedly at times challenging, processes can an effective and balanced system of international protection for data subjects really be achieved.

6.6 Bibliography

30th International Conference of Data Protection and Privacy Commissioners, 'Resolution on Privacy Protection in Social Network Services', Strasbourg 17 October 2008. <https://icdppc.org/wp-content/uploads/2015/02/Resolution-on-Privacy-Protection-in-Social-Network-Services.pdf> [accessed 26 September 2017].

Ambrose ML and Ausloos J (2013). 'The Right to Be Forgotten Across the Pond' (2013) 3 Journal of Information Policy 1-23.

Conseil d'État, 'Right to be delisted' (*Conseil d'État*, 24 February 2017) <http://english.conseil-etat.fr/Activities/Press-releases/Right-to-be-delisted> [accessed 26 September 2017].

OECD, 'Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data' (1980) C(80)58/FINAL, as amended on 11 July 2013 by C(2013)79.

Greenleaf G (2012). 'The influence of European data privacy standards outside Europe: Implications for globalisation of Convention 108?' (2012) University of Edinburgh Research Paper Series no. 12/2012.

Gryffroy P (2016). 'Delisting as a part of the decay of information in the digital age: a critical evaluation of Google Spain (C-131/12) and the right to delist it has created' (2016) 22 (6) Computer and Security Law Review 150.

Lynskey O (2015). 'Control over Personal Data in a Digital Age: *Google Spain v AEPD and Mario Costeja Gonzalez*' (2015) 78 (3) Modern Law Review 522.

Mayer-Schönberger V (2009). *Delete: The Virtue of Forgetting in the Digital Age* (Princeton University Press, 2009).

Moran C (2014). 'Things to remember about Google and the right to be forgotten' *The Guardian* (03 July 2014) <https://www.theguardian.com/technology/2014/jul/03/google-remember-right-to-be-forgotten> [accessed 26 September 2017].

Sullivan D, 'How Google's New "Right To Be Forgotten" Form Works: An Explainer' (*SearchEngineLand*, 30 May 2014) <http://searchengineland.com/google-right-to-be-forgotten-form-192837> [accessed 26 September 2017].

Voss G & Castets-Renard C (2016). 'Proposal for an International Taxonomy on the Various Forms of the Right to Be Forgotten: A Study on the Convergence of Norms' (2016) 14 Colorado Technology Law Journal 281.

7 Data Ownership in Platform Markets

Rolf H. Weber

Abstract

In the past, platform regulations mainly concerned content issues related to accessible information and to provider responsibility. However, the growing debates about data ownership might also extend the scope of regulatory challenges in relation to platform markets. Relevant topics are collective ownership and data portability in the legal ownership context as well as access to data and data sharing in case of an existing factual control about data. Therefore, the future regulatory framework for online platforms will have to be designed in a differentiated manner. This paper analyses the concept of data ownership and the impact of platform markets' characteristics in data ownership. Subsequently, the paper explores the distinction of various types of data "categories" and the main regulatory challenges for online platform markets.

7.1 Introduction

The title "Data Ownership in Platform Markets" encompasses two increasingly important terms used in the information society: (i) Platform markets are a phenomenon having gained more attention over the last few years and causing new legal questions. (ii) Data ownership is a notion that has been coined in view of the increased value of data in the global data economy and information society. The combination of the two terms provokes many economic and regulatory challenges.

7.1.1 Platform Markets

Platform markets in the online environment are designed by some specific features that have not been crucial in traditional (physical) markets. On the one hand, some criteria generally typical for online markets are of relevance, in particular (i) two-sided markets and network effects, (ii) concentration effects ("the winner takes it all"), (iii) switching costs and multi-homing issues and (iv) free

services for one market side.[305] On the other hand, in addition to these criteria, platform markets are characterised by the following elements: (v) *scalability*, *i.e.* the platform growing through more participants help increase its level of efficiency and performance, (vi) *usability*, *i.e.* more participants leads to an improved testing performance, and (vii) *speed of digital cycles*, *i.e.* the creation of new products, processes and services happens more frequently.[306] However, some restrictions such as entry or exit barriers (hurdles due to a lack of data rather than the existence of high financial investment requirements) cannot be overlooked.[307]

A further aspect must be taken into account when addressing data-driven markets: In contrast to brick and mortar enterprises not only the traditional monetary turnover achieved by businesses is to be considered as reference parameter but also the control of data, not depending so much on the monetary wealth of a commercial entity, plays a crucial role. As a consequence, the legal approach needs to be adjusted.

7.1.2 Data Ownership

Since Roman times the legal term "ownership" relates to physical property, later complemented by specific intellectual property rights and adjacent neighbouring *sui generis* rights. Data does not fulfil the respective qualifications mentioned above, since data is untouchable/non-physical and is not based on an intellectual effort.[308] If "ownership" rules should be relevant in respect of data, the traditional notion would have to be extended and/or changed.

So far, the debates about platform markets have not mainly concerned issues related to data ownership. Other topics have been more intensively discussed, for example, the antitrust challenges (Google), the abusive tax evasion schemes and the prevention of so-called "fake news" or "filter bubbles". Legally these topics are related to the applicable regulatory framework and to the potential

305 Rolf H. Weber, Competition Law Issues in the Online World, 20th St. Gallen International Law Forum, April 2013, 2 et seqq. <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2341978> [accessed 1 November 2017].

306 Graef (2015).

307 Weber, *supra* n. 305, 5.

308 See Thouvenin, Weber, Früh (2017:111 et seqq.).

responsibility of platform providers for the contents on the platforms available to everybody. First attempts to introduce responsibility obligations can already be seen in practice.[309] Besides that, general discussions address the compliance of certain (successful) platforms with the applicable labour, social insurance, lease laws, *etc.*[310] In contrast, the data ownership issue on platform markets remained outside the scope of specific attention. Therefore, this contribution looks into its legal challenges.

7.2 Stock-taking of the Relevant Parameters

7.2.1 Impact of Platform Markets' Characteristics in Data Ownership

As mentioned, platform markets are characterised by special features making it challenging to apply the well-known terms of antitrust law. Even in traditional brick and mortar situations, the definition of the relevant product market often creates complications. However, platform markets with their special features are even more complex. The rapid technological changes, the innovative players and the continuous spread of access to data cause difficulties in appreciating and assessing the competitive parameters influencing the platform markets.

The two-sided market characteristics governing online platforms makes it necessary to take into account the interdependence between the market participants and the possible interchangeability of performance streams. The widespread lack of price signal effects in platform markets also raises problems since conventional antitrust models are based on price-sensitive market elements. In other words, in platform markets the price is not the sole competition parameter.[311]

The existence of multi-sided markets is likewise reflected in the fact that the attractiveness of a platform depends on the number of users visiting a website, which does not directly produce

309 See Research Group On The Law Of Digital Services (2016:164 et seqq.).

310 Regulators in several countries and/or municipalities have begun to implement specific provisions governing the business of Uber or Airbnb.

311 See Graef, *supra* n. 306, 487-8.

an economic benefit. But prices of advertising depend on the number of platform participants. In addition, the users principally do not generate the revenues for the platform owners but the remuneration is paid through the advertising companies.[312]

Recent experience has shown that the market incentives for firms to collect and process personal data are high since data represent a (substantial) value that can be monetized in various contexts. In other words, data-based platform enterprises do have the chance that – by collecting data – gains are internalized (for example by enforcing a *de facto* protection of data control); the potential costs are borne by the users of the platform.[313]

Whether the introduction of a data ownership right would strengthen the individual control over personal information, however, appears to be uncertain. Already prior to the establishment of any kind of legal relationship (i.e. during contract negotiations), individuals might lack the bargaining power in respect of the data delivery to companies; in particular, the terms of services are generally non-negotiable. As a result, on the one hand, externalities are economically caused by the fact that individuals are losing control over their data without receiving a "compensation". On the other hand, online platform enterprises do not suffer losses from the disclosure of data nor do they have to internalize any costs for such disclosure.[314]

7.2.2 Complex Data Categories for Ownership Purposes

Daily life shows that not only one specific type of data exists but that many "categories" in several scenarios can be distinguished. A main distinction must be made between personal data and non-personal data since the data protection laws gaining more and more importance in various jurisdictions are only applicable to personal data. Privacy laws usually cover information relating to an identified or identifiable person; an identifiable individual is one who can be directly or indirectly identified by way of any relevant

312 Weber *supra* n. 305, 4.

313 See Geradin & Kuschewsky (2013).

314 See Thouvenin, Weber & Frueh, *supra* n. 309, 117, with further references.

attributes.[315] In practice, this identification process causes many uncertainties due to the fact that re-identification measures often allow changing the character of the data.[316]

A further distinction can be made between the data of individuals and the data of corporate entities; however, this differentiation is not identical to the distinction between personal and non-personal data and does not play a key role in connection with data ownership consideration.

A few years ago, the World Economic Forum (WEF) suggested applying a completely new taxonomy for data: the WEF proposes to differentiate between volunteered data, observed data, and inferred data; this distinction is based on the production element for data:[317] (i) Volunteered data is shared by individuals intentionally since each individual is aware of the fact that his or her data is transferred. The sharing of data depends on the emotional links of the individuals to their volunteered data. (ii) Data is observed if individuals share data produced not by them but about them. In substance, such data is based on the recording of individual behaviour, often without existing awareness about the data collection itself or about the data's subsequent use and value. (iii) Inferred data means different data types originating from various sources, mostly used for predictive purposes. The concerned individuals do not only lack awareness but also control over the actual use of the data. As reflected in the WEF taxonomy the creation of data (even by machines) requires some level of human involvement. In respect of online platform markets, the most important category appears to be the observed data.

The data ownership debates became very lively subsequent to the publication of the European Commission's Communication on the "Building a European Data Economy" in January 2017.[318]

315 Regulation (EU) 2016/679 of the European Parliament and of the Council of 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, GDPR), Art. 4 (1).

316 Weber & Oertly (2015).

317 World Economic Forum (2011:14); for a more detailed explanation, see World Economic Forum (2014:16 et seqq.).

318 European Commission (2017:9).

The Commission discusses several legal instruments to be introduced or modified in view of the needs of the digital society. The most far-reaching proposal is the creation of a data ownership right; alternatives are an amendment to the *sui generis* right contained in the Database Directive 96/9 and the implementation of data access rights based on compulsory licenses.[319]

Whether the endowment effect identified by behavioural economics would contribute to the justification of a data ownership right appears to be doubtful. The endowment effect means that individuals endowed with a property right tend to value a good higher than other individuals without a property right and thus higher than the Coase theorem would suggest (even when transaction costs are close to zero). Therefore, scepticism prevails as to the improvement of the individuals' position if ownership rights would be generated. [320]

7.3 Regulatory Challenges

Online platform markets are gaining importance and the quantity of data on platforms is increasing, as the examples of Airbnb and Uber clearly show. Therefore, the question of who "owns" the data becomes crucial. Data is non-rivalrous and can be re-used by the legal "owner" as well as by the factual "controller." Consequently, ownership by both natural and legal persons merit to be assessed.

7.3.1 Collective Ownership

Particularly in the context of big data analytics, concepts of collective ownership have been developed. Often, the approach is called "sharing the wealth strategy".[321] Such a concept premises on the data controllers to provide individuals with access to their data in a useable format; equally, the individuals should be allowed to take advantage of applications in order to analyse their own data and to draw useful conclusions from it. This concept presupposes that organizations are prepared to share with individuals the wealth their data helps create.

319 For an overview, see the contributions contained in the book edited by Lohsse, Schulze & Staudenmayer (2017).

320 See Thouvenin, Weber & Früh *supra* n. 308, 120 with further references.

321 See Weber (2013); Rubinstein (2013:74, 81); Tene & Polonetsky (2013:263 et seqq.).

First attempts of introducing some kind of "sharing the wealth strategy" can be seen in the health sector. In some countries (amongst others in Switzerland) projects are developed and partly implemented (for example midata.coop) which allow to exchange health data within a certain group of individuals.[322] The preparedness to share their own data and to accept a loss of control is "compensated" by the fact that valuable insights can be gained from available data submitted by third persons.

The legal foundation of collective ownership concepts is not easy to establish. Two approaches appear to be worthwhile for further research:

- On the one hand, it seems feasible that the participants of a "sharing the wealth strategy" would constitute a cooperative;[323] this form of legal entity is known in most Civil and Common Law countries.[324] The incorporation documents and/or the organizational rules would then have to allow the stakeholders to get access to certain data of other participants and to use them for the designed purposes.
- On the other hand, the concept of co-ownership or the concept of joint-ownership (known in most Civil and Common Law countries as well)[325] could be considered as legal foundation for the "sharing the wealth strategy".[326] The main problem consists in the fact that these concepts rely on real property and have not been tested for immaterial data.

In a nutshell, collective ownership could be an appropriate legal tool for designing a data ownership framework that applies to platform markets, however, the details of such a tool would need to be further developed and better refined. Practically, this approach could only work if the participating individuals and enterprises see a certain (monetary or non-monetary) benefit in a collective ownership approach; depending on the given situation further efforts of conviction are needed.

322 Hafen, Kossmann & Brand (2014:82 et seqq.).

323 Hafen, Kossmann & Brand *supra* n. 322, 82 et seqq.

324 E.g. art. 828 et seqq. of the Swiss Code of Obligations, RS 220.

325 E.g. art. 646 resp. art. 652 of the Swiss Civil Code, RS 210.

326 Hess-Odoni (2004).

7.3.2 Data Portability

Usually data represents a certain value. Therefore, the individual might be interested to change the context of his/her data use from time to time. The right to data portability has its roots in the acknowledgement that control over data implies the possibility to move data at the request of the person from one online provider to another.[327] What has been discussed in respect of social media (e.g. Facebook) is equally applicable to online platforms.

The concept of data portability has recently become subject to data protection legislation: As stated in article 20 (1) of the General Data Protection Regulation (GDPR),[328] an individual is entitled to request from the *de facto* data controller to have the data transferred to another entity, thereby overcoming potential lock-in effects. The GDPR only covers personal data, which is portable, in contrast to non-personal data. [329]

However, the same reasoning holds true if individual data or even metadata, being factually controlled by the entity that has collected the data, is re-individualized (de-anonymized) by means of big data analytics (and thereby becomes personal data).[330] Taking into account the ratio of the new article 20 GDPR, the data controller should be obliged to provide all data needed by the user in order to change the platform and utilise the services of another data controller.

The data portability right entitles the data subject to receive the personal data in a structured, commonly used and machine-readable format.[331] Notwithstanding this normative statement, the practical implementation of such a provision is not yet fully clear and certain elements are still contested.[332] This assessment is (at

327 Weber (2016:66-67).

328 For further details see Article 29 Data Protection Working Party (2017: 9 et seqq.).

329 For the strengths and weaknesses of a regulatory right of data portability see Weber, *supra* n. 327, 68-69.

330 European Data Protection Supervisor, 'Preliminary Opinion on Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy' (2014), 9; Mantelero (2014); Gymrek et al. (2013:321 et seqq.); Golle (2006:77 et seqq.).

331 Art. 20 (1) GDPR; however, in times of fast changing technologies the interpretation of the term "commonly used" may cause controversies.

332 Janal (2017:63); Alberini & Benhamou (2017: 520); Schätzle (2016:74).

least partly) due to the fact that the data portability rule has been designed in respect of big market players, particularly social media providers. However, the intention to protect the data subject does also have the consequence that the small and medium size controllers will be charged with an additional burden (delivery of data to another controller in a standardized format).[333]

Non-personal data is not governed by the GDPR, even if data portability could also play a role in respect of machine-generated data.[334] In such a situation, portability can only be founded on antitrust law. Competition-orientated instruments combat customer-lock-in effects, which lead to increased switching costs or even to the creation of market barriers for new providers. In the context of social networks and online platforms, mostly personal data is concerned and the GDPR is applicable. But in case of non-personal data the argument can also be made that users often invest a great amount of time and efforts in providing data to a platform. In the absence of a data portability right, the change to another provider or to another platform would only reluctantly be considered in practice, even if the current service is not convincing or inferior. If a data portability right based on antitrust provisions is granted, switching costs are reduced and the potential competition will most likely be fostered.[335] However, antitrust proceedings are usually lengthy and cost-intensive, meaning that in practice the antitrust instruments only play a limited role.

In a nutshell, the implementation of a data portability right as provided for by article 20 GDPR or by general antitrust rules helps the individual to change the contractual relations and/or the factual environment. However, such a right does not offer an immediate potential to successfully commercialize the individual's own data.

7.3.3 Access to Data

Legal ownership generally implies the right to decide on the use and the exploitation of the owned good. In case of data, the data

333 Graef (2015:508); Swire & Lagos (2013:352).

334 See for example the French Loi Lemaire (Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique), which will allow data portability in the context of industrial data.

335 European Commission, *supra* n. 318, 15; European Commission (2017:47 et seqq.).

subject principally is in a position to exercise these rights, possibly in parallel to other persons since the exclusion function might not apply due to the non-rivalrous character of data. However, factual control over data is at least as important as ownership, if not more. In order to strengthen the (legal) position of the data subject, access rights to data need to be considered.

In case of personal data, most data protection laws contain provisions as to the information rights of individuals.[336] Subject to the details of such provisions, the scope and degree of access to data is established and the respective claims can be made against the data controller. In case of non-personal data or data sets, however, specific legal rules are mostly missing.[337] As a result, the controller of the data is often inclined to retain the data and analyze it in proprietary silos.

This trend is strengthened by the fact that an increasing amount of machine-generated data is created without direct intervention of an individual by computer processes, applications, services, or by sensors processing information received from equipment, software, or machinery.[338]

In its most recent Communication to the data economy of January 2017, called "Building a European Data Economy", the European Commission is proposing specific data access rights.[339] Thereby, the following objectives should be envisaged:

- Improve access to anonymous machine-generated data;
- Facilitate and incentivise the sharing of such data;
- Protect investments and assets;
- Avoid disclosure of confidential data;
- Minimise lock-in effects.

Since the data controller often keeps collected data under its control, access to data is a pre-requisite for transactional processes

336 Eg. art. 15 GDPR and art. 8 of the Swiss Federal Act on Data Protection, RS 235.1.

337 European Commission, *supra* n. 318, 10.

338 *Ibid.*, 9.

339 *Ibid.*, 11 et seqq.

such as information sharing and information transfer. For good reasons a data access right is seen as an alternative to a data ownership right. The Commission is arguing that granting access to data can have a welfare-enhancing effect without impinging on the economic interests of the market participant that has invested into the data collection.[340] Reference is made to "data commons" as a way to describe non-discriminatory access to certain data. Such an approach is not designed to implement an "open data" approach nor to grant access without a remuneration.

To sum up, the factual control of data irrespective of any data ownership considerations is a frequent phenomenon and a serious challenge for data sharing and data transfer in the information society. The respective problems can at least partly be overcome if the legislator implements a data access right. Such a title would empower individuals and businesses to verify which data are stored and available on a specific online platform.

7.3.4 Data Sharing

A data access right as such does not imply a specific scope of use and exploitation of the data. Moreover, the law needs to establish to what extent the accessed data can be re-used by the data subject. If access to data is denied or if a further exploitation of the data is not permitted, a regulatory reaction could consist in a compulsory license regime. The term compulsory license is insofar not very precise as not the concept of licensing of rights is realized but rather rules are proposed that grant an exploitation right in respect of certain data.[341] This assessment is true regardless of the fact that the value intrusive to data is often minimal since access gives the capacity to make sense of the data.

A compulsory licenses system granting access to data (also to non-personal machine-generated raw data) might facilitate the subsequent data sharing due to the availability of the data, *i.e.* the knowledge of the data is a pre-condition of the sharing. The introduction of an interventionist regime such as compulsory

340 *Ibid.*, 37.

341 See Weber in: Lohsse, Schulze & Staudenmayer, *supra* n. 319, 137.

licenses, however, requires the consideration of already existing models that allow data sharing as well as of other available incentives for individuals and businesses to share data (for example pro-competitive data sharing among market participants on specific data platforms as in the automotive industry).[342] Such alternative "arrangements" can consist in consensual solutions or legal requirements.

In the Staff Working Document accompanying the mentioned Communication of January 2017, the European Commission has proposed to introduce a compulsory licenses regime to be tied to a couple of conditions depending on the market circumstances.[343] The respective requirements should encompass pricing rules (reflecting the value of the accessed data), the volume of the data, the scope for re-use and exploitation of data, and the extent of a possible bundling of data.

In antitrust law, the design of appropriate license conditions is a well-known issue. Usually the discussions evolve around the so-called FRAND (fair, reasonable and non-discriminatory) terms. Notwithstanding the fact that the practical implementation problems in the real world (for example in case of "patent ambush" and "patent hold-out") should not be underestimated and that the design of the respective (most likely sector-specific) licenses conditions still needs to be developed, the data sharing based on compulsory licenses seems to constitute a viable legal concept.[344]

In short, if factual data control prevails and data access is given, compulsory licenses could contribute to an improved data sharing to the benefit of individuals, businesses and platform market providers in the future.

7.3.5 Responsibility of Platform Providers for Data Handling

As mentioned in the introduction, the topic of the platform provider responsibility is intensively discussed in the context of "fake news" or – more generally – in relation to illegal contents. Very obviously,

342 Weber, *Ibid.,* p. 147.

343 European Commission, *supra* n. 335, 39.

344 See Weber (2011:51 et seqq.); Méniére & Thumm (2015:12 et seqq.); Mariniello (2011:523 et seqq.).

the platform provider is also responsible for a proper treatment of the data available on the platform. Amongst others, the appropriate data security measures are to be implemented that can reasonably protect the data against cyberattacks and other cyberincidents.[345]

In addition, the platform provider is also responsible for the proper handling of the data with respect to data ownership and data access matters. If a data subject exercises his/her data portability right, the platform provider must be able to transfer the respective data in a structured and machine-readable format. Equally, access must be technically possible if a specific data access right applies or if access must be granted based on a compulsory license.[346]

Furthermore, the platform provider should provide for the technical environment which allows the implementation of a "sharing the wealth strategy". Insofar, the obligation is less specific; moreover, co-operative efforts are to be expected which allow the creation of an information technology structure that enables the concerned data subjects to share their data in the envisaged manner.

7.4 Looking Forward

The growing discussions about data ownership will not make a "detour" around the online platform markets. With the increased quantity (and often also quality) of data available on certain platforms the assessment of "ownership" issues on platform markets becomes imperative. As a result, research efforts must be strengthened in order to develop a differentiated regulatory framework for platform markets.

Thereby, two different routes are to be distinguished: (i) Legal ownership in a narrow sense can play a role on platform markets in certain circumstances; an extension of the traditional ownership notion including data could allow the concerned individuals to establish collective ownership models and to realize a "sharing the

345 See art. 5 (1) (f) and art. 32 GDPR; see also art. 22 of the Regulation (EC) 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data; European Data Protection Supervisor, Guidance on Security Measures for Personal Data Processing – Article 22 of Regulation 45/2001 (2016).

346 Weber, *supra* n. 342, 155-156.

wealth strategy". (ii) The acknowledgment of a data portability right not only for personal data (as in article 20 GDPR) but also for non-personal data would constitute a special kind of "data ownership" allowing to have affected a transfer of data from one provider to another provider.

Apart from a legal title to data, factual control about data is frequently practiced in the real world by storing the data in proprietary silos. In such a situation, the data subject must have a data access right extending beyond the scope of existing data protection laws. Furthermore, the introduction of a compulsory licenses regime would facilitate a regulation of re-use and exploitation rights by applying the FRAND terms known from antitrust law.

7.5 Bibliography

Alberini A & Benhamou Y (2017). 'Data Portability and Interoperability' (2017) 17 (8) Expert Focus.

Article 29 Data Protection Working Party (2017). 'Guidelines on the right to data portability' (2017), WP 242 rev.01.

European Commission (2017). 'Commission Staff Working Document on the free flow of data and emerging issues of the European data economy' (2017), SWD, 2 final.

European Commission (2017). 'Communication on Building a European Data Economy' (2017), 10 January 2017, COM, 9 final.

European Data Protection Supervisor. 'Guidance on Security Measures for Personal Data Processing – Article 22 of Regulation 45/2001' (2016).

Geradin D & Kuschewsky M (2013). 'Competition Law and Personal Data: Preliminary Thoughts on a Complex Issues', <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2216088> [accessed 31 October 2017].

Golle P (2006). 'Revisiting the Uniqueness of Simple Demographics in the US Population' (2006) Proceedings of 5th ACM Workshop on Privacy in Electronic Society.

Graef I (2015). 'Mandating portability and interoperability in online social networks: Regulatory and competition law issues in the European Union' (2015) 39 (6)Telecommunication Policy 502.

Graef I (2015). 'Market Definition and Market Power in Data: The Case of Online Platforms' (2015) 38 (4) World Competition Law and Economics Review 473.

Gymrek M et al. (2013). 'Identifying Personal Genomes by Surname inference' (2013) Science 339.

Hafen E, Kossmann D & Brand A (2014). 'Health Data Cooperatives – Citizen Empowerment' (2014) 53 (2) Methods Inf. Med 82.

Janal R, (2017). 'Data Portability – A Tale of Two Concepts', Journal of Intellectual Property (2017) 8 Information Technology and E-Commerce Law 59.

Mariniello M (2011). 'Fair, reasonable and non-discriminatory (FRAND) terms: A challenge for competition authorities' (2011) 7 (3) J. of Comp. Law & Economics 523.

Mantelero A (2014). 'The future of consumer data protection in the E.U., Re-thinking the "notice and consent" paradigm in the new era of predictive analytics' (2014) 30 Computer Law & Security Review 643.

Méniére Y & Thumm N (2015). 'Fair, Reasonable and Non-Discriminatory (FRAND) Licensing Terms'. Research Analysis of a Controversial Concept'. (2015) JRC Science and Policy Report.

Research Group on the Law of Digital Sevices (2016). 'Discussion Draft of a Directive on Online Intermediary Platforms' (2016) 5 Journal of European Consumer and Market Law 164.

Rubinstein I (2013). 'Big Data: The End of Privacy or a New Beginning?' (2013) 3 (2) International Data Privacy Law 74.

Schätzle D (2016). 'Ein Recht auf die Fahrzeugdaten, Das Recht auf Datenportbailität aus der DS-GVO' (2016), Privacy in Germany 02.16.

Swire P & Lagos Y (2013). 'Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique' (2013) 72 (2) Maryland Law Review 335.

Tene O & Polonetsky J (2013). 'Big Data for All: Privacy and User Control in the Age of Analytics' (2013) 11 (5) Northwestern Journal of Technology and Intellectual Property 239.

Thouvenin F, Weber R & Früh A (2017). 'Data ownership: Taking stock and mapping the issues', in: Dehmer & Emmert-Streib (eds.) (2017), *Frontiers in Data Science* (CRC Press, 2017).

Weber R (2013). 'Big Data: Sprengkörper des Datenschutzrechts?' (2013), Weblaw Jusletter IT of 11 December No. 31.

Weber R 'Competition Law Issues in the Online World', 20th St. Gallen International Law Forum (April 2013) available at <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2341978> [accessed 1 November 2017].

Weber R (2011). 'Competition Law versus FRAND-terms in IT-Markets' (2011) 34 World Competition Law and Economics Review 51.

Weber R (2016). 'Data Portability and Big Data Analytics: New Competition Policy Challenges' (2016) 23 Concorrenza e Mercato 59.

Weber R & Oertly D (2015). 'Aushöhlung des Datenschutzes durch De-Anonymisierung bei Big Data Analytics?' (2015) Weblaw Jusletter IT of 21 May 2015.

Lohsse S, Schulze R & Staudenmayer D (2017) (eds.), *Trading Data in the Digital Economy: Legal Concepts and Tools* (Nomos, 2017).

Hess-Odoni U (2004). 'Die Herrschaftsrechte an Daten' (2004) Weblaw Jusletter of 17 May 2004.

World Economic Forum (2011). 'Personal Data: The Emergence of a New Asset Class' (World Economic Forum, 2011).

World Economic Forum (2014). 'Rethinking Personal Data: A New Lens for Strengthening Trust' (World Economic Forum, 2014).

8 What Legal Framework for Data Ownership and Access? The French Digital Council's Opinion

Célia Zolynski,* on behalf of the *French Digital Council

Abstract

*To encourage the free flow of data, the European commission announced in January 2017 that it was exploring various legislative and non-legislative options, including the creation of a property right over non-personal data. This chapter is based on an opinion issued by the French Digital Council (*Conseil National du Numérique*) in April 2017 to respond to the Commission's consultation. First, the chapter stresses that value creation mostly occurs when data is contextualized and combined with data from other datasets in order to produce new insights. Thus, the issue is not to establish a hypothetical right of data ownership; rather, it is about thinking and designing incentive regimes of data access and exchange between data controllers so as to encourage value creation. Indeed, contrary to a widely held belief, data ownership does not necessarily facilitate data exchanges - it could actually limit them. Above all, the free flow of data should be envisioned between online platforms and not only between states. These new forms of sharing are essential to the development of a European data economy.*

8.1 Introduction

As part of its strategy for the Digital Single Market, the European Commission has announced in January 2017 the preparation of several initiatives to develop a data-driven European economy. The General Data Protection Regulation has established the framework for the processing of personal data,[347] while the directive on the re-use of public sector information addressed that of public sector

347 Regulation (EU) 2016/679 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 and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) OJ L 119, 4.5.2016, p. 1–88. Available at http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=FR [accessed 1 November 2017].

data.[348] As a further step, the European Commission is currently aiming to regulate the free flow of non-personal data. In doing so, it intends to pursue several objectives: the harmonisation and the reduction of data localisation restrictions within EU Member States; the clarification of the legal framework of data to protect investment and reduce legal uncertainty; as well as the promotion of data sharing among data controllers.[349]

The French Digital Council wished to react to the public consultation launched by the Commission on this matter. Current reflexions on the creation of a fifth freedom of movement in Europe – namely, free flow of data, which would complement free movement of goods, services, capital and persons – are still in their infancy. The introduction, at this stage, of a principle of free movement of data could lead to unforeseen consequences, considering the extreme variety of realities covered by the term "data," and the diversity of uses and markets that could emerge. In addition, the opinion of the French Digital Council is that the barriers to the free flow data are primarily caused by the lock-in strategies developed by prominent economic actors rather than by national legislations. Thus, the Commission should also investigate the means to remove "cross-platforms" barriers, and not only "cross-borders" ones.

Finally, the recognition of a principle of free flow of data within the EU could be used as an argument for enshrining it in future free trade agreements. This would facilitate the unregulated transfer of data outside the EU, which raises major concerns in terms of competitiveness, consumer protection and respect for fundamental rights[350]. On the one hand, the important asymmetries that currently characterise data flows across the world justify an approach that focuses on the interests of European companies. On the other hand, the recognition of such principle could constitute a

348 Directive 2013/37/EU of the European Parliament and of the Council of 26 June 2013, amending Directive 2003/98/EC on the re-use of public sector information OJ L 175, 27.6.2013, p. 1–8, available at http://eur-lex.europa.eu/legal- content/EN/TXT/HTML/?uri=CELEX:32013L0037&from=FR [accessed 1 November 2017].

349 Economic and Social Committee and the Committee of Regions "Building a European Data Economy" available at http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52017DC0009&from=FR [accessed 1 November 2017].

350 Report on the Free Flow of Data and International Trade Agreements, Inspection générale des finances et Conseil général de l'économie, 2016 <https://www.economie.gouv.fr/libre-circulation-des-donnees-et-accords-commerciaux> [accessed 1 November 2017].

threat to the sovereignty of EU Member States in terms of taxation, national security and public policy.

8.2 Data and Ownership

One of the options currently being explored by the Commission is the recognition of a property right over non-personal data. This proposal has become a recurrent theme in the debates surrounding the digital economy. It has been promoted most notably by Jaron Lanier[351] and Evgeny Morozov[352] in the context of personal data protection, where it is both considered as an answer to the loss of control of citizens over their data and antitrust issues arising with the concentration of data in the hands of a few Internet giants. The idea was also used to imagine solutions to the loss of sovereignty implied by asymmetric data flows between economic regions – as highlighted by Pierre Bellanger, in France[353] – or as a part of an industrial strategy that grants more rights to industrial actors "generating data." This latter option has been suggested in various academic and policy debates in Germany for instance.[354]

First, it should be noted that this proposal, if implemented, would reverse the traditional paradigm that governs data protection. A general principle of data ownership would notably conflict with the approach established by the European directive 96/9 of March 11, 1996 relating to legal protection of databases,[355] which grants to its rightholders a double protection, thanks to copyright and *sui generis* right. However, the latter protection, which exists to recognise the substantial investment that is made in compiling a database, is not intended to apply to data itself, as the European Court of Justice has pointed out. By extending the right of ownership to personal data, we may cause a general shift toward ownership over all "raw" data.

351 See Lanier (2014).

352 See Evgeny Morozov. 'Data populists must seize our information – for the benefit of us all'. (*The Guardian*, 04 December 2016) <https://www.theguardian.com/commentisfree/2016/dec/04/data-populists-must-seize-information-for-benefit-of-all-evgeny-morozov> [accessed 1 November 2017].

353 Bellanger (2014).

354 Zech (2015).

355 Directive96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, OJ L 77, 27.3.1996, p. 20–28. Available at <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31996L0009> [accessed 1 November 2017].

Consequently, it would be difficult to determine the ownership regimes and their beneficiaries: who could claim ownership over data? The owner of the data sensor? The owner of the building in which the sensor is located? The data subject? Contrary to the original intention of clarifying the legal framework, such a proposal would increase the likelihood of litigation over the contracts governing those exchanges. Thus, this option may considerably increase legal uncertainty.

Furthermore, the boundary between personal and non-personal data is very thin, when one considers the real risks of re-identification. The limits of anonymisation and pseudonymisation have been decisively proven and, to date, there is no technical guarantee that personal data would not be affected by a potential right of ownership on anonymised or pseudonimised data. Consequently, this paradigm shift is likely to spark a domino effect and ultimately being applied to all data, personal and non-personal. Yet, the introduction of a right of ownership over personal data can be deemed as a dangerous proposal in several respects. It would call into question the very nature of this protection for individuals and communities in democratic societies, because the commodification of data goes against the essence of the right to data protection, grounded in human dignity.

The option of a right of ownership is mentioned by the Commission as a means to facilitate the sharing of data between actors and, ultimately, of the value being created by this data. At the very least, it would be necessary to study further this proposal in order to demonstrate that the establishment of a right of ownership over non-personal data would bring real benefits. Currently, the sharing of data is organised by contractual means, which can lead to misbalances of power to industrialists' disadvantage vis-à-vis service providers. Yet, there is no evidence that the recognition of a right of data ownership would address this asymmetry. Far from restoring the balance of power between these two parties, the right of data ownership could instead lead to the inclusion of clauses of compulsory divestiture within contractual terms between operators, and thus, increasing the risk of dispossession.

8.3 Rules of Access and Data Sharing

The value created by data use mostly derives from the cross-referencing of datasets. The issue that arises is therefore not so

much that of the protection of investment for the constitution of large databases but, rather, it is that of the incentives to cross-referencing of datasets between various actors. In many instances, data collection and categorisation is a by-product activity of an industrial process: data is a means, not an end in itself. On the other hand, the cross-referencing of datasets serves a new purpose: it is this essential phase, which covers the true potential of Big Data and the emergence of new services, which should be promoted by new incentives. Moreover, in the age of Artificial Intelligence (AI), the matter of data access becomes even more crucial. Frequently, AI algorithms are programmed under open source licenses and, therefore, all the players in the sector can have access to the source code. This means that the main comparative advantage lies in the access to the data used to train the algorithms. Therefore, it is even more necessary to think about the modalities of data sharing between actors in order to ensure that the development of this key technology does not benefit only a few companies able to collect and process a critical mass of data.

In this context, it is critical to consider the situations in which value creation and the development of new uses are dependent on data sharing. These models are yet to be invented. In this regard, two types of reflection must be undertaken. First, we need to consider the modalities of data access by third parties and, second, the means to share data between them.

8.3.1 Rules of Data Access

- *Creation of a right to non-personal data portability in order to allow any individual and company to recover the data generated by its use of a service and to easily transfer these data to another provider.*

Similarly to the portability of personal data enshrined in the GDPR, the portability of non-personal data would facilitate the development of the various markets interested by such data, by encouraging competition between service providers and solution providers. This right could be inspired by article 48 of the French law for a digital Republic, which enshrines an expanded right to portability of all data[356].

356 Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique: <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000033202746&categorieLien=id> [accessed 1 November 2017].

BOX: The right to non-personal data portability

In a digital economy increasingly marked by platforms domination and closed systems, a right to non-personal data portability will facilitate the flow of data "across-platforms" and not just across borders. This right has two objectives:

1 Encourage competition between digital services

This right will enable a company to recover data which has been generated and which are stored and processed by a service provider and to transfer data to another service provider or to use such data internally or as part of commercial and industrial partnerships. This right will concern non-personal data, *i.e*. non-identifying data and, as such, mainly economic and financial, agricultural or industrial data.[357] By facilitating the switching of provider, the right to data portability is intended to promote competition between cloud services.

2 Giving companies control over their data

Beyond the first objective of switching business services, such as cloud services, the right to non-personal data portability would also give companies control over their data. Indeed, the right to non-personal data portability would allow companies to retain control over their data, in the context of a platform economy, where value is usually created and captured by external actors offering services from their users' data. Such right will then make it possible to combat the effects of lock-in and leakage of value by making it possible to develop services in-house or at the level of a professional sector, based on the data recovered.

Moreover, that portability would favour the cross-fertilisation of data from third-party services and, therefore, the emergence

357 Mid-Term review of the Digital Single Market (DSM) – a good moment to take stock : <https://ec.europa.eu/digital-single-market/en/content/mid-term-review-digital-single-market-dsm-good-moment-take-stock> [accessed 1 November 2017]. Examples of non-personal data include tax records such as invoices, accounting documents or documents supporting company registration. Other examples include data on precision farming (helping to monitor and optimise the use of pesticides, nutrients and water) or from sensors communicating the data it records such as temperature or wind conditions in, for instance, wind turbines, or data on maintenance needs for industrial robots for example when they are out of paint.

of new business models, such as Personal Information Management Services (PIMS) for personal data. The value is now in cross-referencing of datasets between various actors. For instance, smart building is a relevant example where many data could be cross-referenced: temperature data could be cross-referenced with the data of the circulation of persons and the data concerning the maintenance of the premises.

By fighting against data silos, the right to non-personal data portability is intended to support the development of a European data industry, in particular for the benefit of the most innovative players, able to challenge the positions acquired.

In order to be efficient, the enshrining of the juridical principle of the non-personal data portability must be supported by a deep study of interoperability standards and technical strategies by granting access to data in particular via Application Programming Interface (API).

The portability of industrial data - an example

Many industrial SMEs have begun a transition of their business and production models. Several companies have already connected machines producing data via the sensors. Generally, these data are often captured and stored by a service provider (*i.e.* the machine manufacturer or a cloud provider). However, it is among its service providers, via data analysis, that more and more services are produced, potentially leading to a situation of leakage of value and dependence.

A right to portability should enable these SMEs to easily retrieve their data and transfer them to another provider without interruption of service. It will also allow these business players to use data internally or together with other businesses in their sector to develop innovative new services.

In order to be efficient, the introduction of the right to non-personal data portability must be supported by a deep study on interoperability standards and technical strategies to access data, in particular via Application Programming Interfaces (API).

- *Identification of situations where data can be considered as infrastructures, where the development of economic products and models is conditional on access to such data, and where it is not possible to reproduce them by reasonable means.*

The viability of industrial projects for semi-autonomous vehicles or intelligent building applications thus depends on the sharing of data between the players in the automotive sector or in the construction sector. Non-discriminatory licensing requirements could thus be established at sectoral level, as provided for in Regulation 715/2007 of 20 June 2007 on the approval of motor vehicles concerning private vehicles' emissions and light commercial vehicles, and information on vehicle repair and maintenance.

- *Revision of Directive 96/9 on databases in favour of a more favourable balance for the circulation of data and for the access to data of certain audiences.*

It seems urgent, for example, to provide for an exception for searches of texts and data in order to enable European researchers to make digital copies or reproductions of a database from a licit source in a scientific non-commercial purposes. Europe and its Member States will have to work towards the diffusion of these techniques in the academic world, bringing great potential for scientific discovery and the development of new knowledge. Rather than creating new forms of ownership that could limit access to scientific data, the aim is to enable the research community to benefit from the progress made possible by data analysis. This exception would allow researchers to carry out automated searches in the vast amount of scientific literature available, particularly in interdisciplinary research that requires cross-referencing databases of a different nature.

8.3.2 Rules of Data Sharing

- *Promotion of the voluntary pooling of data, which may be essential for the realization of major European projects and the development of competitiveness of European companies.*

Member States could encourage different players to share their data, on a voluntary basis, in order to contribute to a research program,

an industrial project or a public policy, either occasionally or on a long-term basis. The pooled data could be collected by a public body and be aggregated before being reused or redistributed, similar to what the US Bureau of Transportations has put in practice by opening US airline data on air navigation. Therefore, experiments in key sectors (health, sustainable development, housing, transport, *etc.*) could be launched at different scales to assess the positive externalities derived from opening the data, both for the companies involved and for society as a whole. Pooling of data among actors could in fact serve many public interest objectives – *i.e.* fostering competition and innovation in specific sectors – is not the only one. Several examples exist in the field of climate change policies: the Intergovernmental Panel on Climate Change (IPCC) for instance opened a Data Distribution Centre (DDC)[358] or the Global Pulse initiative of the United Nations Secretary-General on big data[359].

8.4 Conclusion

The wide potential of data for promoting innovation, growth and well-being is now widely recognized*360*. In order to foster the control by individuals or organisations over the data they produce, or to support the development of a data economy, it can be tempting to create a property right on data. This approach however would miss the specific nature of data as an economic good: it is non-rival and it has not much value in itself. In fact, the value created by data use mostly derives from the cross-referencing of datasets. The issue that arises is therefore not so much that of the protection of investment for the constitution of large databases but rather, it is that of the incentives to cross-referencing of datasets between various actors.

Moreover, data can be reused in many different contexts from the one it was produced or collected. Sometimes it even can't be properly exploited by the actor responsible for its collection alone. For this reason, it is necessary to promote the movement of data between actors in order to maximize its economic and social value.

358 See <http://www.ipcc-data.org/> [accessed 1 November 2017].

359 See <https://www.unglobalpulse.org/about-new> [accessed 1 November 2017].

360 OECD (2015).

How can this free movement be supported? For the French Digital Council, the barriers to data circulation are mainly to be found in lock-in strategies and retention actions among economic actors, rather than in national barriers, which some governments try to address with the implementation of "free flow of data" principle in trade agreements for instance. In its opinion on the initiative suggested by the European Commission, the Council rather considers that decision-makers should primarily pursue the objective of building a framework for the emergence of trust in a data economy that is open, competition-friendly and allows spreading innovation capabilities. In this regard, it seems crucial to carry on the discussion on fostering data sharing and the new usages they may offer. Among them, the Council has suggested to include a right to the portability of data, the granting of new access rights to datasets for research purposes, the support of interoperability of services, as well as the pooling or licensing of shared datasets.

8.5 Bibliography

Bellanger P (2014). *La souveraineté numérique* (Stock, 2014).

Inspection générale des finances et Conseil général de l'économie. (2016). Report on the Free Flow of Data and International Trade Agreements <https://www.economie.gouv.fr/libre-circulation-des-donnees-et-accords-commerciaux> [accessed 1 November 2017].

Lanier J (2014). '*Who Owns the Future?*' (Simon & Schuster, 2014).

Morozov E (2016). 'Data populists must seize our information – for the benefit of us all'. (*The Guardian*, 04 December 2016) <https://www.theguardian.com/commentisfree/2016/dec/04/data-populists-must-seize-information-for-benefit-of-all-evgeny-morozov> [accessed 1 November 2017].

OECD (2015). 'Data-Driven Innovation: Big Data for Growth and Well-Being' (OECD Publishing, 2015).

Zech H (2015). 'Industrie 4.0 - Rechtsrahmen für eine Datenwirtschaft im digitalen Binnenmarkt. Gewerblicher Rechtsschutz und Urheberrecht' (2015) 12 Gewerblicher Rechtsschutz und Urheberrecht, 117.

PART III

New Roles Calling for New Solutions

9 Regulation at the Age of Online Platform-Based Economy: Accountability, User Empowerment and Responsiveness

Marc Tessier, Judith Herzog **and** ***Lofred Madzou***

Abstract

This chapter expresses the views of the French Digital Council on the regulatory challenges associated with the development of the digital platform economy. The Council issues independent opinions and recommendations on any question relating to the impact of digital technologies on the economy and society; as well as advising the French Government and MPs on digital policy issues. In this piece, we expose how our traditional regulatory tools are being challenged by platform development models; we subsequently suggest a comprehensive policy to address those challenges; and finally we illustrate possible fields of intervention for an Agency for Trust in the Digital Platform Economy.

This piece is part of a more comprehensive reflexion on policy issues related to online platforms, developed by the Council since 2013, when the Council organised a consultation with the French plaintiffs involved in the Google Shopping antitrust investigation and elaborated recommendations on several policy issues posed by the rise of digital platforms. Subsequently, in 2014, the former Prime Minister asked the Council to organise a national consultation to elaborate France's digital strategy, addressing concerns of various stakeholders with regard to the lack of transparency of online platform activities and the asymmetry of power in their relationships between platform operators and users. To address these legitimate concerns, we made several recommendations; including the need to develop the technical and policy means to assess the accountability and fairness of online platforms. In 2016, following this recommendation, the government entrusted us with the task of overseeing the creation of an agency with these capabilities. The present reflexion is primarily aimed at providing input to the national and European debate on online platforms. Yet, considering the global reach of these players and the global nature of the issues at stake, we hope that this reflection can also serve foreign audiences.

9.1 Introduction

The rise of the digital platform economy is now an established fact. Indeed, over the last two decades, few online platforms have managed to become some of the most powerful organisations by various metrics. In 2016, the added market capitalisation of GAFA (Google, Amazon, Facebook and Apple) has reached 1,845.45 billion[361], exceeding that of any other economic sectors. If we look at the advertising market, Google and Facebook captured one-fifth of global advertising revenue, earning a combined $106.3 billion, in 2016, doubling their revenue in five years[362]. Yet the impacts of their activities reach far beyond the economic sphere. In fact, it is possible to state that these platforms have disrupted various aspects of our social lives. We increasingly get our news on social media (44 percent of the overall U.S. population accesses news on Facebook[363]), shop on e-commerce platforms (Amazon accounts for 43% of US online retail sales[364]) stream videos on YouTube (80% of European Internet users had used the digital video platform within the past month[365]). The web might be a vast universe of network-accessible information, however, for a significant part of Internet users it all comes down to a few digital "empires," controlled by increasingly powerful actors.

This dominance could adversely affect the economic welfare, as exemplified by the Google shopping antirust case. On 27 June 2017, the European Commission officially revealed its decision to fine Google €2.42 billion for abusing dominance as a search engine by giving an illegal advantage to its own comparison

361 See Oremus (2016). 'Tech Companies Are Dominating the Stock Market as Never Before', *Slate* (29 July 2016). <http://www.slate.com/blogs/moneybox/2016/07/29/the_world_s_5_most_valuable_companies_apple_google_microsoft_amazon_facebook.html> [accessed 31 October 2017].

362 See Kollewe (2017) 'Google and Facebook bring in one-fifth of global ad revenue', *The Guardian* (2 May 2017) <https://www.theguardian.com/media/2017/may/02/google-and-facebook-bring-in-one-fifth-of-global-ad-revenue> [accessed 31 October 2017].

363 See Gottfried & Shearer (2016). 'News Use Across Social Media Platforms 2016' (*Pew Research Center*, 26 May 2016) <http://www.journalism.org/2016/05/26/news-use-across-social-media-platforms-2016/> [accessed 31 October 2017].

364 Business Insider, 'Amazon accounts for 43% of US online retail sales' (*Business Insider*, 03 February 2017) <http://www.businessinsider.fr/us/amazon-accounts-for-43-of-us-online-retail-sales-2017-2/> [accessed 31 October 2017].

365 'Usage penetration of YouTube in global regions as of 3rd quarter 2015' <https://www.statista.com/statistics/483583/youtube-penetration-regions/> [accessed 31 October 2017].

service,[366] closing a seven-year investigation. Margrethe Vestager, the EU competition commissioner, concluded that the company had actually breached EU antitrust rules by both denying other companies the chance to compete on the merits and negating European consumers a genuine choice of services and the full benefits of innovation.[367] The amount of the fine, an EU-record for an antitrust investigation, perfectly illustrates the seriousness of the alleged misconduct and the deep concern of European Institutions about the adverse effects of online platforms practices on economic and social welfare. Indeed, this litigation is part of a more global series of controversies surrounding their activities.

Alongside this case, the Commission also initiated a probe into Google's Android operating system and ordered Apple to pay 13 billion euros in tax clampdown. Parallel to this, the European Commission[368] and several EU member states have taken various legislative initiatives to address sectoral policy issues related to online platform activities. These initiatives have sometimes been harshly criticised by various stakeholders because of several shortcomings, notably the fact that Google is not an adequate example to build policies able to seize the diversity and complexity of online platforms, and that such posture could be harmful to innovation or counterproductive, for instance favouring incumbent actors by raising market entry costs.

Regardless of the diverging opinions on the most appropriate strategy to frame the "platform model," it seems undeniable that some platform providers have managed to acquire a remarkable influence over Internet users. Therefore, there is a pressing need to counterbalance their power; develop the means to hold them accountable to society and maintain the conditions for a competitive environment that allows the arrival of new entrants.

366 See European Commission, 'Antitrust: Commission fines Google ¢2.42 billion for abusing dominance as search engine by giving illegal advantage to own comparison shopping service' <http://europa.eu/rapid/press-release_IP-17-1784_en.htm> [accessed 31 October 2017].

367 *Ibid.*

368 European Commission (2016), 'Communication on Online Platforms and the Digital Single Market Opportunities and Challenges for Europe' <https://ec.europa.eu/digital-single-market/en/news/communication-online-platforms-and-digital-single-market-opportunities-and-challenges-europe> [accessed 31 October 2017].

Yet, focusing only on the GAFA would be a mistake because this would not address the structural causes of the issue at stake, which are related to the platform model, based on generating – and stimulating the generation of – large flows of data, hosting engaged communities, providing useful services, optimising externalities[369] and governing ecosystems. These features have allowed platforms to affect and disrupt numerous fields, such as work and interpersonal relationships, housing and education. However, it is not absurd to argue that platforms could go way further.

Potentially, the platform model could disrupt every aspect of our lives. Thus, because we consider a specific model composed of unique characteristics and flourishing in a distinctive ecosystem, the present reflection would remain relevant even if platforms such as Facebook or Google should terminate their operation. Our focus is much broader than the mere GAFA (Google, Amazon, Facebook and Apple) group. Further, given that various organisations, including "traditional" businesses, associations, political parties and even governments are trying to reproduce some of the platform features to ensure the sustainability of their activities in the Digital Age, we are likely to experience some of its adverse effects more widely in society. Those organisations are particularly appealed by the extreme productivity of the platform model, as explained in the box below.

BOX: What are the features of the platform model?

French law defines as an online platform the operator or any natural or legal person offering, on a professional basis, on a remunerated basis or not, an online public communications service based on[370]:

1. The classification or referencing, by means of computer algorithms, of content, goods or services offered or made available online by third parties;
2. Or, the connections between several parties with a view to the sale of a good, the supply of a service or exchange or sharing of content, good or service.

369 See Biacabe & Vadcar (2017).

370 See Article L111-7 of the French *Code de la consommation*, available at <https://www.legifrance.gouv.fr/ affichCodeArticle> [accessed 1 November 2017].

Their intermediary position operating in-between multi-sided markets, combined with network effects – *i.e.* the fact that more usage of the product by any user increases the product's value for other users – have allowed some platform operators to become critical market access points. In addition, it allows them to develop excellent market knowledge since they design the market they host and collect the information that flows within it. As such, they are uniquely informed about the state of supply (stocks, product's characteristics, prices, *etc.)* and demand (demographics, expressed needs, location, *etc.)* and can leverage this information for various purposes, thus increasing their control over the value chain. This often raises concerns, when platforms compete with their customers in downstream markets by developing their own offerings.

Second, platform operators have the ability to optimise value creation by relying on distributed network of contributors, particularly for research and development (Van Alstyne 2016) and actively coordinate market actors for their own benefits (Benavent 2016). Indeed, the platform model does not simply allow easing transactions between third parties. It allows deploying various techniques to leverage users' capabilities to innovate (as it happens in the case of Salesforce that incentivise users to produce new features that will be subsequently marketed to other clients), produce more content or incentivise users to frequently use their services and thus generate more data (Harris 2015). Furthermore, the platform model does not follow classic horizontal integration strategies of industrial-age companies because their operators understand that the control of the ecosystem is more important than that of the territory (i.e. business partners' assets) as long as they ensure that value creation happens on their platforms.

The systemic and long-term effect of the platform model is not wrong in itself. It actually brings various benefits to Internet users. Consider how much its development has facilitated user access to information and cultural goods, opened up new business opportunities and

reduced transaction costs. Nonetheless, the sustainability of this model depends on its ability to be trusted by those who directly contribute to its success; that is its users, suppliers, and society as a whole. In other words, Metcalfe's law should not undermine its own contributors. Building this trust would depend on our ability, as a society, which includes civil society organisations, regulators, policy makers and businesses, to tackle critical challenges. In this first section, we present these challenges.

9.2 The Shortcomings of Our Traditional Regulatory Tools

Our classic regulatory framework struggles to deal with the policy issues brought about by online platforms because it suffers from three serious shortcomings:

- **The speed of digital cycles**. The European Commission is expected to propose, in September 2017, a legislation to prohibit certain unfair practices of online platforms towards their business partners. This is a positive initiative that many actors have been calling for, over the past years. For instance, it took nearly a decade after the probe of investigation to the Commission to sanction Google for abusing dominance as a search engine by giving an illegal advantage to its Google shopping service. Such delays are not adapted to digital cycles and disproportionately favours incumbents market actors and undermine competition.
- **The diversity of platforms**. Every platform creates its own universe. Even though most of them share the key features exposed in the first section, there is no unique type of platform and they constantly evolve. Consequently, it would be pointless to impose on them one single model of regulation. Instead, each of them should be subject to a specific treatment based on the principles of transparency and accountability. Such treatment would imply, for instance, disclosure of the platform's processes to end users in a format that is understandable and, as far as possible, verifiable by the average user.
- **The opacity of online platforms**. We as a society know very little about the inner functioning of platforms. This informational

asymmetry between them and the rest of us poses a significant democratic problem, because despite being privately owned companies, we can legitimately fear that they leverage their position as powerful intermediaries to engage in practices likely to reduce economic and social welfare. All the more so as they are able to see everything, without being seen. In this respect, they embody digital versions of the Panopticon, as conceptualised by the French Philosopher Michel Foucault. Indeed, they collect a massive amount of data about their users; they govern large ecosystems and markets alike. However, when we raise questions about their recommendation systems, platform can hide behind trade secret. When we insist, they argue that they keep it secret for our own sake, preventing anyone to game the system, besides them. They get to decide, who sees what and when. We have just to accept it or leave it. Thus, there is a pressing need to develop mechanisms to reduce this opacity to mitigate the feeling of impunity that they may develop if this situation persists. This endeavour has led us to primarily criticize the lack of transparency of their activities and to argue for the deployment of enforcement mechanisms of consumers/citizens' rights on online platforms. In fact, our intention is to democratically question their model because it increasingly affects every social domain and deeply challenges our traditional regulatory tools, as we stressed by our previous reports on online platforms.[371] [372]

France took the first step in this direction by adopting the Law for a Digital Republic[373], in an effort to compel platforms to provide consumers with fair, clear and transparent information. This is an excellent start but more should be done. First, we have to collectively improve our capabilities of observation of online platforms. In doing so, we would identify misbehaviours and/or unintended adverse effects more promptly and take the necessary measures

371 Conseil National du Numérique, 'Avis sur les écosystèmes des plateformes : réunir les conditions d'un environnement numérique ouvert et soutenable' <https://cnnumerique.fr/plateformes/> [accessed 1 November 2017].

372 Conseil National du Numérique, Rapport 'Ambition numérique' <https://cnnumerique.fr/plateformes/> [accessed 1 November 2017].

373 Loi pour une République numérique <https://www.legifrance.gouv.fr/affichLoiPubliee.do?idDocument=JORFDOLE000031589829&type=general&legislature=14> [accessed 1 November 2017].

to address them. Second, we should develop inter-regulation mechanisms alone capable of coping with the transversal nature of the policy challenges arising with the digital platform economy. Finally, because online platforms heavily govern the interactions of their users and the latter have limited means to influence the former on how this such interactions should be regulated, we must find ways to empower users in their dialogue with platform operators, as it will be explained in the next section.

In doing so, we would ensure that the development of the digital platform economy respects the democratic aspirations and fosters an atmosphere of trust. Importantly, at the European level, this could be done by associating soft regulation methods to the current regulatory regimes.

9.3 A Proposed Upgrade for the European Regulatory Framework: an Agency for Trust in the Digital Platform Economy

The abovementioned mission should be entrusted to a European independent body whose governance and positioning within the current EU regulatory ecosystem will be discussed during a public consultation, launched by the French Digital Council, in October 2017.[374] In this section, we share our insights, arguing that this body should initiate an open dialogue with the platforms by incentivising them to make commitments vis-à-vis their users and partners.

- A list of concerns to be addressed would be established based on the information gathered by the body and each platform would report their internal policy responses. Their responses would differ according to their respective sectors of activity, modes of operation and sectoral regulations.
- On this basis, the body would organise the conditions of balanced exchanges with online platforms and examine their policy responses. As a mediator, the body would foster dialogue between online platforms and their users/consumers on the one hand, and their business partners on the other hand so that they could formulate their requests to platform operators and

374 See <https://plateformes.cnnumerique.fr/> [accessed 1 November 2017].

analyse their answers. Currently, the Commission is considering the establishment of a *dispute settlement* mechanism between platforms and third-party companies. This could be part of the future agency's prerogatives

- In addition, additional safeguards could be requested from the platforms to ensure the transparency of their operations. More specifically, the body would ensure that the platforms provide the means to audit their own practices while conserving some business confidentiality and the security of collected data, which means that neither their algorithms nor data would be publicly disclosed. It is worth noting that the audit mechanism has yet to be specified because it is a highly political matter and as such should first be discussed among EU member states. This European body for trust in the Digital Economy would then monitor the fulfilment of the commitments made and formulate, where appropriate, additional measures. Doing so would require:
  - Having in-house expertise and technical resources to conduct those assessments: legal knowledge, interface design, sociology, economics, philosophy, reverse engineering (programming, data science). The agency could rely on a global network of experts that it could leverage depending on its needs.
  - Establishing channels for information-gathering based on civil society. First, a public channel which would provide consumers and civil society with a clearly identified contact point to collect concerns and grievances and report them to platform operators (our council is currently experimenting with this process). Then, a confidential channel should be developed to allow businesses, employees and other witnesses of wrong practices to report them without fear of retaliation.

Therefore, it would be an institution of a new kind. It would have no sanctioning power - that is reserved to the courts and independent regulatory authorities - but would make recommendations and have investigative capacities. It would have the right to publicize the results of its investigations. *A fortiori* when a platform does not respect its voluntary commitments or when it refuses to be independently evaluated, the agency could also publicly disclosed the results of its investigation.

These missions would not undermine regulatory authorities but would empower them by facilitating the reporting of misbehaviours; practices that are not illegal per se but which do raise serious concerns among citizens and businesses Also, regulatory authorities and civil society organisations - ill equipped to address their digital-related issues - could seek technical assistance from this agency. Finally, it would help lay down the foundations of the regulatory framework of the digital age, facilitating inter-regulation coordination and play the role of "think tank" that regulatory agencies can only partially fulfil.

To a certain extent, our approach intends to transcend the binary opposition between regulation and non-regulation. Rather, we aim to empower regulators in their mission by helping them to:

- *Make an informed decision*, if it wishes to pass a specific legislation *Establish concrete objectives and measure compliance with these voluntary commitments co-determined with concerned stakeholders,* if it wishes to resort to a soft regulation approach

9.4 Possible fields of intervention of the Agency for Trust in the Digital Platform Economy

To further illustrate the relevance of this agency, here are some concrete fields where it should primarily intervene: content removal, discrimination against end users, transparency on data uses and Business-to-Business relationships. Though this list is not exhaustive, it provides an insightful illustration of the possible implementation of our agency. It is based on some of the major controversies surrounding the rise of online platform observed by the French Digital Council, the European commission and EU member states; most notably France and Germany.

9.4.1 Content Removal

With regards to illegal content, the agency would ensure the traceability of the policies implemented to detect and remove content that promotes violence, justifies terrorism or infringes copyright by gathering the relevant data (e.g: number of requests received, number of requests accepted, onset of action, reason for withdrawal, self and external evaluations of efficiency,

measures taken to address potential side effects, platform by platform comparison, cooperation of the platform for the evaluation,...). In addition, the agency could assess the policies developed by platform operators to limit the spread of "fake news" on their platforms and the implementation of the right to be forgotten, while engaging in a debate with third parties (news outlets, consumer protection associations,...). In the same manner, it would incentivise platforms to involve their users in the development of community standards regarding for instance, whether or not some types of content should be censored beyond the legal requirements.

9.4.2 Discrimination against End-users

The agency would organize the public debate about online platforms liabilities related to the potentially discriminatory effects, established or anticipated, of algorithmic decisions based on data processing. Most notably, the agency could ensure the auditability of dynamic personalization algorithms (content, prices or information). It is essential that those who consider that they have been subject to discriminatory treatments can question these algorithmic systems through independent assessments. Finally, platform operators should justify their positions in the current debate about the effects of their algorithms on society, especially considering the controversy surrounding the economy of attention (filter bubbles).

9.4.3 Transparency on Data Uses

The agency would actively promote transparency measures about data collection, curation, processing, use and sharing with third parties in coordination with national data protection bodies. In the same line of thinking, the disclosure of those processes should enable users to better grasp how the use of their data affects the functioning of their digital services. To this end, the agency could organise various experiments (*e.g.* user testing on terms and conditions) and request additional commitments from platform operators based on their results.

9.4.4 Business to Business Relationships

Various market actors are calling for increased transparency and negotiability about access conditions to platform databases and Application Programming Interfaces (APIs). Most notably, they are concerned about value and asset transfers that they are constrained to accept as well as the restrictions on data portability. As consumer activity continues to move toward digital, consumer-centric companies increasingly depend upon online platforms to get access to markets, which confers a huge power to platform operators and increase the risk of misbehaviour that we described in the second section. Here again, the European Commission has taken legislative measures to regulate the relationships between online platforms and businesses. Yet, they would not be effective if they are not complemented with an open discussion about fair conditions of visibility on online platforms. Above all, companies require at least to be noticed in advance before any significant changes in ranking algorithms and a clarification about the conditions for the uses of the data that the platform gathered about them. Competing firms are particularly threatened when platforms that control access to downstream markets decide to compete in those markets by leveraging the data that they owned about their customers/competitors. Finally, the agency could implement balanced negotiating conditions between the platforms and their independent suppliers (transparency, contractual balances, contributions to social protections and training, *etc.*

9.5 Conclusion

The rise of the digital platform economy deeply challenges our classic regulatory framework organised in silos (consumer rights, privacy, antitrust, etc.) because they have blurred the distinctions between the public and the private spheres, the consumer and the supplier, the citizen and the worker. In doing so, it has undermined something more fundamental; the very concepts that we have relied upon to regulate social and economic interactions in our society. Indeed, what becomes to

consumer optimum in these digital spaces where the consumer is simultaneously user, worker and citizen? What means privacy in the age of ubiquitous social media? What is the future of public sphere at the age of global attention crisis? The apparent solidity of these concepts and the institutions in charge to protect these common goods (consumer optimum, privacy and the public sphere, etc.) appears to be an illusion. Now that their inconsistencies are brought to light by online platforms activities, there is a pressing need to upgrade our regulatory framework to ensure the social sustainability of the "platform model" that is, subjecting its development to the respect of the democratic and sovereign aspirations of citizens. Our proposal of European Agency for trust in the Digital Economy is the first step toward this goal, but this should be a global initiative. You could read this piece as an invitation to join the movement.

9.6 Bibliography

Biacabe. J L & Vadcar C (2017). 'Création de valeur dans un monde numérique' (2017) Institut Friedland.

Business Insider, 'Amazon accounts for 43% of US online retail sales' (*Business Insider*, 3 February 2017) <http://www.businessinsider.fr/us/amazon-accounts-for-43-of-us-online-retail-sales-2017-2/> [accessed 31 October 2017].

Conseil National du Numérique (2014). '*Avis sur les écosystèmes des plateformes: réunir les conditions d'un environnement numérique ouvert et soutenable'* <https://cnnumerique.fr/plateformes/> [accessed 1 November 2017].

Conseil National du Numérique (2015). 'Rapport *Ambition numérique*' <https://cnnumerique.fr/plateformes/> [accessed 31 October 2017].

Conseil National du Numérique (2017). *Predictions, encryption and digital rights*: <https://cnnumerique.fr/wp-content/uploads/2017/09/CNNum_avis_predictions_encryption_freedoms_sept2017.pdf>, 2017.

Conseil National du Numérique (2015b). 'Rapport *travail, emploi, numérique — Les nouvelles trajectoires'* <https://cnnumerique.fr/wp-content/uploads/2015/12/Rapport-travail-version-finale-janv2016.pdf> [accessed 31 October 2017].

European Commission (2016). 'Communication on Online Platforms and the Digital Single Market Opportunities and Challenges for Europe' <https://ec.europa.eu/digital-single-market/en/news/communication-online-platforms-and-digital-single-market-opportunities-and-challenges-europe> [accessed 31 October 2017].

Kollewe J (2017). 'Google and Facebook bring in one-fifth of global ad revenue', *The Guardian* (2 May 2017) <https://www.theguardian.com/media/2017/may/02/google-and-facebook-bring-in-one-fifth-of-global-ad-revenue> [accessed 31 October 2017].

Gottfried J & Shearer E (2016). 'News Use Across Social Media Platforms 2016' (*Pew Research Center*, 26 May 2016) <http://www.journalism.org/2016/05/26/news-use-across-social-media-platforms-2016/> [accessed 31 October 2017].

Oremus W (2016). 'Tech Companies Are Dominating the Stock Market as Never Before', *Slate* (29 July 2016) <http://www.slate.com/blogs/moneybox/2016/07/29/the_world_s_5_most_valuable_companies_apple_google_microsoft_amazon_facebook.html> [Accessed 31 October 2017].

10 Countering Terrorism and Violent Extremism Online: What Role for Social Media Platforms?

Krisztina Huszti-Orban[375]

Abstract

Social media platforms have been facing considerable pressure on part of States to 'do more' in the fight against terrorism and violent extremism online. As a result, many social media companies have set up individual and joint efforts to spot unlawful content in a more efficient manner, thereby becoming the de facto regulators of online content and the gatekeepers of freedom of expression and interlinked rights in cyberspace. However, having corporate entities carry out quasi-executive and quasi-adjudicative tasks, outsourced to them by governments under the banner of self- or co-regulation, raises a series of difficult questions under human rights law.

This paper outlines the main human rights challenges arising in this context, by reference to European Union laws and policies as well as Member State practices. It argues that the lack of internationally agreed definitions of violent extremism and terrorism-related offences raises the risk of excessive measures with potential cross-border human rights implications. It further notes the problems linked to attempts aimed at broadening the liability of Internet intermediaries in the counter-terrorism context. The paper raises the need to provide social media platforms with human rights-compliant guidance on conducting content review, the criteria used in this respect and the specialist knowledge required. It also stresses the role of transparency, accountability and independent oversight, particularly in light of the public interest role that social media platforms play by regulating content in the interest of preventing and countering terrorism and violent extremism.

375 This work was supported by the UK's Economic and Social Research Council [grant number ES/M010236/1].

10.1 Introduction: the Role and Influence of Social Media Platforms

The Internet and Information Communication Technologies (ICTs) have, in the past couple of decades, rewired the way society functions. Access to and use of the Internet and ICTs has now become essential to the conduct of government operations, to business, and to individuals' day-to-day lives in many countries. In this sense, the United Nations Human Rights Council has affirmed the importance of 'applying a comprehensive human rights-based approach in providing and in expanding access to the Internet.'[376]

In light of the capacity of ICTs to store and communicate vast amounts of information as well as their relative accessibility, they play an important role in enhancing the public's access to seek, receive and impart information. They enable governments to communicate with their constituencies but similarly facilitate the dissemination of messages by other actors. Indeed, many argue that online platforms have become the digital age equivalent of public squares where individuals gather to share and debate views and opinions.[377] Just recently, the Supreme Court of the United States has held that access to social media was a constitutional right.[378]

Unlike public squares, however, these outlets are privately owned and operated[379], and, while most offer their services 'free of charge'[380], access to them cannot be construed as a right in the sense access to public spaces can. At the same time, due to their reach and use, some of these online platforms arguably play a public

376 United Nations Human Rights Council (June 2016). *Resolution on the promotion, protection and enjoyment of human rights on the Internet* (A/HRC/RES/32/13).

377 See Alissa Starzak, 'When the Internet (Officially) Became the Public Square' (*Cloudfare,* 21 June 2017) <https://blog.cloudflare.com/internet-became-public-square/> [accessed 2 November 2017]. ; Ephrat Livni 'The US Supreme Court just ruled that using social media is a constitutional right' (*Quartz,* 19 June 2017) <https://qz.com/1009546/the-us-supreme-court-just-decided-access-to-facebook-twitter-or-snapchat-is-fundamental-to-free-speech/> [accessed 2 November 2017].

378 *Packingham v. North Carolina* 582 U.S. ___ (2017) (Supreme Court of the United States).

379 The Editorial Board, 'Facebook Is Not the Public Square' *The New York Times* (25 December 2014) <https://www.nytimes.com/2014/12/26/opinion/facebook-is-not-the-public-square.html.> [accessed 2 November 2017].

380 Membership on these platforms is free in the sense that there is no membership fee. However, users 'pay' for services offered with their data.

interest role. The largest social media platforms can demonstrate extremely high levels of user activity[381] and interactivity[382], with a staggering amount of content generated by the day, the hour, and even by the minute. This allows them to reach broad and diverse audiences in a manner that was not feasible before.[383]

Studies show that people have increasingly been getting their news from social media.[384] Social media platforms have been instrumental in disseminating information about political developments at home and abroad, humanitarian crises, as well as allegations of human rights violations and abuses committed by States and non-state actors.[385] Moreover, the role of social media in facilitating advocacy for political change and even coordinating protest is well-documented.[386]

The full picture needs to be considered in light of technological developments that have provided for new means and modalities for controlling information and content available online. Online platforms and those who provide and facilitate access to them have considerable power in shaping information that is disseminated, that is, they have the *de facto* authority when it

381 Facebook has close to 2 billion monthly active users. YouTube has over 1 billion. Instagram has 700 million. Twitter has 313 million.

382 It has been reported that every 60 seconds on Facebook 510,000 comments are posted, 293,000 statuses are updated, and 136,000 photos are uploaded. In this sense, see Zephoria Digital Marketing, 'The Top 20 Valuable Facebook Statistics' (*Zephoria*, 01 November 2017) <https://zephoria.com/top-15-valuable-facebook-statistics/> [accessed 2 November 2017]. The daily video content watched on YouTube has reached 1billion hours this year. See YouTube Official Blog, 'You know what's cool? A billion hours' (*Youtube*, 27 February 2017) https://youtube.googleblog.com/2017/02/you-know-whats-cool-billion-hours.html [accessed 2 November 2017].

383 Governments and other public authorities, United Nations entities and other international and regional organizations, as well as private actors use these outlets in an attempt to have their messaging disseminated. See Dave Chaffey, 'Global social media research summary 2017' (*Smart insights*, 27 April 2017) <http://www.smartinsights.com/social-media-marketing/social-media-strategy/new-global-social-media-research/> [accessed 2 November 2017].

384 See Jordan Crook, '62% of U.S. adults get their news from social media, says report' (*Techcrunch*, 26 May 2016) <https://techcrunch.com/2016/05/26/most-people-get-their-news-from-social-media-says-report/> [accessed 2 November 2017]; Jane Wakefield, 'Social media 'outstrips TV' as news source for young people' (*BBC News*, 15 June 2016) <http://www.bbc.co.uk/news/uk-36528256> [accessed 2 November 2017].

385 Cristoph Koettl, 'Twitter to the Rescue? How Social Media is Transforming Human Rights Monitoring' (*Amnesty USA Blog*, 20 February 2013) <http://blog.amnestyusa.org/middle-east/twitter-to-the-rescue-how-social-media-is-transforming-human-rights-monitoring/>[accessed 2 November 2017].

386 Garside (2011). ''Rioters' use of social media throws telecoms firms into spotlight', *The Guardian* (21 August 2011) <https://www.theguardian.com/business/2011/aug/21/riots-throw-telecoms-firms-social-media-controls-into-spotlight> [accessed 2 November 2017]; Chidi (2016).

comes to regulating online content. Through this power, relevant actors can exert significant influence over individuals' access to information, freedom of opinion, expression, and association, and over interlinked political and public interest processes.[387]

Against the above set out background, this paper outlines the main human rights challenges arising in the context of social media's role in the fight against terrorism and violent extremism online, by reference to European Union (EU) laws and policies as well as Member State practices.[388] It does so by addressing 1) the implications of the lack of internationally agreed definitions of violent extremism and terrorism-related offences; 2) issues linked to attempts aimed at broadening the liability of Internet intermediaries in this context; and 3) the importance of a human rights-compliant approach on part of relevant companies.

10.2 State Trends to Outsource Online (Content) Policing

As a result of the previously outlined developments, the private sector now plays an increasingly substantial role in providing governments with tools and assistance for censorship. As highlighted by the Special Rapporteur on freedom of expression, the capacity of states in this regard may 'depend on the extent to which business enterprises cooperate with or resist' such measures.[389]

Host providers face increasing pressure to monitor and police content generated or disseminated by users. This trend is further motivated by the use of ICTs as a tool for recruitment, financing and planning of operations by terrorist and violent

387 Schneier (2015:114-116).

388 The reason for choosing to demonstrate related issues by reference to the EU framework lies on the one hand in the more detailed nature of EU regulation and its interpretation as well as in the existence of numerous current developments at the EU and Member State level. Many of the concerns raised are however valid beyond the EU.

389 United Nations Human Rights Council (June 2016). *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*. (A/HRC/32/38), para. 57; see also United Nations Human Rights Council (June 2017). *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*. (A/HRC/35/22), para. 1.

extremist groups.[390] Discussions on the role and responsibilities of social media in preventing and countering terrorism and violent extremism were re-ignited in the wake of recent attacks perpetrated by individuals linked to or inspired by ISIL,[391] with pressure mounting on social media companies to 'do more'.[392]

In response, the tech industry attempted to tackle the problems posed by terrorist or extremist third-party content through coordinated initiatives as well as standalone measures. Coordinated initiatives include the EU Internet Forum[393], the Shared Industry Hash Database[394] as well as the Global Internet Forum to Counter Terrorism,[395] to name a few. Individually, companies have pledged to take further action to counter the use of their platforms for terrorist and other unlawful purposes by employing artificial intelligence as well as 'human expertise' to identify 'extremist and

390 See Brendan Koerner 'Why ISIS IS Winning the Social Media War', *The Guardian (*21 August 2011) <https://www.wired.com/2016/03/isis-winning-social-media-war-heres-beat/> [accessed 2 November 2017]; David Fidler, 'Countering Islamic State Exploitation of the Internet', *Council on Foreign Relations, (*18 June 2015) <https://www.cfr.org/report/countering-islamic-state-exploitation-internet> [accessed 2 November 2017]. See also United Nations Office on Drugs and Crime (2012:3-13) <https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf> [accessed 2 November 2017]. Reports indicate that social media platforms, such as Facebook also host black market sites where individuals can seek out and purchase items such as firearms or even the services of a hit person. See Beer (2017) 'Pumpgun? Gefällt mir!', *Die Zeit* (26 April 2017) <http://www.zeit.de/2017/18/strafverfolgung-facebook-schwarzmarkt-waffen-internet>[accessed 2 November 2017].

391 Sparrow & Hern (2017), 'Internet firms must do more to tackle online extremism, says No 10', *The Guardian* (24 March 2017) <http://www.theguardian.com/media/2017/mar/24/internet-firms-must-do-more-to-tackle-online-extremism-no-10> [accessed 2 November 2017]; Elgot 'May and Macron plan joint crackdown on online terror', *The Guardian* (12 June 2017) <https://www.theguardian.com/politics/2017/jun/12/may-macron-online-terror-radicalisation> [accessed 2 November 2017].

392 Amar Toor 'France and the UK consider fining social media companies over terrorist content', *The Verge* (13 June 2017) <https://www.theverge.com/2017/6/13/15790034/france-uk-social-media-fine-terrorism-may-macron> [accessed 2 November 2017]; Gibbs (2017), 'Facebook and YouTube face tough new laws on extremist and explicit video', *The Guardian* (24 May 2017) <https://www.theguardian.com/technology/2017/may/24/facebook-youtube-tough-new-laws-extremist-explicit-video-europe> [accessed 2 November 2017]; McCann (2017), 'Facebook 'must pay to police internet or face fines: UK Parliament', *The Canberra Times* (01 May 2017) <http://www.canberratimes.com.au/technology/technology-news/facebook-must-pay-to-police-internet-20170430-gvvz2e.html> [accessed 2 November 2017].

393 European Commission. (2016), *EU Internet Forum: a major step forward in curbing terrorist content on the internet. Press release* <http://europa.eu/rapid/press-release_IP-16-4328_en.htm>. [accessed 2 November 2017].

394 Google, 'Partnering to help curb the spread of terrorist content online', *Google Keyword* (5 December, 2016) <https://www.blog.google/topics/google-europe/partnering-help-curb-spread-terrorist-content-online/>. [accessed 2 November 2017].

395 Microsoft Corporate Blogs, 'Facebook, Microsoft, Twitter and YouTube announce formation of the Global Internet Forum to Counter Terrorism', *Microsoft Blog* (26 June 2017) <https://blogs.microsoft.com/on-the-issues/2017/06/26/facebook-microsoft-twitter-youtube-announce-formation-global-internet-forum-counter-terrorism/> [accessed 2 November 2017].

terrorism-related' content.[396] Some companies are also involved in counter-radicalization initiatives. For example, Google and YouTube work with Jigsaw using targeted online advertising to reach potential ISIL sympathizers with counter-messaging.[397]

10.3 Social Media Platforms and the Counter-terrorism Agenda

States and international organizations have long called for public-private partnerships to aid efforts to counter terrorism and violent extremism. The Secretary-General's Plan of Action to Prevent Violent Extremism[398] calls for concerted action involving the private sector at national, regional and international level. To the extent such efforts include regulation of online content hosted by social media platforms, such action cannot meaningfully be undertaken without the cooperation of the respective companies. The challenge however revolves around defining the contours of such cooperation. How should responsibilities be divided between the public and private spheres? What are the legitimate expectations that can be imposed on companies and what are the aspects that public authorities need to take responsibility for? The answers to these questions are neither obvious nor uncontroversial.

Legally speaking, related corporate obligations are included in a variety of laws, among others those tackling hate speech, cybercrime, counter-terrorism, violent extremism and intermediary liability. Many jurisdictions also encourage self and co-regulation.

396 See, for example, Google, 'Four steps we're taking today to fight terrorism online', *Google Keyword* (18 June 2017) <https://www.blog.google/topics/google-europe/four-steps-were-taking-today-fight-online-terror/> [accessed 2 November 2017]; Monika Bickert & Brian Fishman 'Hard Questions: How We Counter Terrorism', *Facebook Newsroom* (15 June 2017) <https://newsroom.fb.com/news/2017/06/how-we-counter-terrorism/> [accessed 2 November 2017]; Twitter Inc. 'An update on our efforts to combat violent extremism' (*Twitter Blog*, 18 August 2016) <https://blog.twitter.com/official/en_us/a/2016/an-update-on-our-efforts-to-combat-violent-extremism.html> [accessed 2 November 2017].

397 Taylor Hatmaker 'YouTube launches its counter-terrorism experiment for would-e ISIS recruits' (*Techcrunch*, 20 July 2017) <https://techcrunch.com/2017/07/20/google-jigsaw-redirect-method-launch-youtube-isis/>. See also O'Hara (2016) 'The Limits of Redirection', *Slate* (27 September 2016) <http://www.slate.com/articles/technology/future_tense/2016/09/the_problem_with_google_jigsaw_s_anti_extremism_plan_redirect.html> [accessed 2 November 2017].

398 United Nations General Assembly (2015, December 24). *Plan of Action to Prevent Violent Extremism. Report of the Secretary-General*. (A/70/674).

Potential human rights implications raised by the role social media platforms play in the counter-terrorism effort will be addressed below.

10.3.1 Terrorism and Violent Extremism: Definitional Dilemmas

Despite numerous treaties, Security Council resolutions and other international and regional instruments addressing terrorism-related issues,[399] there is no internationally agreed definition of terrorism or an agreed list of terrorism-related offences. As a result, these notions are addressed in accordance with State laws and policies, leading to considerable discrepancies between different domestic frameworks. United Nations human rights mechanisms and other stakeholders have repeatedly raised concerns about the implications of overly broad definitions of terrorism and related offences.[400]

Particularly pertinent to our context are ancillary offenses (including providing material support to terrorism, incitement to terrorism and, newly, 'glorification', 'praise' or 'justification' of terrorism).[401] Under counter-terrorism frameworks, platforms will likely be called to remove content that amounts to incitement to terrorism, 'glorification' of terrorism or a related offence. However, platforms may themselves end up on the wrong side of the law. The presence of material contravening

399 See United Nations Counter-Terrorism Implementation Task Force, *International Legal Instruments*. Retrieved from <https://www.un.org/counterterrorism/ctitf/en/international-legal-instruments> [accessed 2 November 2017].

400 See, for example, United Nations General Assembly (July 2013), *Protecting human rights and fundamental freedoms while countering terrorism. Report of the Secretary-General*. (A/68/298); United Nations Human Rights Council (December 2019). *Report of the United Nations High Commissioner for Human Rights on the protection of human rights and fundamental freedoms while countering terrorism* (A/HRC/28/28); International Commission of Jurists (2009), *Report of the Eminent Jurists Panel on Terrorism, Counter-terrorism and Human Rights*.

401 The UN Human Rights Committee has stressed that offences such as 'praising', 'glorifying', or 'justifying' terrorism must be clearly defined to ensure that they do not lead to unnecessary or disproportionate interferences with freedom of expression. See United Nations Human Rights Committee (2011, September 12), *General Comment 34. Article 19: Freedoms of opinion and expression* (CCPR/C/GC/34), para. 46. Similarly, the Secretary-General and the UN Special Rapporteur on counter-terrorism have expressed concerns about the 'troubling trend' of criminalising the glorification of terrorism, stating that this amounts to an inappropriate restriction on expression. See United Nations General Assembly (2008, August 28). *Protecting human rights and fundamental freedoms while countering terrorism. Report of the Secretary-General* (A/63/337) and United Nations Human Rights Council (2016, February 22). *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism* (A/HRC/31/65).

counter-terrorism legislation on a platform may, under certain circumstances, qualify as material support to terrorism. Moreover, advertising revenue derived from videos with 'terrorist content' may be penalized as terrorist financing.[402]

Laws and policies addressing violent extremism similarly raise definitional concerns. While the term "violent extremism" and related notions, such as "extremism" and "radicalization" are prominently present in current political discourse at the international, regional and national levels, none of these terms have internationally agreed definitions.[403]

Definitions are therefore found in domestic laws and policies. Many of these have however been criticized for being vague and at times encompassing manifestations that are lawful under international human rights law.[404] Moreover, in some jurisdictions these concepts have become dissociated from violence[405], thereby raising the potential for abusive implementation, as such definitions risk to selectively blur the distinction between belief and violent conduct. Under the guise of preventing 'extremism', almost any kind of views that deviate from the social norms accepted by the majority may be suppressed and measures may target thought, belief, and opinion,

---

402 See House of Commons Home Affairs Committee (2017, April 25). *Hate crime: abuse, hate and extremism online*, p 10.

403 Acknowledging this shortcoming, the Secretary-General in his Plan of Action to Prevent Violent Extremism stated that violent extremism is to be defined at the national level, while emphasizing that such definitions must be consistent with obligations under international human rights law. Violent extremism and terrorism are at times defined in a similar manner or even used interchangeably. The conditions conducive to terrorism (identified in Pillar I of the Global Counter-Terrorism Strategy) and to violent extremism (identified in the Secretary-General's Plan of Action) are also largely identical. While the Plan of Action stressed that violent extremism encompassed a wider category of manifestations than terrorism, it is not clear how it proposes to distinguish the two terms.

404 See United Nations Human Rights Council. (February 2016), *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism* (A/HRC/31/65) and United Nations Human Rights Council (July 2016), *Report on best practices and lessons learned on how protecting and promoting human rights contribute to preventing and countering violent extremism. Report of the United Nations High Commissioner for Human Rights* (A/HRC/33/29).

405 A number of countries also target 'extremism' that is non-violent. For example, extremism is defined in the United Kingdom as "the vocal or active opposition to fundamental values, including democracy, the rule of law, individual liberty and the mutual respect and tolerance of different faiths and beliefs." See HM Government. *Prevent Strategy* (2011), Annex A; HM Government. *Counter-Extremism Strategy* (2015, October), para. 1. However, the more the concept becomes dissociated from violence, the more the potential of abuse is raised.

rather than actual conduct.[406] This is of particular concern where legislation creates criminal offences based on these definitions.

The potential and actual uses of the counter-terrorism and preventing violent extremism framework to stifle dissent, persecute journalists, human rights defenders and the political opposition, restrict civil society space, and to criminalize the work of humanitarian organizations has been addressed at length elsewhere.[407] Online platforms having to operationalize such laws and policies may find themselves contributing to the negative human rights impact of these frameworks, in contradiction with their responsibilities under the UN Guiding Principles on Business and Human Rights.[408]

Due to the non-territorial nature of cyberspace, the impact of local laws may also reach beyond the territory of the State enacting and enforcing them, potentially impacting the human rights of individuals that are not within the respective State's jurisdiction. This means that the discrepancy in domestic frameworks may have far-reaching effects that are difficult to monitor and related jurisdictional complexities have the potential to make redress difficult or even impossible.

10.3.2 The Counter-terrorism Framework and Rules on Intermediary Liability

Online platforms, as outlets that host or store user-generated content and enable access to and retrieval of this content by the

406 Under international human rights law, however, no exceptions or restrictions are permissible to the right to hold an opinion (see Article 19(1), *International Covenant on Civil and Political Rights*; United Nations Human Rights Committee (September 2011), *General Comment 34. Article 19: Freedoms of opinion and expression*. (CCPR/C/GC/34), para. 9) and freedom to have or adopt a religion or belief of one's choice is also protected unconditionally. See Article 18(1), *International Covenant on Civil and Political Rights*; United Nations Human Rights Committee (July 2013), *General Comment No. 22: Article 18 (Freedom of Thought, Conscience or Religion)*. (CCPR/C/21/Rev.1/Add.4), paras. 2-3.

407 See, for example, Interagency Standing Committee (2004). *Sanctions Assessment Handbook: Assessing the Humanitarian Implications of Sanctions*. (United Nations); Mackintosh and Duplat (2013), *Study of the Impact of Donor Counter-Terrorism Measures on Principled Humanitarian Action*. Report commissioned by United Nations Office for the Coordination of Humanitarian Affairs and the Norwegian Refugee Council; Banisar (2008). *Speaking of Terror. A survey of the effects of counter-terrorism legislation on freedom of the media in Europe*. (Council of Europe); Hayes (2012). *Counter-terrorism, 'policy laundering' and the FATF: legalizing surveillance, regulating civil society*. (Transnational Institute/ Statewatch); Duke Law International Human Rights Clinic and Women Peacemakers Program (2017). *Tightening the Purse Strings: What Countering Terrorism Financing Costs Gender Equality and Security*.

408 The Guiding Principles were endorsed by the Human Rights Council in Resolution 17/4 of 16 June 2011.

author and other users,[409] qualify as Internet intermediaries. Such intermediaries, as opposed to authors and publishers of content, are generally protected against liability for third-party content, with certain caveats. The scope of this exemption differs in different jurisdictions.[410] Under the EU's e-Commerce Directive, hosting intermediaries do not incur liability as long as they 'expeditiously' remove or disable access to illegal content once they have 'actual knowledge' of its existence.[411] Existing jurisprudence suggests that providing content organization (such as cataloguing, indexing, search algorithms), even if done for profit, does not exclude the host from liability exemption.[412]

Imposing a general obligation to monitor content or to 'actively seek facts or circumstances indicating illegal activity' go against EU law.[413] Similarly, so-called stay-down injunctions, involving an obligation to ensure that once certain content has been removed, it will not reappear on the platform, are also problematic to the extent their implementation requires general monitoring of content.

The idea of introducing such burden on intermediaries has however surfaced in current debates. For example, the United Kingdom House of Commons Home Affairs Committee has recommended that Internet intermediaries proactively identify illegal content and expressed dissatisfaction with such platforms only reviewing content after having been flagged by users or other stakeholders

409 Horten (2016:5).

410 See Article 19 (2013); Goldman (2016).

411 Article 14, *Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (e-Commerce Directive)*.

412 The European Court of Justice held that such exemption from liability only exists where the role played by the provider is neutral 'in the sense that its conduct is merely technical, automatic and passive, pointing to a lack of knowledge or control of the data which it stores'. See Judgment of the Court (Grand Chamber) of 23 March 2010. Joined cases C-236/08 to C-238/08, *Google France SARL and Google Inc. v Louis Vuitton Malletier SA* (C-236/08), *Google France SARL v Viaticum SA and Luteciel SARL* (C-237/08) *and Google France SARL v Centre national de recherche en relations humaines (CNRRH) SARL and Others* (C-238/08), paras. 110ff. See also *Reti Televisive Italiane S.p.A. (RTI) v. Yahoo! Italia S.r.l. (Yahoo!) et al.* 3821/2011. (2015) (Milan Court of Appeal, Italy). See also Marco Berliri & Giulia Mariuz, '*The Court of Appel of Milan rules on Yahoo's liability with respect to copyright infringement*' (HL Media Comms, 25 February 2015) (WITH "HL Media <http://www.hlmediacomms.com/2015/02/25/the-court-of-appeal-of-milan-rules-on-yahoos-liability-with-respect-to-copyright-infringement/> [accessed 2 November 2017].

413 Article 15, e-Commerce Directive. See also Case C-360/10 (2012), *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v. Netlog NV*. EU:C:2012:85.

and for not ensuring that blocked and removed content does not resurface.[414]

At the same time, the internal consistency of EU legislation may also leave something to desire. Article 28a of the review proposal to the Audio-Visual Media Services (AVMS) Directive[415] provides that video-sharing platforms must take measures to 'protect all citizens' from content containing incitement to violence, discrimination or hate.[416] In addition to providing for a rather vague definition of such content,[417] the provision may be interpreted as requiring proactive monitoring.[418]

In addition to such far-reaching obligations being incompatible with the e-Commerce Directive, they may also be problematic from a human rights perspective as their implementation may require imposing prior restraint. Human rights concerns posed by far-reaching intermediary liability, and, in particular, its negative impact on freedom of speech and interlinked rights, have already been flagged by international human rights mechanisms[419] and

414 House of Commons Home Affairs Committee, *Hate crime: abuse, hate and extremism online* (25 April 2015). See also Elliot Harmin, *'"Notice-and-Stay-Down" Is Really "Filter-Everything"'* (*EFF Deeplinks*, 21 January 2016) <https://www.eff.org/deeplinks/2016/01/notice-and-stay-down-really-filter-everything> [accessed 2 November 2017].

415 European Commission (2016). *Proposal for a Directive of the European Parliament and of the Council 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 in view of changing market realities,* <http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52016PC0287&from=EN> [accessed 2 November 2017].

416 See European Digital Rights (EDRi). 'EDRi's analysis on the CULT compromise on Article 28a of the draft Audiovisual Media Services Directive (AVMSD) proposal'. (*EDRi*, 13 April 2017) <https://edri.org/files/AVMSD/compromise_article28a_analysis_20170413.pdf> [accessed 2 November 2017].

417 For example, a compromise amendment under discussion provides for the following: 'protect all citizens from content containing incitement undermining human dignity, incitement to terrorism or content containing incitement to violence or hatred directed against a person or a group of persons defined by reference to nationality, sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or *any other opinion*, membership of a national minority, property, birth, disability, age, gender, gender expression, gender identity, sexual orientation, residence status or health.' (emphasis added) See European Parliament, Committee on Civil Liberties, Justice and Home Affairs (2016), *Amendments 47-171* (2016/0151(COD)).

418 While the draft explicitly mentions that it is without prejudice to articles 14 and 15 of the e-Commerce Directive, the intended scope of the duty of care is still unclear. See also Horten. (2016:14); Frosio (2017).

419 See United Nations Human Rights Council (June 2017), *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression* (A/HRC/35/22), para. 49. See also, Joint declaration by the United Nations (UN) Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media, the Organization of American States (OAS) Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information, presented at the UNESCO World Press Freedom Day event (3 May 2016).

civil society actors.[420] Nonetheless, calls for stricter regulation of intermediary liability to counter terrorism, violent extremism and hate speech have been heard in numerous jurisdictions. Proposals include imposing fines and other sanctions on social media platforms "'that fail to take action' against terrorist propaganda and violent content",[421] and even having social media companies bear the costs of authorities policing content online.[422] The introduction of criminal liability for platforms was discussed and ultimately discarded by the European Parliament in the context of the Directive on Combating Terrorism.

At Member State level, Germany has recently adopted the controversial[423] Network Enforcement Act[424]. While the law is only applicable to social media platforms with more than two million registered users, the obligations contained therein are onerous. Platforms falling within the ambit of the law face a fine of up to 5 million Euros in case they fail to remove or block access to 'clearly illegal' content within 24 hours[425] and other illegal content within 7 days[426] after having been put on notice through a complaint (including user complaints). The law includes no guidance on how to distinguish 'clearly illegal' entries from merely 'illegal' ones. The Act entered into

420 See Article 19 (2013).

421 Amar Toor, 'France and the UK consider fining social media companies over terrorist content', *The Verge* (13 June 2017) <https://www.theverge.com/2017/6/13/15790034/france-uk-social-media-fine-terrorism-may-macron> [accessed 2 November 2017]; Gibbs, 'Facebook and YouTube face tough new laws on extremist and explicit video', *The Guardian* (24 May 2017) <https://www.theguardian.com/technology/2017/may/24/facebook-youtube-tough-new-laws-extremist-explicit-video-europe> [accessed 2 November 2017].

422 See House of Commons Home Affairs Committee. (2017); Kate McCann, 'Facebook 'must pay to police internet' or face fines: UK Parliament', *The Canberra Times*, (01 May 2017) <http://www.canberratimes.com.au/technology/technology-news/facebook-must-pay-to-police-internet-20170430-gvvz2e.html> [accessed 2 November 2017].

423 'Wirtschaft und Aktivisten verbünden sich gegen Maas-Gesetz', *Der Spiegel* (11 April 2017) <http://www.spiegel.de/netzwelt/netzpolitik/heiko-maas-wirtschaft-und-netzszene-protestieren-gegen-hassrede-gesetz-a-1142861.html> [accessed 2 November 2017].

424 *Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken [Netzwerksdurchsetzungsgesetz - NetzDG]* 2017 (Germany) <https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/NetzDG.pdf?__blob=publicationFile&v=2> [accessed 2 November 2017].

425 Unless the social media network agrees a different timeline with the competent law enforcement authority. See Netzwerksdurchsetzungsgesetz, Article 1 §3 (2) No. 2. The draft law originally provided for a fine of up to 50 million Euros.

426 Unless the unlawful character of the content in question depends on factual circumstances to be determined or unless the social media network transmits the case to an authorized self-regulatory mechanism (Einrichtung der regulierten Selbstregulierung). *Netzwerksdurchsetzungsgesetz*, Article 1 §3 (2) No. 3.

force on 1 October 2017 and will inevitably influence how major social media sites will approach users' freedom of expression, the threat of hefty fines being a clear incentive to over-censor in case of doubt. The impact of the law will in all probability extend beyond Germany's borders due to the cross-border nature of information flows but also due to the likelihood of copycat laws springing up.[427]

These developments will likely also force the EU to explore the compatibility of the e-Commerce Directive with other instruments addressing the role of Internet intermediaries in combating hate speech and other illegal content, such as the Directive on Combating Terrorism or the AVMS Directive, the latter currently under review. In light of the decision not to reopen the e-Commerce Directive, it is likely that diffusing tension between these instruments will require significant level of self- and/ or co-regulation. In this sense, the European Commission is exploring the need to issue a Guidance on voluntary measures.[428] It is also expected to announce measures that set common requirements for companies when it comes to removing illegal content, applicable across the bloc, as a means to avoid 'overzealous rules that differ between EU countries'.[429]

Potential human rights concerns raised by such rules resulting from self- and/ or co-regulation are discussed below.

10.3.3 Social Media Companies as *de facto* Content Regulators

Online platforms generally filter, remove or otherwise restrict content on the basis of their terms of service and community standards and, when pertinent and necessary, domestic law.

Terms of service and community standards instituted by platforms commonly impose restrictions that go beyond what the State could

427 A new Russian draft law has reportedly incorporated many of the elements of the German law, however, with even broader obligations, extending to fake news, defamation and libel. Elena Chernievska, OSCE, Office of the Representative on Freedom of the Media, presentation at the Conference on Freedom of Expression: Facing up to the Threat, organised by the Qatar National Human Rights Committee, in cooperation with the International Press Institute (IPI) and the International Federation of Journalists (IFJ), 24-25 July 2017, Doha.

428 European Commission (June 2017), *Liability of Internet Intermediaries* <https://ec.europa.eu/digital-single-market/en/liability-online-intermediaries> [accessed 2 November 2017].

429 Catherine Stupp, 'Gabriel to start EU expert group on fake news' (*Euractiv* 30 August 2017) <https://www.euractiv.com/section/digital/news/gabriel-to-start-eu-expert-group-on-fake-news/> [accessed 2 November 2017].

lawfully impose in compliance with its obligation to respect freedom of expression.[430] As privately-run outlets, social media platforms can of course decide to shape the content hosted by them in order to facilitate the creation of a space that fits their business model, by enabling a more family-friendly or minor-friendly environment, for example. This however becomes problematic if we are to accept that some of these platforms also fulfil public interest functions. With this premise, restricting speech in a manner that goes against internationally recognized free speech standards becomes unacceptable.

10.3.3.1 Informal State-business Cooperation

Censorship in accordance with terms of service or community standards may also cause for concern when States use extra-legal and/or informal means to coerce or influence businesses to interfere with user content. For example, in some countries public authorities resort to flagging content as violations of company terms of service and community standards.[431] This approach creates the risk that States expand their possibilities to have content blocked, filtered, or removed beyond what is provided for under national law and what would be permissible under international human rights law. Even if the respective public authorities only request restrictions that they deem to be in accordance with the law, this method may result in undermining the regular safeguards that protect against excessive interference, including the right to an effective remedy, as the end decision is ultimately delegated to private entities who are thereby effectively given law enforcement and quasi-adjudicative responsibilities.[432]

---

430 Elizabeth Nolan Brown, 'YouTube Says No to Sexual Humor, Profanity, Partial Nudity, Political Conflict, and 'Sensitive Subjects' in Partner Content' (*Reason*, 01 September 2016) <http://reason.com/blog/2016/09/01/youtube-bans-sex-drugs-and-politics> [accessed 2 November 2017]; Twitter, *Twitter media policy*. <https://support.twitter.com/articles/20169199> [accessed 2 November 2017]; Facebook, *Community standards* <https://www.facebook.com/communitystandards#nudity> [accessed 2 November 2017].

431 In this respect, countries have also created dedicated counter-terrorism flagging units, such as the British Counter-Terrorism Internet Referral Unit or the European Union Referral Unit. See, for example, Joseph Menn, 'Social media companies step up battle against militant propaganda' (*Reuters*, 07 December 2015) <http://www.reuters.com/article/us-california-shooting-socialmedia-insig-idUSKBN0TO0OS20151207#GKDRWLDec4JBQEYI.97> [accessed 2 November 2017]. See also Center for Democracy and Technology, 'Pressuring Platforms to Censor Content is Wrong Approach to Combat Terrorism' (*CDT*, 05 November 2015) <https://cdt.org/blog/pressuring-platforms-to-censor-content-is-wrong-approach-to-combatting-terrorism/> [accessed 2 November 2017].

432 See European Digital Rights (EDRi), 'The Slide from "Self-Regulation" to "Corporate Censorship"'. <https://edri.org/files/EDRI_selfreg_final_20110124.pdf> [accessed 2 November 2017].

10.3.3.2 Means and Modalities of Content Review

Many platforms use a mixture of artificial intelligence and human expertise to review and moderate content. Using algorithms to assess compliance with the law, terms of service and community standards provides for a time-efficient way for dealing with large volume of material. Algorithms however are not fault-proof, which may lead to screening that is over- or under-inclusive. For example, algorithms are not necessarily well-equipped to understand context, different forms of humour, and may not pick up on certain subtleties. For this reason, certain kinds of material are best dealt with by humans. Unfortunately, most social media platforms do not provide meaningful information on content review procedures and the criteria that determines whether certain content will be reviewed by artificial intelligence, human moderators, or both.[433]

At the same time, having content reviewed by human moderators does not necessarily lift all concerns. Assessing what may amount to hate speech, incitement to terrorism, 'glorification' of terrorism or violent extremist content frequently requires a rather sophisticated analysis. This in turn would require social media platforms to employ a highly trained and specialized workforce. Reports however indicate that it is frequently low-paid and insufficiently trained moderators that end up being the *de facto* 'sentinels' of freedom of expression online.[434]

433 For example, Facebook disclosed that the use of artificial intelligence to spot terrorist content is relatively new and it comes with some limitations, causing the company to also employ human expertise in dealing with such entries. See Monika Bickert, Brian Fishman, 'Hard Questions: How We Counter Terrorism' (*Facebook Newsroom*, 15 June 2017) <https://newsroom.fb.com/news/2017/06/how-we-counter-terrorism/> [accessed 2 November 2017]. While the so-called 'Facebook files' provide some insight into the moderation process, many questions remain. Moreover, moderation policies of other major social network platforms remain obscure.

434 Olivia Solon, 'Counter-terrorism was never meant to be Silicon Valley's job. Is that why it's failing?' (*The Guardian*, 29 June 2017) <https://www.theguardian.com/technology/2017/jun/29/silicon-valley-counter-terrorism-facebook-twitter-youtube-google>; Olivia Solon, 'Underpaid and overburdened: The life of a Facebook moderator', *The Guardian* (25 May 2017) <https://www.theguardian.com/news/2017/may/25/facebook-moderator-underpaid-overburdened-extreme-content>. Facebook has indicated the number of persons involved in content moderation (some employed for Facebook, others working for contractors such as Arvato in Germany). Employees interviewed by media platforms claimed that they were expected to review around 2000 posts per day, leaving less than 10 seconds for the assessment of a single post. See Till Krause & Hannes Grassegger 'Inside Facebook', *Süddeutsche Zeitung* (15 December 2016) <http://www.sueddeutsche.de/digital/exklusive-sz-magazin-recherche-inside-facebook-1.3297138>; Nick Hopkins, 'Facebook struggles with 'mission impossible' to stop online extremism', *The Guardian* (24 May 2017) <https://www.theguardian.com/news/2017/may/24/facebook-struggles-with-mission-impossible-to-stop-online-extremism> [accessed 2 November 2017]. Corresponding information about the moderation policies and processes of other major social media platforms is not publicly available.

Many large social media platforms operate worldwide (or at least in numerous jurisdictions). This makes it difficult or even impossible to come up with a universally valid set of rules for their algorithms and moderators. As such rules need to take into account the differences between domestic legal systems and the scope of prohibited content in different jurisdictions as well as linguistic, cultural and other contexts, certain discrepancies in approach will be inevitable.

10.3.3.3 Transparency and Accountability

Information on means and modalities of content control exercised by online platforms is scarce and, even when available, rather murky. Terms of service and community standards are commonly drafted in vague terms and do not provide sufficiently clear guidance on the circumstances under which content may be blocked, removed or restricted or access to a service restricted or terminated, including the criteria used for such assessments. Facebook's Director of Global Policy Management, Monika Bickert explained that the company does not share details of their policies to avoid encouraging people 'to find workarounds'.[435] On the negative side, this approach means reduced transparency and may as a result lead to reduced accountability.

Information provided *ex post facto* (if at all) is similarly lacking. Users are frequently not informed of the origin of removal requests, the procedure that led to removal or rejection of removal and the criteria used. They also have limited possibilities to challenge decisions to restrict material or access to a service. This is even more valid when it comes to challenging decisions rejecting requests for removal.

To tackle this shortcoming, the German Network Enforcement Act requires companies to report on a biannual basis about means and modalities for handling complaints and to disclose, among others, the criteria for removing or blocking content. It similarly calls on companies to inform both the complainant and the user affected

435 Monika Bickert, 'At Facebook we get things wrong – but we take our safety role seriously', *The Guardian* (22 May 2017) <https://www.theguardian.com/commentisfree/2017/may/22/facebook-get-things-wrong-but-safety-role-seriously> [accessed 2 November 2017].

by the measure and give reasons for the decision. The law however comes short of requiring companies to provide users with the option to challenge decisions.

As relevant measures by private companies are usually not taken pursuant to specific legislation, it is frequently not possible to challenge them in court. This may be the case even when such platforms remove content pursuant to it having been flagged by state authorities. Moreover, as private bodies, such platforms are generally not subject to any sort of democratic or independent oversight.[436] Removing the possibility of independent, including judicial, review of measures that interfere with human rights is problematic in general and particularly so in the current climate. Businesses are potentially facing fines and sanctions imposed by states if they do not restrict unlawful content. On the other hand, should they remove lawful content in the process, affected individuals have limited ways of redress. In case of doubt businesses will more likely err on the side of over-censoring.

10.4 Safeguarding Freedom of Expression and Related Rights: Whose Job is It Anyway?

The duty of States to protect persons within their jurisdiction from undue interference with their human rights by third parties, including businesses, is well-established. It requires States to adopt reasonable and adequate legislative and other measures to protect relevant rights, including the right to freedom of opinion and expression.

Against the above background, a plausible argument can be made that States may be falling behind on their obligation to protect freedom of expression and interlinked rights. As discussed above, there seems to be a clear tendency on part of States to effectively outsource certain law enforcement-linked tasks to private outlets, particularly in the counter-terrorism context. The tendency can in part be explained by political expediency: this approach provides the opportunity to shift the blame onto social media platforms if and when terrorist or

436 Zachary Loeb, 'Who moderates the moderators? The Facebook files' (*B2O*, 07 June 2017) <http://www.boundary2.org/2017/06/zachary-loeb-who-moderates-the-moderators-on-the-facebook-files/> [accessed 2 November 2017].

violent extremist incidents or hate crimes occur. At the same time, there are also legitimate practical justifications for stressing the role and responsibility of social media companies. Due to the control and influence they exercise over content on their platforms, meaningful action could not be taken without their cooperation.

However, States should aim at the establishment of veritable public–private partnerships to address illegal content disseminated online, as opposed to merely outsourcing the implementation of domestic laws and policies. While it is inevitable for relevant private actors to play an increasingly significant role, including the taking up of quasi-executive and quasi-adjudicative tasks, this should not be done without proper guidance and safeguards. At this point, however, the outsourcing results in lowering or removing existing human rights safeguards and protections. Social media companies are stuck with tasks that they are not particularly well equipped to carry out. For example, it is questionable whether private actors, in particular corporations, are well placed to assess whether a particular measure is necessary and proportionate in the interest of national security or public order. Social media platforms should be given clear and detailed instructions and guidance if they are to carry out such assessments. Moreover, if control over elements of the right to freedom of expression is outsourced to these outlets, independent oversight of their conduct in this respect needs to be ensured in order to guarantee transparency, accountability, and respect for the right to remedy of individuals whose rights are unjustly interfered with in the process.

10.5 Conclusion

As the Special Rapporteur on freedom of expression noted in his latest report to the Human Rights Council, 'the intersection of State behaviour and corporate roles in the digital age remains somewhat new for many States.'[437]

Having private actors, such as social media companies, increasingly undertake traditionally public tasks in the context of Internet

437 United Nations Human Rights Council (June 2017), *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression* (A/HRC/35/22), para. 81.

governance is likely unavoidable, if for no other reason, for lack of alternatives. The state apparatus (including the judiciary) in most States does not have the human or technical resources to satisfactorily perform these tasks. For this reason, a better understanding and in-depth exploration of related challenges is crucial in light of the Internet having become an indispensable enabler of freedom of expression and allied rights.

Businesses can undoubtedly do more to mitigate the negative human rights impact of their newly-found role. For adequate results, however, a series of additional steps are needed, and these steps should be guided and spearheaded by governments.

10.6 Bibliography

Article 19 (2013). 'Internet Intermediaries: Dilemma of Liability' (*Article 19*, 2013).

Beer I (2017). 'Pumpgun? Gefällt mir!', *Die Zeit* (26 April 2017) <http://www.zeit.de/2017/18/strafverfolgung-facebook-schwarzmarkt-waffen-internet> [accessed 11 November 2017].

Berliri M and Mariuz G (2015). 'The Court of Appel of Milan rules on Yahoo's liability with respect to copyright infringement' (*Hogan Lovells*, 25 February 2015) <http://www.hlmediacomms.com/2015/02/25/the-court-of-appeal-of-milan-rules-on-yahoos-liability-with-respect-to-copyright-infringement/> [accessed 10 November 2017].

Bickert M and Fishman B (2017). 'Hard Questions: How We Counter Terrorism', (*Facebook Newsroom*, 15 June 2017) <https://newsroom.fb.com/news/2017/06/how-we-counter-terrorism/> [accessed 11 November 2017].

Center for Democracy and Technology (2015). 'Pressuring Platforms to Censor Content is Wrong Approach to Combat Terrorism', (*CDT*, 5 November 2015) <https://cdt.org/blog/pressuring-platforms-to-censor-content-is-wrong-approach-to-combatting-terrorism/> [accessed 11 November 2017].

Chaffey D (2017). 'Global social media research summary 2017', (*Smart insights*, 27 April 2017) <http://www.smartinsights.com/social-media-marketing/social-media-strategy/new-global-social-media-research/> [accessed 11 November 2017].

Chidi A M and Chimes I N (2016). 'Social Media and Political Change in the 21st Century: the African Experience' (2016) 1 Glocalism: Journal of Culture, Politics and Innovation 1.

Cristoph K (2013). 'Twitter to the Rescue? How Social Media is Transforming Human Rights Monitoring' (*Amnesty USA Blog*, 20 February 2013) <http://blog.amnestyusa.org/middle-east/twitter-to-the-rescue-how-social-media-is-transforming-human-rights-monitoring/> [accessed 11 November 2017].

Crook J (2016). '62% of U.S. adults get their news from social media, says report' (*Techcrunch,* 26 May 2016) <https://techcrunch.com/2016/05/26/most-people-get-their-news-from-social-media-says-report/> [accessed 11 November 2017].

Elgot J (2017). 'May and Macron plan joint crackdown on online terror', *The Guardian* (12 June 2017) <https://www.theguardian.com/politics/2017/jun/12/may-macron-online-terror-radicalisation> [accessed 11 November 2017].

European Commission. 'EU Internet Forum: a major step forward in curbing terrorist content on the internet', (European Commission, 08 December 2016), <http://europa.eu/rapid/press-release_IP-16-4328_en.htm> [accessed 11 November 2017].

European Commission. 'Liability of online intermediaries' <https://ec.europa.eu/digital-single-market/en/liability-online-intermediaries> [accessed 11 November 2017].

European Commission. 'Proposal for a Directive of the European Parliament and of the Council 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 in view of changing market realities' <http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52016PC0287&from=EN> [accessed 11 November 2017].

European Digital Rights (EDRi) (2017). 'EDRi's analysis on the CULT compromise on Article 28a of the draft Audiovisual Media Services Directive (AVMSD) proposal', (*EDRi*, 13 April 2017) <https://edri.org/files/AVMSD/compromise_article28a_analysis_20170413.pdf> [accessed 11 November 2017].

European Digital Rights (EDRi). 'The Slide from "Self-Regulation" to "Corporate Censorship', EDRI Discussion Paper 01/2011 <https://edri.org/files/EDRI_selfreg_final_20110124.pdf> [accessed 11 November 2017].

European Parliament, Committee on Civil Liberties, Justice and Home Affairs (2016). Amendments 47-171 (2016/0151(COD)).

Fidler D (2015). 'Countering Islamic State Exploitation of the Internet', (Council on Foreign Relations, 18 June 2015) <https://www.cfr.org/report/countering-islamic-state-exploitation-internet> [accessed 11 November 2017].

Frosio G (2017). 'Reforming Intermediary Liability in the Platform Economy: A European Digital Single Market Strategy' (2017), 112 Northwestern University Law Review 19.

Garside J (2011). 'Rioters' use of social media throws telecoms firms into spotlight', (The Guardian, 21 August 2011), <https://www.theguardian.com/business/2011/aug/21/riots-throw-telecoms-firms-social-media-controls-into-spotlight> [accessed 11 November 2017].

Gibbs S (2017). 'Facebook and YouTube face tough new laws on extremist and explicit video' *The Guardian* (24 May 2017) <https://www.theguardian.com/technology/2017/may/24/facebook-youtube-tough-new-laws-extremist-explicit-video-europe> [accessed 11 November 2017].

Goldman E (2016). 'Facebook Isn't Liable for Fake User Account Containing Non-Consensual Pornography', *Forbes* (08 March 2016,) <https://www.forbes.com/sites/ericgoldman/2016/03/08/facebook-isnt-liable-for-fake-user-account-containing-non-consensual-pornography/#40ba670379b2> [accessed 11 November 2017].

Google (2016). 'Partnering to help curb the spread of terrorist content online' (*Google Blog*, 05 December, 2016) <https://www.blog.google/topics/google-europe/partnering-help-curb-spread-terrorist-content-online/> [accessed 11 November 2017].

Google (2017). 'Four steps we're taking today to fight terrorism online', (*Google Keyword*, 18 June 2017) <https://www.blog.google/topics/google-europe/four-steps-were-taking-today-fight-online-terror/> [accessed 11 November 2017].

Harmon E (2016). '"Notice-and-Stay-Down' Is Really 'Filter-Everything'" (EFF, 21 January, 2016) <https://www.eff.org/deeplinks/2016/01/notice-and-stay-down-really-filter-everything> [accessed 11 November 2017].

Hatmaker T (2017). 'YouTube launches its counter-terrorism experiment for would-e ISIS recruits', (*Techcrunch*, 20 July 2017) <https://techcrunch.com/2017/07/20/google-jigsaw-redirect-method-launch-youtube-isis/> [accessed 11 November 2017].

HM Government (2011). 'Prevent Strategy (2011), Annex A'.

HM Government (2015). 'Counter-Extremism Strategy' (2015).

Hopkins N (2017). 'Facebook struggles with 'mission impossible' to stop online extremism', *The Guardian* (24 May 2017) <https://www.theguardian.com/news/2017/may/24/facebook-struggles-with-mission-impossible-to-stop-online-extremism> [accessed 11 November 2017].

Horten M (2016). 'Content 'responsibility': The looming cloud of uncertainty for internet intermediaries' (*CDT*, 06 September 2016) <https://cdt.org/insight/content-responsibility-the-looming-cloud-of-uncertainty-for-internet-intermediaries/> [accessed 11 November 2017].

House of Commons Home Affairs Committee (25 April 2017). 'Hate crime: abuse, hate and extremism online'.

Interagency Standing Committee (2004). 'Sanctions Assessment Handbook: Assessing the Humanitarian Implications of Sanctions' (United Nations, 2004).

International Commission of Jurists (2009). 'Report of the Eminent Jurists Panel on Terrorism, Counter-terrorism and Human Rights' (ICJ, 2009).

Koerner B (2011). 'Why ISIS IS Winning the Social Media War', *The Guardian*, (21 August 2011) <https://www.wired.com/2016/03/isis-winning-social-media-war-heres-beat/> [accessed 11 November 2017].

Krause T and Grassegger H (2016). 'Inside Facebook' *Süddeutsche Zeitung* (15 December 2016) <http://www.sueddeutsche.de/digital/exklusive-sz-magazin-recherche-inside-facebook-1.3297138> [accessed 11 November 2017].

Livni E (2017). 'The US Supreme Court just ruled that using social media is a constitutional right' (*Quartz*, 19 June 2017) <https://qz.com/1009546/the-us-supreme-court-just-decided-access-to-facebook-twitter-or-snapchat-is-fundamental-to-free-speech/> [accessed 11 November 2017].

Loeb Z (2017). 'Who moderates the moderators? The Facebook files' (*B2O*, 07 June 2017) <http://www.boundary2.org/2017/06/zachary-loeb-who-moderates-the-moderators-on-the-facebook-files/> [accessed 11 November 2017].

Mackintoshh K and Duplat P (2013). 'Study of the Impact of Donor Counter-Terrorism Measures on Principled Humanitarian Action' (2013). Report commissioned by United Nations Office for the Coordination of Humanitarian Affairs and the Norwegian Refugee Council.

McCann K (2017). 'Facebook 'must pay to police internet' or face fines: UK Parliament'. *The Canberra Times* (01 May 2017) <http://www.canberratimes.com.au/technology/technology-news/facebook-must-pay-to-police-internet-20170430-gvvz2e.html> [accessed 11 November 2017].

Menn J (2015). 'Social media companies step up battle against militant propaganda' (*Reuters*, 07 December 2015) <http://www.reuters.com/article/us-california-shooting-socialmedia-insig-idUSKBN0TO0OS20151207#GKDRWLDec4JBQEYI.97> [accessed 11 November 2017].

Microsoft Corporate Blogs (2017). 'Facebook, Microsoft, Twitter and YouTube announce formation of the Global Internet Forum to Counter Terrorism' (*Microsoft Blog*, 26 June 2017) <https://blogs.microsoft.com/on-the-issues/2017/06/26/facebook-microsoft-twitter-youtube-announce-formation-global-internet-forum-counter-terrorism/> [accessed 11 November 2017].

Bickert M (2017). 'At Facebook we get things wrong – but we take our safety role seriously' (*The Guardian*, 22 May 2017) <https://www.theguardian.com/commentisfree/2017/may/22/facebook-get-things-wrong-but-safety-role-seriously> [accessed 11 November 2017].

Nolan Brown E (2016). 'YouTube Says No to Sexual Humor, Profanity, Partial Nudity, Political Conflict, and 'Sensitive Subjects' in Partner Content', (*Reason*, 01 September 2016) <http://reason.com/blog/2016/09/01/youtube-bans-sex-drugs-and-politics> [accessed 11 November 2017].

O'Hara K (2016). 'The Limits of Redirection ' *Slate* (27 September 2016) <http://www.slate.com/articles/technology/future_tense/2016/09/the_problem_with_google_jigsaw_s_anti_extremism_plan_redirect.html> [accessed 11 November 2017].

Schneier B (2015). *Data and Goliath: The Hidden Battle to Collect Your Data and Control Your Word* (W.W. Norton & Company, 2015).

Shirky C (2011). 'The Political Power of Social Media: Technology, the Public Sphere and Political Change' (2011) 90 (1) Foreign Affairs 28.

Solon O (2017). 'Counter-terrorism was never meant to be Silicon Valley's job. Is that why it's failing?', *The Guardian* (29 June 2017) <https://www.theguardian.com/technology/2017/jun/29/silicon-valley-counter-terrorism-facebook-twitter-youtube-google> [accessed 1 November 2017].

Solon O (2017). 'Underpaid and overburdened: The life of a Facebook moderator', *The Guardian* (25 May 2017) <https://www.theguardian.com/news/2017/may/25/facebook-moderator-underpaid-overburdened-extreme-content> [accessed 1 November 2017].

Sparrow A and Hern A (2017). 'Internet firms must do more to tackle online extremism, says No 10', *The Guardian* (24 March 2017) <http://www.theguardian.com/media/2017/mar/24/internet-firms-must-do-more-to-tackle-online-extremism-no-10> [accessed 1 November 2017].

Spiegel (2017). 'Wirtschaft und Aktivisten verbünden sich gegen Maas-Gesetzz', *Der Spiegel* (11 April 2017) <http://www.spiegel.de/netzwelt/netzpolitik/heiko-maas-wirtschaft-und-netzszene-protestieren-gegen-hassrede-gesetz-a-1142861.html> [accessed 1 November 2017].

Starzak A (2017). 'When the Internet (Officially) Became the Public Square', (*Cloudfare*, 21 June 2017) <https://blog.cloudflare.com/internet-became-public-square/> [accessed 1 November 2017].

Stupp C (2017). 'Gabriel to start EU expert group on fake news', (*Euractiv*, 30 August 2017) <https://www.euractiv.com/section/digital/news/gabriel-to-start-eu-expert-group-on-fake-news/> [accessed 11 November 2017].

Toor A (2017). 'France and the UK consider fining social media companies over terrorist content', (*The Verge*, 46 June 2017) <https://www.theverge.com/2017/6/13/15790034/france-uk-social-media-fine-terrorism-may-macron> [accessed 11 November 2017].

The Editorial Board (2014). 'Facebook Is Not the Public Square', *The New York Times* (25 December 2014), <https://www.nytimes.com/2014/12/26/opinion/facebook-is-not-the-public-square.html> [accessed 11 November 2017].

Twitter Inc (2016). 'An update on our efforts to combat violent extremism', (*Twitter Blog*, <18 August 2016). https://blog.twitter.com/official/en_us/a/2016/an-update-on-our-efforts-to-combat-violent-extremism.html> [accessed 11 November 2017].

Twitter, 'Twitter media policy', <https://support.twitter.com/articles/20169199> [accessed 1 November 2017].

United Nations Counter-Terrorism Implementation Task Force, 'International Legal Instruments' <https://www.un.org/counterterrorism/ctitf/en/international-legal-instruments> [accessed 1 November 2017].

United Nations General Assembly (2013). 'Protecting human rights and fundamental freedoms while countering terrorism', Report of the Secretary-General (A/68/298).

United Nations General Assembly (2015). 'Plan of Action to Prevent Violent Extremism', Report of the Secretary-General (A/70/674).

United Nations Human Rights Committee (2011). 'General Comment 34. Article 19: Freedoms of opinion and expression' (CCPR/C/GC/34).

United Nations Human Rights Council (2014). 'Report of the United Nations High Commissioner for Human Rights on the protection of human rights and fundamental freedoms while countering terrorism' (A/HRC/28/28).

United Nations Human Rights Council (2016). 'Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism' (A/HRC/31/65).

United Nations Human Rights Council (2016). 'Report on best practices and lessons learned on how protecting and promoting human rights contribute to preventing and countering violent extremism'. Report of the United Nations High Commissioner for Human Rights. (A/HRC/33/29).

United Nations Human Rights Council (2016). 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression' (A/HRC/32/38).

United Nations Human Rights Council (2016). 'Resolution on the promotion, protection and enjoyment of human rights on the Internet' (A/HRC/RES/32/13).

United Nations Human Rights Council (2017). 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression' (A/HRC/35/22).

United Nations Office on Drugs and Crime (2012). 'The use of the Internet for terrorist purposes' (United Nations, 2012) <https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf> [accessed 11 November 2017].

Wakefield J (2016). 'Social media 'outstrips TV' as news source for young people', (*BBC News*, 15 June 2016) <http://www.bbc.co.uk/news/uk-36528256> [accessed 11 November 2017].

YouTube Official Blog (2017). 'You know what's cool? A billion hours' (*Google Blog*, 27 February 2017) <https://youtube.googleblog.com/2017/02/you-know-whats-cool-billion-hours.html> [accessed 11 November 2017].

Zephoria Digital Marketing (2017). 'The Top 20 Valuable Facebook Statistics', (Zephoria, 01 November 2017) <https://zephoria.com/top-15-valuable-facebook-statistics/> [accessed 11 November 2017].

11 Revenue Chokepoints: Global Regulation *by* Payment Intermediaries

Natasha Tusikov

Abstract

Payment intermediaries are becoming go-to regulators for governments and, in a recent development, for multinational corporations intent on protecting their valuable intellectual property rights. Intermediaries undertake many of these regulatory efforts in the absence of legislation and formal legal orders in what is commonly termed "voluntary industry regulation." Those intermediaries that dominate the online payment industry (namely Visa, MasterCard and PayPal) can enact revenue chokepoints that starve targeted entities of sales revenue or donations. This paper explores how major payment intermediaries act as global regulators, especially in the context of "voluntary" regulation, and considers the effects on Internet governance. In its case study, the paper explores why the U.S. government in 2011 pressured payment intermediaries into a non-legally binding enforcement campaign to protect intellectual property rights. The paper argues that governments strategically employ the narrative of "voluntary intermediary-led" in order to distance the state from problematic practices. Further, it contends that payment intermediaries' regulatory efforts are part of a broader effort to shape Internet governance in ways that benefit largely western legal, economic, and security interests, especially those of the United States. To make this argument, the paper draws upon interviews with policymakers, intermediaries, and rights holders in the United States. It concludes that intermediary-facilitated regulation raises serious challenges, especially when payment providers act as private regulators for private actors' material benefit.

11.1 Introduction

The torch-lit march of heavily armed white supremacists in Charlottesville, Virginia in August 2017, which ended with the death of civil rights activist Heather Heyer, highlighted the role of Internet intermediaries in policing content online. In the days after

Heyer's death, Google, PayPal, GoDaddy, Spotify, and Apple all withdrew their services from white supremacist groups (Tusikov 2017). The violence in Charlottesville underlined the extent to which large, globally operating intermediaries have become the new global regulators responsible for policing an array of online wrongdoing. These companies are important regulators because they provide essential services in the online environment, such as search, payment, domain name, or web hosting services. Google, PayPal and Facebook have a considerable regulatory capacity because of their global platforms, significant market share, and sophisticated enforcement capacities that protect their systems and users from wrongdoing like fraud or spam.

Payment intermediaries facilitate online payment processing and transactions, and by withdrawing their payment services, these intermediaries can seriously disrupt the capacity of businesses or individuals to generate revenue by raising donations or selling goods and services. Payment intermediaries are ideal gatekeepers given the market concentration and the high barriers to entry in the payment industry (Mann & Belzley, 2005, p. 258). Payment processing is also more difficult, costly, and time consuming to replace than domain names or web hosts as these sectors have considerable competition, and websites can easily acquire new domain or hosting services. Financial services are therefore "a 'weak point' in the value chain" (McCoy et al., 2012, p. 15). While the payment industry is evolving with the growth of cryptocurrencies, particularly Bitcoin, Visa, PayPal and MasterCard, along with American Express remain highly popular and trusted payment methods. Large-scale commercially oriented websites generally offer one or more of these popular payment options.

When the dominant payment providers withdraw their services, they can effectively establish chokepoints that starve the targeted entities of revenue and cut them off from the global marketplace. For example, following WikiLeaks' release of classified U.S. diplomatic cables in 2010, the U.S. government pressured intermediaries to terminate their services to the organization. PayPal, Visa and MasterCard did so, terminating their payment-processing services. Julian Assange, WikiLeaks' leader, characterised the payment

blockade as an "economic death sentence" and reported that it wiped out 95 percent of WikiLeaks' revenue (Press Association 2012). Intermediaries' control over the provision of payment processing thus accords them significant regulatory power.

Importantly, payment providers like other Internet intermediaries, can act in the absence of formal legal orders as they draw legal authority from their contractual terms-of-service agreements with their users. This means that payment intermediaries can act independently – and sometimes arbitrarily – against companies or entities that they contend violate their policies. Even when the content or behaviour in question is legal, intermediaries can terminate their services to their users. The capacity for arbitrary regulation is thus baked into intermediaries' internal rules.

Two questions guide the paper: how do major payment intermediaries act as global regulators and with what effects on Internet governance? Internet governance broadly refers to the "ongoing set of disputes and deliberations over how the Internet is coordinated, managed, and shaped to reflect policies" (Mueller, 2010, p. 9). To explore these questions, the paper examines payment intermediaries' regulatory efforts on behalf of rights holders of multinational intellectual property like Nike. This paper argues that the state plays a key role in directing specific regulatory outcomes, often strategically employing the narrative of "voluntary intermediary-led" regulation in order to distance the state from any problematic practices. Regulation in this context refers to the practice of setting and enforcing rules, standards, and policies both through formal and informal means by state or non-state actors.

To make its argument, the paper draws upon the regulatory literature to explain state coercion in ostensibly voluntary regulatory arrangements. For its case study, the paper explores the U.S. government's recruitment of Visa, MasterCard and PayPal into a non-legally binding enforcement campaign to withdraw their services from websites selling counterfeit goods (a form of trademark infringement) and copyright-infringing content, such

as unauthorized downloads of music, movies, and software.[438] The paper offers original research from twenty interviews with policymakers, intermediaries, and rights holders in the United States.

11.2 Payment Intermediaries Become Global Regulators

Brick-and-mortar financial institutions have a long history of working with governments to detect and prevent suspicious or illegal transactions, as part of efforts related to anti-money laundering and anti-terrorist financing legislation (Levi, 2010). Since the late 1990s, payment intermediaries have worked with various governments to address issues of online criminality. Importantly, many of these efforts occur voluntarily, that is in the absence of legislation or formal legal orders. In 1996, for example, the U.K. government brought together Internet companies, including payment providers, to target websites offering the sale of child sexual abuse content.[439] Similarly, in the early 2000s, the U.S. government designated payment providers as responsible for tracking and blocking online payments related to child pornography, unlawful sales of tobacco, and Internet gambling (see MacCarthy, 2010). These efforts are proactive, instead of in response to formal legal orders. The payment providers decline to process payments related to these issues and, where relevant, terminate their payment processing services to targeted websites.

Between the late 1990s and early 2000s, as e-commerce evolved rapidly and online shopping and file sharing become commonplace, and so did the illicit trade in copyright-infringing content and counterfeit goods. Multinational intellectual property owners, like Nike and their representatives, such as the Motion Picture Association of America, lobbied governments in the United States and European Union to force intermediaries to assume greater regulatory responsibility for the distribution of intellectual property-infringing goods (Tusikov, 2016). In response to intense

438 Copyright law lays out rules that determine how knowledge and creative and artistic works like music, films, and books can be accessed, used, and shared, by whom, and with what technologies. Trademark law determines the entities that can lawfully manufacture, distribute, advertise, and sell trademarked products.

439 This organization, the Internet Watch Foundation, is a non-profit group funded, in part, by the European Union and by Internet companies like Google, and it counts PayPal among its membership (see Laidlaw, 2015).

industry pressure, the U.S. and U.K. governments and the European Commission each created programs, between 2010 and 2011, to pressure multiple intermediaries, including payment providers to withdraw their services from targeted websites voluntarily (see Tusikov, 2016).[440] The United Kingdom, for example, created the world's first non-legally binding code of conduct for search engines to remove search results relating to copyright-infringing content (Tusikov, 2016). The European Commission, meanwhile, created a similar program for marketplaces operating within the European Economic Area to remove sales listings for counterfeit goods (see Tusikov, 2016).

In the United States, a small office is at the epicentre of informal regulatory efforts to combat intellectual property rights infringement, the Office of the U.S. Intellectual Property Enforcement Coordinator (IPEC). In 2010, officials from IPEC initiated negotiations among payment intermediaries. The goal was a non-legally binding agreement in which intermediaries would police their platforms for the trade in counterfeit and copyright-infringing goods. Victoria Espinel, who was then head of IPEC, said the agreements "encourage practical and effective voluntary actions to address repeated acts of infringement" (Espinel, 2011, p. 7).

Government officials often term these arrangements, in the words of Espinel, "voluntary best practices" (Espinel, 2012). The term "voluntary," is a misnomer as the threat of legislation hung over the negotiations. While Espinel was discussing voluntary industry regulation with the payment intermediaries, the U.S. Congress debated two intellectual property bills: the *Combating Online Infringement and Counterfeits Act* and the *Protecting Intellectual Property Act* (PIPA) that were forerunners to the later much-maligned and controversial *Stop Online Piracy Act* (SOPA). These three bills failed to pass, and PIPA and SOPA in particular elicited unprecedented online protests as opponents argued they would increase censorship and destabilize the technical functioning of the Internet (see Sell, 2013). These bills would have required

440 These programs involve payment, search, advertising, marketplace and domain name intermediaries withdrawing their services from websites involved in distributing copyright-infringing and counterfeit goods (see Tusikov, 2016).

payment intermediaries to withdraw their services from websites distributing counterfeit goods and copyright-infringing content aimed at U.S. consumers.

Intermediaries were motivated to adopt the non-legally binding agreements in order to avoid possible stricter legislative requirements. Payment providers also conceded direct pressure from Espinel was also a factor in adopting informal regulatory agreements.[441] A senior executive at MasterCard candidly acknowledged Espinel's role in shaping the informal agreements: "We have, thanks to Ms. Espinel, an established best-practices policy that all of us have signed up for, a set of minimum standards that many of us far exceed" (Kirkpatrick, 2012).

11.2.1 Non-binding Enforcement Agreements

In June 2011, Espinel announced that major payment providers "reached an agreement to develop voluntary best practices to withdraw payment services for sites selling counterfeit and pirated [copyright-infringing] goods" (Office of Intellectual Property Enforcement Coordinator, 2012, p. 2).[442] Signatories to this agreement are MasterCard, PayPal, Visa and American Express. These agreements explicitly state that they do not introduce new or amend existing laws. In fact, the payment providers' agreement stipulates that it lays out "voluntary and non-legally-binding" best practices that "shall not replace, modify or interpret existing law or legal framework."[443] Overall, the informal agreements streamline and better coordinate payment intermediaries' practices for sanctioning websites distributing counterfeit goods and copyright-infringing content by removing their critically important payment processing services.[444]

441 Interviews with two payment intermediaries in 2012.

442 The payment providers' non-binding agreements have not been released publicly but copies are on file with the author. These two documents that outline industry-described 'best practices' for payment providers and rights holders respectively.

443 From the payment providers' agreement titled "Best Practices to Address Copyright Infringement and the Sale of Counterfeit Products on the Internet" and dated 16 May 2011.

444 Interviews with trade associations, payment intermediaries and rights holders conducted in 2012.

11.3 Enforced Hybrid Regulation

Given this direct governmental pressure on payment providers, their work as regulators under the non-legally binding agreements is best understood as a form of enforced hybrid regulation, not voluntary regulation. Hybrid regulation refers to both the regulatory measures (hard law and soft law) and the actors (state and corporate) (see Trubek & Trubek, 2005). Hard law measures are legally binding obligations, while soft law lacks legal bindingness (Abbott & Snidal, 2000; see also Scott, 2011). The non-binding agreements guiding payment intermediaries' enforcement efforts are characterised by hard-soft law hybridity. Intermediaries' terms-of-service agreements with their users, which incorporate national laws, is the hard law that grants these entities the legal authority to act as regulators even in the absence of legal orders or legislation. Paired with intermediaries' contractual agreements are the non-legally binding agreements that are composed of best practices, a form of soft law, which are intended to guide intermediaries' enforcement actions. Although the agreements are not legally binding, IPEC's pressure on intermediaries to adopt them had coercive force. Coercive state pressure, in other words, produced informal industry best practices in which intermediaries are pressured to go beyond their legal responsibilities in what some advocates refer to as "beyond compliance" regulation (European Commission, 2013:5-6).

Payment intermediaries are not voluntary gatekeepers but actors that IPEC designated as responsible for policing their platforms for violations of intellectual property law. Here enforced hybrid regulation has similarities with "enforced self regulation" (Ayres & Braithwaite, 1992), coerced self-regulation (Black, 2001), and state-promoted private ordering (Bridy, 2011). In enforced hybrid regulation, corporate actors set and enforce rules, typically in some arrangement with government that govern their industry sectors and generally in response to government pressure, which often takes the form of a threat of statutory regulation. Corporate actors may acquiesce to state pressure "not in the shadow of existing law, but in the shadow of potential law" (Mann & Belzley, 2005: 260). These non-state regulators may be "reluctant governors"

(Haufler, 2010) that are compelled to accept greater enforcement responsibilities. This is the case for payment intermediaries.

11.4 Payment Intermediaries as Regulators

To understand payment providers' role as regulators, it is important to consider how they operate online. PayPal directly interacts with its users by enabling them to transfer funds from various sources, such as bank accounts, credit cards, or PayPal accounts to recipients. Visa and MasterCard, in contrast, are card associations, which means that they each operate through a network of thousands of formally affiliated and licensed financial institutions globally. They do not issue credit cards directly to users. Rather, card associations work within their network of affiliated banks that grant Visa- or MasterCard-branded credit cards to users. These affiliated institutions also grant merchant accounts that enable websites to accept payments by credit cards.

Payment intermediaries' legal authority for setting and enforcing rules comes from the contractual terms-of-service agreements they have with their users. Merely by visiting some websites users signal acceptance of the companies' policies. Following an update to its terms-of-service agreement PayPal states "your use of the services, including our website" means "you agree to the update" (PayPal, 2016). These agreements outline users' obligations and incorporate national laws. Visa states that any transactions "must be legal in both the Cardholder's jurisdiction and the Merchant Outlet's jurisdiction" (Visa, 2013:57).

Payment intermediaries can impose fines, block payments, or force merchants to reimburse customers in cases of fraud, a practice termed mandatory chargeback. PayPal tells its users that if it "believes that you may have engaged in any Restricted Activities," the company "may close, suspend, or limit your access to your Account" which includes restricting users' ability to send money or make withdrawals (PayPal, 2016). Payment intermediaries' most powerful regulatory tool is the removal of their payment services from targeted websites, which has the goal of starving targeted websites of revenue. While website operators may seek out another payment provider, it is difficult to replace the commercially popular

providers: Visa, MasterCard and PayPal. Recent academic research concurs with this idea: a study of unlawfully operating online pharmacies concludes "reliable merchant banking is a scarce and critical resource (McCoy et al., 2012:1).

The regulatory capacity embedded within their terms-of-service contracts is significant as intermediaries have the latitude to amend or interpret their provisions as suits their interests (see e.g., Braman & Roberts, 2003). Intermediaries typically include a clause that gives them the right to terminate service at any time for any reason. In its agreement, PayPal states that it "reserves the right to terminate this Agreement, access to its website, or access to the Services for any reason and at any time upon notice to you" (PayPal, 2016). Consequently, even if the content or transactions in question are lawful, intermediaries may remove their services from users. PayPal, for example, has terminated services to online file storage services, virtual private networks, and domain name service masking services that PayPal considers may facilitate copyright infringement (see Ernesto, 2016). These services, however, are legal even though some users may employ them for illegal activities.

In short, intermediaries' flexibility as regulators relies upon these contracts that are often unread by consumers (Obar & Oeldorf-Hirsch, 2016). As a result, intermediaries' regulatory efforts can be global, rapid and highly flexible.

11.5 Setting Global Standards

At the heart of many debates over power and regulation on the Internet are concerns over who sets and enforces certain rules, whose interests are served, and how this may affect global flows of information. Related to these concerns are questions of jurisdiction: whose rules applies and where? Control key intermediaries and one controls the provision and operation of important services and infrastructure, an observation long noted by scholars of Internet governance (e.g., Zittrain, 2003).

By working with intermediaries with global operations, states and, increasingly, multinational corporate actors can tap into an

extra-territorial and extra-legal regulatory capacity. Legal scholar Yochai Benkler, referring to the retaliation against WikiLeaks by intermediaries, argues that intermediaries enabled the U.S. government "to achieve extra-legally much more than law would have allowed the state to do by itself" (Benkler, 2011:342). Intermediaries can regulate activities and impose sanctions when other actors are constrained or unwilling to do so. In the absence of legal orders against WikiLeaks, the U.S. government was limited in the actions it could take directly but intermediaries have the latitude to remove services from any user. Governments explicitly recognize the value of intermediary-facilitated regulation. Victoria Espinel, former IPEC leader, praised intermediaries for their informal regulatory efforts against websites selling counterfeit goods as having an "impact on websites that are beyond the reach of U.S. law enforcement agencies" (Bason, 2012).

In addition to their efforts as global regulators, we should consider major intermediaries as de facto policymakers (see DeNardis, 2014). Intermediaries' work as regulators on a range of social problems, from child pornography and gambling to shutting down white supremacist websites is shaping rules and standards that affect Internet governance. As these companies remove content or withdraw their services, they are influencing policies in areas such as data retention, hate speech, privacy, and the protection of intellectual property rights. In the case of intellectual property rights, for example, intermediaries are increasingly adopting a hard-line approach, normalizing the disabling of entire websites instead of removing specific problematic content, such as sales listings for counterfeit goods.

Intermediaries set and enforce rules that tend to reflect certain norms, as well as benefiting their material interests. Those intermediaries acting as regulators and policymakers are generally large, U.S.-based companies that explicitly value freedom of speech (a U.S. constitutional right) as a fundamental operating principle. For these Internet companies, freedom of speech can be understood as the global flow of information, a foundational element of many online business models. U.S.-based intermediaries are generally reluctant to police speech, citing their commitment to protecting the right of freedom of expression. In the Charlottesville case, it

was intense public pressure, coupled with the explicit displays of racism and violence that pushed intermediaries to withdraw their services (see Tusikov, 2017).

The U.S. prioritization of freedom of expression over other rights, however, is not universal. In Europe, there is a strong norm of privacy. The European Right-to-be-Forgotten ruling, for example, asserts that individuals should have the right to remove search results in cases relating to personal information that is "inaccurate, inadequate, irrelevant or excessive."[445] This ruling, based on European Union data protection rules, contends that intermediaries, specifically Google as the largest search engine in Europe, have a role to play in safeguarding privacy, not simply ensuring the flow of information. Thus, there is a clash between norms for freedom of speech and those for privacy. In both cases, state actors want to work through intermediaries to export their preferred regulatory standards globally. Prominent European voices want the Right-to-be-Forgotten ruling to apply globally, not just within the European Union,[446] while the U.S. government works to export its preferred standards on intellectual property rights and its national security programs.

The United States is the foremost global champion of ever-stronger intellectual property rights. It pursues its interests in intellectual property standard setting through international trade agreements (see Sell, 2003), by pressuring countries to adopt its standards (see Drahos & Braithwaite, 2002), and through informal intermediary-facilitated regulation. This is because intellectual property is integral to economic dominance: economic benefits flow to those who control intellectual property rights (see Dedrick et al., 2009). By working with intermediaries, the U.S. government is able to export globally its hard-line approach to destroying websites distributing copyright-infringing and counterfeit goods.

Equally important, by working with and through major U.S.-based intermediaries the U.S. government further entrenches its national

445 Case C-131/12, Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González, ECLI:EU:C:2014:317, para. 92.

446 For example, a French court, the Paris Tribunal de Grande Instance, ordered Google in September 2014 to implement the Right-to-be-Forgotten ruling in its global network, not simply its European Union platforms. The European Union's body of privacy regulators, the Article 29 Working Party, has made the same demand (see Halper, 2014).

security surveillance programs within the Internet. The classified files Edward Snowden leaked revealed the U.S. National Security Agency's dependence on sometimes-reluctant Internet companies (see Greenwald, 2014). There are shared interests between the U.S. government and many Internet companies in maintaining permissive rules on the collection and use of personal data, as well as narrowed conceptions of online privacy. Such data-intensive practices are integral to the businesses of many intermediaries, especially those in the search, advertising, and social networking sectors. Thus, there are common state-corporate interests in the massive accumulation and mining of personal data to influence and predict human behaviour. These preferences – for maximalist accumulation of personal data, minimized privacy, and strong protection for intellectual property rights – primarily benefit western legal, economic, and security interests, especially those of the United States (see Powers & Jablonski, 2015).

11.6 Conclusion

We may welcome intermediaries' efforts to combat child pornography or the sale of dangerous goods. Payment intermediaries, in particular, may be effective regulators in that they can starve websites of funds, thereby crippling their commercial viability. However, there are significant problems in governments offloading regulatory responsibility to companies without any of the oversight or accountability that may accompany legislation or formal legal orders. As intermediaries' efforts occur outside the authority of the courts and public scrutiny, their actions display a troubling lack of accountability, and have the potential to chill free expression and undermine human rights (see Laidlaw, 2015). Intermediaries' informal enforcement efforts generally have weak due-process measures, as intermediaries remove content or withdraw services based on allegations, not proof, of wrongdoing (Tusikov, 2016). As well, intermediaries may lack precision in their enforcement efforts and mistakenly target websites with legal content and lawful services. This is because intermediaries are typically ill equipped to differentiate legality from illegality online, especially in complex cases of intellectual property rights, or to mediate effectively among

competing legal claims.[447] Intermediaries' enforcement processes are often opaque as their content moderators arbitrarily interpret their complex, fast-changing internal rules. These problems are further exacerbated when governments are hesitant to impose oversight requirements because of a fear that it would "add layers of difficulty that might drive [industry] participants away."[448]

By virtue of their market concentration, major payment providers can effectively cut off targeted websites from the global marketplace. But in doing so, they may stifle innovation and unfairly constrain lawful behaviour. Intermediaries may inadvertently – or, more troublingly, deliberately – set rules that benefit their interests and those of other corporate actors at the expense of the general public. Revenue chokepoints have the potential to affect lawfully operating sites that may share payment channels with targeted sites, or legally operating businesses whose services can be used to facilitate infringement, such as virtual private networks. Shifting greater regulatory responsibility to intermediaries can chill not only the "provision of valuable goods and services" but also "legal conduct that is adjacent to the targeted conduct" (Mann & Belzley 2005, p. 26). This regulatory chill can dissuade new businesses, technologies and ideas.

By working with intermediaries, states and, increasingly, rights holders of intellectual property, have access to a considerable regulatory capacity. When major intermediaries become regulators responsible for policing their platforms on behalf of governments or in response to high-profile protests, their already considerable power increases. U.S.-based companies already dominate many industry sectors, including search, advertising, domain registration, payment and social media. These intermediaries can reach globally, act swiftly and in the absence of formal legal orders, and have the latitude to designate even lawful behaviour as unwelcome on their services.

States facing controversial, difficult, or unpopular regulatory options can delegate authority to non-state actors and govern indirectly. In doing so, state officials can strategically distance governments

447 Interview with intermediaries and rights holders.

448 Interview with U.S. government official 2012.

from any public criticism and sidestep the often-onerous legislative process, while also legitimizing corporate regulatory efforts, whether formally or tacitly. For example, following the massive public protests that killed the U.S. *Stop Online Piracy Act*, public officials in the United States have become wary of regulating the Internet through legislation. When rules are quietly struck between industry and government, the regulatory process is profoundly undemocratic, especially when it affects the global operation of Internet services and tools that people rely upon.

11.7 Bibliography

Abbott K W & Snidal D (2000). 'Hard and Soft Law in International Governance'. (2000) 54 (3) International Organization 421.

Ayres I & Braithwaite J (1992). *Responsive Regulation: Transcending the Regulation Debate* (Cambridge University Press,1992).

Bason T H (2012, May 17). 'IP Czar: Voluntary Industry Agreements Could Be Key to Combatting IP Infringement' (*Bloomberg BNA*, 17 May 2012) <www.bna.com/ip-czar-voluntary-industry/> [accessed 17 November 2017].

Benkler Y (2011). 'WikiLeaks and the Protect-IP Act: A New Public-Private Threat to the Internet Commons' (2011) 140(4) Daedalus, 154.

Black J (2001). 'Decentring Regulation: Understanding the Role of Regulation and Self-Regulation in a 'Post-Regulatory' World' (2001) 54(1) Current Legal Problems 103.

Braman S & Roberts S (2003). 'Advantage ISP: Terms of Service as Media Law' (2003) 5 New Media Society 422.

Bridy A. (2011). 'ACTA and the Specter of Graduated Response' (2011) 26(3) American University International Law Review 559.

Bridy A (2015). 'Internet Payment Blockades' (2015) 67(5) Florida Law Review 1523.

Dedrick J, Kraemer K L, & Linden G (2009). 'Who profits from innovation in global value chains?: a study of the iPod and notebook PCs' (2009) 19 Industrial and Corporate Change, 81.

Drahos P, & Braithwaite J (2002), *Information Feudalism: Who Owns the Knowledge Economy?* (Oxford University Press, 2003).

Ernesto, 'PayPal Starts Banning VPN and SmartDNS Services' (*TorrentFreak*, 05 February 2016) <https://torrentfreak.com/paypal-starts-banning-vpn-and-smartdns-services-160205> [accessed 17 November 2017].

Espinel V (2011). 'Testimony of Victoria A. Espinel, Intellectual Property Enforcement Coordinator, Executive Office of the President, Office of Management and Budget, Before the Committee on the Judiciary' (2011).

Espinel V (2012). 'Testimony of Victoria A. Espinel, Intellectual Property Enforcement Coordinator, Executive Office of the President, Office of Management and Budget, Before the U.S. Senate Committee on the Judiciary' (2012).

European Commission (2013). 'Report from the Commission to the European Parliament and the Council on the Functioning of the Memorandum of Understanding on the Sale of Counterfeit Goods via the Internet' (2013) <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2013:0209:FIN:EN:PDF> [accessed 17 November 2017].

Greenwald G (2014). *No Place to Hide: Edward Snowden, the NSA and the U.S. Surveillance State* (Metropolitan Books, 2014).

Haufler V (2001). *A Public Role for the Private Sector: Industry Self-Regulation in a Global Economy* (Carnegie Endowment for Int'l Peace, 2001).

Haufler V (2010). 'Corporations in zones of conflict: issues, actors, and institutions'. In Avant D, Finnemore M, & Sell S K (Eds.), *Who Governs the Globe?* (Cambridge University Press, 2012).

Kraakman R H (1986). 'Gatekeepers: The Anatomy of a Third-Party Enforcement Strategy' (1986) 2 Journal of Law, Economics, & Organization 53.

Kirkpatrick L (2012). 'Rooting Out Rogue Merchants: The IACC Payment Processor Portal Mid-Year Review and Vision for the Future'. Presentation by the group head, franchise development and customer compliance, MasterCard, at the International Anti-Counterfeiting Coalition Spring Conference.

Laidlaw E (2015). *Regulating Speech in Cyberspace: Gatekeepers, Human Rights and Corporate Responsibility* (Cambridge University Press, 2015).

Levi M (2010). 'Combating the Financing of Terrorism: A History and Assessment of the Control of 'Threat Finance'' (2010) 50(4) British Journal of Criminology 650.

MacCarthy M (2010). 'What Payment Intermediaries Are Doing about Online Liability and Why It Matters' (2010) 25 Berkeley Technology Law Journal 1038.

Mann R J & Belzley S R (2005). 'The Promise of Internet Intermediary Liability' (2005) 47 William and Mary Law Review 239.

McCoy D, Dharmdasani H, Kreibich C, Voelker G M, & Stefan S (2012). 'Priceless: The Role of Payments in Abuse-Advertised Goods'. In 'Proceedings of the 2012 ACM Conference on Computer and Communications Security' <http://dl.acm.org/citation.cfm?id=2382285> [accessed 17 November 2017].

Mueller M L (2010). *Networks and States: The Global Politics of Internet Governance* (MIT Press, 2010).

Obar J A & Oeldorf-Hirsch A (2016). 'The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services' TPRC 44: The 44th Research Conference on Communication, Information and Internet Policy 2016 <https://ssrn.com/abstract=2757465> [accessed 17 November 2017].

Office of Intellectual Property Enforcement Coordinator. (2012). '2011 U.S. Intellectual Property Enforcement Coordinator Annual Report on Intellectual Property Enforcement' <www.whitehouse.gov/omb/intellectualproperty> [accessed 17 November 2017].

PayPal (2016). 'PayPal User Agreement' <https://www.paypal.com/ca/webapps/mpp/ua/useragreement-full> [accessed 17 November 2017].

Powers S M & Jablonski M (2015). *The Real Cyber War: The Political Economy of Internet Freed*om (University of Illinois Press, 2015).

Scott C (2011). 'Regulating Global Regimes'. In Levi-Faur D. (Ed.), *Handbook on the Politics of Regulation* (Edward Elgar Publishing, 2011).

Sell S K (2003). *Private Power, Public Law: The Globalization of Intellectual Property Rights* (Cambridge University Press, 2011).

Sell S K (2013). 'Revenge of the 'Nerds': Collective Action against Intellectual Property Maximalism in the Global Information Age' (2013) 15 (1) International Studies Review 67.

Swire P (2005). 'Elephants and Mice Revisited: Law and Choice of Law on the Internet' (2005) 153 University of Pennsylvania Law Review 1975.

Trubek D & Trubek L (2005). 'Hard and Soft Law in the Construction of Social Europe: The Roles of the Open Method of Co-ordination' (2005) 11 European Law Journal 343.

Visa, 'Visa International Operating Regulations' (*Visa*, 15 October 2013) <https://usa.visa.com/dam/VCOM/download/merchants/visa-international-operatingregulations-main.pdf> [accessed 17 November 2017].

Zittrain J (2003). 'Internet Points of Control' (2003) 44 (2)'Boston College Law Review 653.

12 ANNEX: Recommendations on Terms of Service & Human Rights

These Recommendations were developed via a multistakeholder participatory process, facilitated by the Dynamic Coalition on Platform Responsibility, between February and October 2015. The document was edited by Luca Belli, Primavera de Filippi and Nicolo Zingales, consolidating the comments of a wide range of stakeholders[449] who participated to two public consultations. These Recommendations have also been annexed to the study on Terms of Service and Human Rights conducted by the Center for Technology and Society at Fundação Getulio Vargas in partnership with the Council of Europe.[450]

12.1 Introduction

The following recommendations aim at fostering online platforms' responsibility to respect human rights, in accordance with the UN Guiding Principles on Business and Human Rights, by providing guidance for "responsible" terms of service. For the purpose of these recommendations, the term "responsible" should be understood as respectful of internationally agreed human rights standards. Besides identifying minimum standards for the respect of human rights by platform operators (standards that "**shall**" be met), these recommendations suggest best practices (which are "**recommended**", or "**should**" be followed) for the most "responsible" adherence to human rights principles in the drafting of terms of service.

12.1.1 Background

The digital environment is characterised by ubiquitous intermediation: most of the actions we take on the web are enabled, controlled or otherwise regulated through the operation of online platforms (see: definition n in Appendix 1). Online platforms are essential instruments for individuals to educate themselves, communicate information, store and share data (see definition d in Appendix). Increasingly, the

449 A non-exhaustive list of the stakeholders that participated to the DCPR process can be found at tinyurl.com/UNIGFplatforms.

450 For further information about the study see tinyurl.com/toshr.

operation of these platforms affects individuals' ability to develop their own personality and engage in a substantial amount of social interactions. The online world might thus challenge the system of human rights protection traditionally used in the offline world, which relies predominantly on a public infrastructure. While private actors are traditionally not considered as duty-bearers in international human rights law, they are indirectly subject to international law through the laws of the countries in which they operate. However, since national laws do not always adequately implement internationally-agreed human rights, there is a need to define minimum standards and develop voluntary best practices at the international level to ensure protection of human rights by transnational corporations.

Respect of human rights undoubtedly represents an important factor in assessing the conduct of corporations from the perspective of a variety of stakeholders, including governments, investors and increasingly, consumers. This is especially relevant in the context of online platforms designed to serve the needs of a global community, and forced to satisfy different, often conflicting legal requirements across the various jurisdictions where they operate. In light of the key role that online platforms are playing in shaping a global information society and the significant impact they have on the exercise of the rights of Internet users (see definition k in Appendix), an expectation exists that such entities behave "responsibly", thus refraining from the violation of internationally recognised human rights standards and offering effective remedies aimed at repairing the negative consequences that their activities may have on users' rights.[1]

The existence of a responsibility of private sector actors to respect human rights, which was affirmed in the UN Guiding Principles on Business and Human Rights[2] and unanimously endorsed by the UN Human Rights Council, is grounded upon the tripartite framework developed by the UN Special Rapporteur for Business and Human Rights, according to which States are the primary duty bearers in securing the protection of human rights, corporations have the responsibility to respect human rights, and both entities are joint duty holders in providing effective remedies against human rights violations.

As part of this responsibility, corporations should:

1. make a policy commitment to the respect of human rights
2. adopt a human rights due-diligence process to identify, prevent, mitigate and account for how they address their impacts on human rights; and
3. have in place processes to enable the remediation of any adverse human rights impacts they cause or to which they contribute[3].

These recommendations focus on one of the most concrete and tangible means for online platforms to bring that responsibility to bear: the contractual agreement which Internet users are required to adhere to in order to utilise their services (usually called "Terms of Service", see definition s in appendix 1). Specifically, the recommendations constitute an attempt to define "due diligence" standards for online platforms with regard to **three essential components: privacy, freedom of expression and due process**. In doing so, they aim to provide a benchmark for respect of human rights, both in the relation of a platform's own conduct as well as with regard to the scrutiny of governmental requests that they receive. As recently stressed by the Council of Europe's Commissioner for Human Rights[4], guidance on these matters is particularly important due to the current lack of clear standards.

12.2 Privacy & Data Protection (see definition q in Appendix)

The first section of these recommendations provides guidance over the rules that online platform operators (see definition o in Appendix) can adopt in order to guarantee that their users are not subject to unnecessary or unreasonable collection, use and disclosure of their personal data (see definition m in Appendix).

12.2.1 Data Collection

Platform operators **should** limit the collection of personal information (see definition m in Appendix) from Internet users to what is directly relevant and necessary to accomplish a specific, clearly defined and explicitly communicated purpose[5]. The platform's terms of service (ToS) **shall** also specify every type or

category of information collected, rather than requiring a general-purpose consent (see definition c in Appendix)[6]. If consent is withdrawn, the platform is no longer entitled to process such data for the related purpose. Although withdrawal is not retroactive, i.e. it cannot invalidate the data processing that took place in the period during which the data was collected and retained legitimately, it **shall** prevent any further processing of the individual's data by the controller and should imply deletion unless further use is permitted and regulated by a legitimate law (see definition l in Appendix)[7].

Platform operators **shall** also refrain from collecting data by automatically scanning content (see definition b in Appendix) privately shared by their users, in the absence of platform-users' consent. Admissible derogations to this principle include the need to fight against unsolicited communications (spam), maintain network security (e.g. preventing the diffusion of malware) or give force to court order or provisions defined by a legitimate law.

Platform operators **shall** always obtain user consent before tracking their behaviour (both within the platform and outside, e.g. through social plugins on third-party sites). Even after consent has been given, they **shall** always provide a way for users to opt-out at a later stage by the platform within other services. In order to facilitate user oversight on the application of these principles, platform operators **shall** allow their users to view, copy, modify and delete the personal information they have made available to the platform, both within its own services or by other services within the platform, and are encouraged to do so enabling download of a copy of their personal data (see definition m in Appendix) in interoperable format[8]. Platform operators **shall** also allow their users to view, modify and delete the personal information that platform operators have shared with third parties for marketing purposes.

12.2.2 Data Retention

Platform operators **should** clearly communicate in their terms of service whether and for how long they are storing any personal data. As a general rule, any retention beyond the period necessary to accomplish the purpose (not exceeding 180 days)[9] **should** be specifically foreseen by a "legitimate law"[10].

12.2.3 Data aggregation

As a best practice, aggregation of platform users' data **should** only be done subject to express consent (see definition g in Appendix). Aggregation of data across multiple services or devices requires extra diligence from the part of the data controller (see definition e of Annex 1), since it might result in data being processed beyond the original purpose for which it was collected and the generation of new data, whose nature, volume and significance may nor be known or knowable by the platform user (see definition p in Appendix). The purpose of the data aggregation and the nature of the new data resulting from the aggregation **should** be clearly stated, in order to allow the platform users to properly understand the scope of the given consent. Although this does not prevent the implementation of cross-device functionalities[11], it is necessary to ensure that platform users understand the reason, scope and outputs of the data aggregation.

12.3.4 Data Use

Platforms **shall** obtain consent in order to use personal data (including platform users' contacts and recipients) for the legitimate purpose and duration as specified within the Terms of Service. Additional use of platform user's personal data does not require the platform user' consent when such use is necessary: (a) for compliance with a legal obligation to which the platform operator is subject; or (b) in order to protect the vital interests or the physical integrity of the platform user or of a third person; (c) for the performance of a task carried out in the public interest or in the exercise of official authority as specified by a legitimate law. (d) for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject[12]. However, express consent **should** be required for making personal data available to the public. Platform users **should** have the possibility to redefine the extent to which their personal data are available to the public.

A broad and open-ended permission on the use of platform users' personal data for "future services"[13] can be in conflict with the right of users to informational self-determination[14]. For this

reason, it **is recommended** that platforms specify in their ToS that the processing of personal data is limited to the scope of existing services, or explicitly state that the data can be used for specified additional services. The enrolment of platform users into any new service shall require the acceptance of new ToS.

Platform operators shall also give users the possibility to demand the rectification of inaccurate data and to object to the use of their personal data on legitimate grounds, unless such use is mandated by a legitimate law[16]. Furthermore, platform users **shall** always be able to obtain information about any predictive or probabilistic techniques that have been used to profile them and the underlying rationale of such profiling[17].

Lastly, platform operators **shall** always permit their users to delete their account in a permanent fashion[18]. Likewise, if there is no other legal reason justifying the further storage of the data, the data processor shall proceed with the permanent deletion of all or portions of the relevant data associated with the platform user's account[19], in a time that is reasonable for its technical implementation. While anonymous data (see definition a in Appendix) can be kept and processed without consent, pseudonymous data (see definition r in Appendix) should not be subject to different treatment in that regard.

12.3.5 Data protection *vis-à-vis* third parties

Platform operators **shall** provide effective remedies against the violation of internationally recognised human rights. For this reason, they **should** establish clear mechanisms for platform users to gain access to all of their personal data held by a third party to whom their data have been transferred, as well as to be informed of the actual usage thereof[20]. Platform operators **should** also enable their users to report privacy-offending content and to submit takedown requests[21]. When such requests are submitted, a balance of the relevant rights and interests should be made and the outcome may depend on the nature and sensitivity of the privacy-offending content and on the interest of the public in having access to that particular information[22]. They **should** also implement a system to prevent the impersonation of platform

users by third parties, although exceptions can be made with regard to public figures where pertinent to contribute to the public debate in a democratic society[23].

A second set of concerns pertains to the possibility to preempt any interference with platform users' personal data, by preventing third parties' access to platform user's content and metadata. Firstly, platform operators **should** allow users to preserve their anonymity vis-à-vis third parties to the extent permitted by legitimate laws. Secondly, it is **recommended** that platforms enable end-to-end encryption of communications and other personal information, in the context of both storage and transmission[24]. In that respect, **best practice** is when the decryption key is retained by the platform user, except where the provider needs to hold the decryption key in order to provide the service and the platform user has provided informed consent.

As regards the handing over of platform users' data upon governmental request, platform operators **should** specify that they execute such request only in the presence of a valid form of legal process, and release a periodic transparency report providing, per each jurisdiction in which they operate, the amount and type of such requests, and the platforms' response (in aggregate numbers).[25]

12.4 Due Process

Due process (see definition f in Appendix) is a fundamental requirement for any legal system based on the rule of law. "Due" process refers to the non-derogability of certain procedures in situations which may adversely affect individuals within the legal system. These procedures are grounded upon essential principles such as the clarity and predictability of the substantive law, the right to an effective remedy against any human rights violations and the right to be heard before any potentially adverse decision is taken regarding oneself. In particular, while a law must be clear and accessible to the platform user, the latter principles translate into the need for an appeal system and the respect of the core minimum of the right to be heard, including: (1) a form of legal process which respects the guarantees of independence and impartiality; (2) the right to receive notice of the allegations and the basic evidence in

support, and comment upon them, to the extent that not doing so may prejudice the outcome of the dispute; and (3) the right to a reasoned decision.

Due process has significant implications with regards to potential amendment and termination of contractual agreements, as well as the adjudication of potential disputes.

12.4.1 Amendment and termination of contracts

Terms of Service **should** be written in plain language that is easy to understand. The platform operators should provide an accessible summary of the key provisions of the terms of service. The platform operators **should** give their users meaningful notice of any amendment of the ToS affecting the rights and obligation of the users. Meaningful notice **should** be provided in a way, format and timing that enable platform users to see, process and understand the changes without unreasonable effort. Contractual clauses that permit termination by platforms without clear and meaningful notice **shall** not be used.

In addition, platform operators **should** consider giving notice even of less significant changes, and enabling their users to access previous versions of the terms of service. Ideally, platforms operators **should** enable their users to continue using the platform without having to accept the new terms of service related to the additional functionalities. Additional functionalities should never be imposed to the user when it is possible to provide the original service without implementing the additional functionalities. The platform user should have the possibility to opt in in for new functionalities. Meaningful notice **should** also be given prior to termination of the contract or services. Besides, to reduce the imbalance between platform users and platforms owners when it comes to litigation, it is **recommendable** that the ToS be negotiated beforehand with consumer associations or other organisations representing Internet users. In order to prevent wrongful decisions, it is **also recommended** that platforms make termination of accounts of particular platform users possible only upon repeated violation of ToS or on the basis of a court order.

12.4.2 Adjudication

Disputes can arise both between platform users and between a particular platform user and the platform operator. In both cases, platform operators **should** provide alternative dispute resolutions systems to allow for quicker and potentially more granular solutions than litigation for the settling of disputes. However, in view of the fundamental importance of the right of access to court, alternative dispute resolution systems **should** not be presented as a replacement of regular court proceedings, but only as an additional remedy. In particular, platform operators **should** not impose waiver of class action rights or other hindrances to the right of an effective access to justice, such as mandatory jurisdiction outside the place of residence of Internet users. Any dispute settlement mechanism **should** be clearly explained and offer the possibility of appealing against the final decision.

12.5 Freedom of Expression

Freedom of expression (see definition h in Appendix) is a fundamental right consisting of the freedom to hold opinions without interference and Freedom of expression may be subject to certain restrictions that shall be explicitly defined by a legitimate law. In the online platform context, the effectiveness of this right can be seriously undermined by disproportionate monitoring of online speech and repeated government blocking and takedown. The following section provides guidance as to how platforms should handle such matters through their terms of service.

12.5.1 Degree of monitoring

Although there are no rules to determine, in general terms, what kind of speech should or should not be allowed in private online platforms, certain platforms **should** be seen more as “public spaces” to the extent that occupy an important role in the public sphere.[26] These actors have assumed functions in the production and distribution process of media services which, until recently, had been performed only (or mostly) by traditional media organisations[27]. As a matter of fact, online platforms increasingly play an essential role of speech enablers and pathfinders to information, becoming instrumental for media’s outreach as well as for Internet users’ access to them[28].

As a general rule, any restriction on the kind of content permitted on a particular platform should be clearly stated and communicated within the ToS. In addition, platforms **should** provide effective mechanisms aimed at signalling and requesting the removal of content that is forbidden under the applicable legitimate laws (e.g. illegal content such as child pornography as well as other kinds of undesirable content, such as hate speech, spam or malware). However, such mechanisms shall be necessary and proportionate to their purpose.[29] It is of utmost importance that the rules and procedures imposing such restrictions are not formulated in a way that might affect potentially legitimate content, as they would otherwise constitute a basis for censorship. To this end, content restriction requests pertaining to unlawful content shall specify the legal basis for the assertion that the content is unlawful; the Internet identifier and description of the allegedly unlawful content; and the procedure to be followed in order to challenge the removal of the content[30].

Similarly, although platforms can legitimately remove content that is not allowed by their terms of service, either on their own motion or upon complaint, such terms of service **should** be clear and transparent in their definition of the content that will be restricted within the platform. However, when platforms offer services which have become essential for the enjoyment of fundamental rights in a given country, they should not restrict content beyond the limits defined by the legitimate law. Lastly, **platforms may** legitimately prohibit the use of the name, trademark or likeness of others, when such use would constitute an infringement of the rights of third parties. However, platforms operator **should** always provide clear mechanisms to notify those platform users whose content has been removed or prohibited and provide them with an opportunity to challenge and override illegitimate restrictions.

12.5.2 Government blocking and takedowns

Transparent procedures should be adopted for the handling and reporting of governmental requests for blocking and takedown in a way that is consistent with internationally recognised laws and standards.[31] Firstly, platform operators **should** execute such requests only when these are grounded on legitimate law.

The content should be permanently removed only when such operation is justified by a judicial order, or the takedown request has not been appealed or countered in due course. Secondly, platforms operators **should** notify their users of such requests, ideally giving them an opportunity to reply and challenge their validity, unless specifically prohibited by a legitimate law. Finally, as already mentioned in the context of government requests for data, platform operators **should** adopt law enforcement guidelines and release periodic transparency reports.

12.6 Protection of Children and Young People

A special category of concerns arises in the case of children and young people, towards which platform operators **should** exercise a higher level of care. Platform operators **should** adopt particular arrangements, beyond warning for inappropriate content and age verification that can be imposed by legitimate law for certain types of content.

First, parental consent **should** be required for the processing of personal data of minors, in accordance with the applicable legislation. Secondly, although terms of service **should** generally be drafted in an intelligible fashion, those regulating platforms open to children and young people **should** consider including facilitated language or an educational video-clip and, ideally, a set of standardised badges[32] to make their basic rules comprehensible by all users regardless of their age and willingness to read the actual terms of use[33].

Secondly, **it is recommended** that platforms provide measures that can be taken by children and young people in order to protect themselves while using the platform[34], such as utilising a “safer navigation” mode. Thirdly, platform operators **shall** offer specific mechanisms to report inappropriate content, and **should** providing a mechanism to ensure removal or erasure of content created by children and young people[35].

As an element of media literacy, all platform users **should** be informed about their right to remove incorrect or excessive personal data[36].

12.7 Appendix: Definitions

a Anonymous data:

Anonymous data means personal data processed in such a way that it can no longer be used to identify a natural person by using all the available means likely to be used" by either the controller or a third party.

b Content:

Text, image, audio or video provided to particular platform user within the platform, even on a transient basis. This includes content produced and/or published by the platform operator, by another platform user or by a third party having a contractual relationship with the platform operator.

c Consent:

Consent means any freely given, specific, and informed indication of the data subject's wishes by which s/he signifies her/his agreement to personal data relating to her/himself being processed.[37] To that end, every user shall be able to exercise a real choice with no risk of deception, intimidation, coercion or significant negative consequences if he/she does not consent.

d Data:

Content and/or personal information. Data can belong to both categories simultaneously.

e Data controller:

Data controller is the institution or body that determines the purposes and means of the processing of personal data

f Due Process:

Due process is a concept referring to procedural rights which are essential for the respect of the rule of law, comprising: (1) a form of legal process which respects the guarantees of independence and impartiality; (2) the right to receive notice of the allegations and the basic evidence in support, and comment upon them, to the extent that not doing so may prejudice the outcome of the dispute; and (3) the right to a reasoned decision.

g Express Consent:

Express consent is a type of consent which (in contrast with "implicit" or "implied" consent) requires an affirmative step in addition to the acceptance of the general ToS, such as clicking or ticking a specific box or acceptance of the terms and conditions of a separate document.

h Freedom of Expression:

The right to freedom of expression, enshrined in article 19 of the International Covenant on Civil and Political Rights consist of the freedom to hold opinions without interference and include freedom to seek, receive and impart information and ideas, regardless of frontiers. Freedom of expression may be subject to certain restrictions that shall be explicitly defined by a legitimate law. The right to freedom of opinion and expression is as much a fundamental right on its own accord as it is an "enabler" of other rights, including economic, social and cultural rights.[38]

i Function of the Platform:

Function that the community has attributed to the platform on the basis of the legal, commercial and social expectations that it has generated. This should not be confused with a platform's functionalities, which constitute merely one (albeit important) element to identify the overall function(s).

j Hate Speech:

Although there is no universally accepted definition of "hate speech", the term shall be understood as covering all forms of expression which spread, incite, promote or justify racial hatred, xenophobia, anti-Semitism or other forms of hatred based on intolerance, including: intolerance expressed by aggressive nationalism and ethnocentrism, discrimination on any grounds such as race, ethnicity, colour, sex, language, religion, political or other opinion, national or social origin, property, disability, birth, sexual orientation or other status[39]. In this sense, "hate speech" covers comments which are necessarily directed against a person or a particular group of persons[40].

k Internet User

An individual who is using Internet access service, and in that capacity has the freedom to impart and receive information. The Internet user may be the subscriber, or any person to whom the subscriber has granted the right to use the Internet access service s/he receives.

l Legitimate Law:

Laws and regulations are procedurally legitimate when they are enacted on the basis of a democratic process. In order to be regarded also as substantively legitimate, they must respond to a pressing social need and, having regard to their impact, they can be considered as proportional to the aim pursued[41].

(a) It must be provided by law, which is clear and accessible to everyone (principles of predictability and transparency);
(b) It must pursue a legitimate purpose (principle of legitimacy) [42]; and
(c) It must be proven as necessary and the least restrictive means required to achieve the purported aim (principles of necessity and proportionality).

If it is manifest that the measure would not pass this three-pronged test, the platform operator should deny the request and, to the extent possible, challenge it before the relevant court.

m Personal Data & Personal Information:

Personal data is any information about an individual that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, etc.[43] This is not intended to cover identification which can be accomplished via very sophisticated methods[44]. This notion of personal data is sometimes also referred to as Personally Identifiable Information (PII), defined as "any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information."[45]

n Platform:

For the purpose of these recommendations, platforms are understood as any applications allowing users to seek, impart and receive information or ideas according to the rules defined into a contractual agreement.

o Platform Operator

Natural or legal person defining and having the possibility to amend the platform's terms of service.

p Platform User

Natural or legal person entering into a contractual relationship defined by the platform's terms of service.

q Privacy & Data Protection:

Privacy is an inalienable human right enshrined in Article 12 of the Universal Declaration of Human Rights, which establishes the right of everyone to be protected against arbitrary interference with their privacy, family, home or correspondence, and against attacks upon his honour and reputation. In the context of online platforms, this encompasses the ability for data subjects to determine the extent to which and the purpose for which their personal data is used by data controllers, including the conditions upon which such data can be processed by the holder of data (the platform) and/or made available to third parties (right to informational self-determination).

r Pseudonymous Data:

Pseudonymous data means personal data that cannot be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately and subject to technical and organisational measures to ensure non-attribution

s Terms of Service:

The concept of "terms of service" utilised here covers not only the contractual document available under the traditional heading of "terms of service" or "terms of use", but also any other platform's policy document (*e.g.* privacy policy, community guidelines, *etc.*) that is linked or referred to therein.

12.8 Footnotes

[1] See Council of Europe, Recommendation CM/Rec(2011)7 of the Committee of Ministers to member states on a new notion of media

[2] Report of the Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises, John Ruggie: Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework, UN Human Rights Council Document A/HRC/17/31, 21 March 2011 {"Guiding Principles"), p. 1

[3] Guiding Principles, Part II, B, para. 15

[4] Council of Europe, "The Rule of Law on the Internet and in the Wider Digital World", footnotes 181-187 and corresponding text.

[5] See Principle I.3 of the OECD Privacy Principles ("The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose."); Principle III of the APEC Privacy Framework which " limits collection of information by reference to the purposes for which it is collected. The collection of the information should be relevant to such purposes, and proportionality to the fulfilment of such purposes may be a factor in determining what is relevant"; and Principle 3 of the UN Data Protection Principles and Rights, according to which "The purpose which a file is to serve and its utilisation in terms of that purpose should be specified, legitimate and, when it is established, receive a certain amount of publicity or be brought to the attention of the person concerned, in order to make it possible subsequently to ensure that: (a) All the personal data collected and recorded remain relevant and adequate to the purposes so specified; (b) None of the said personal data is used or disclosed, except with the consent of the person concerned, for purposes incompatible with those specified? (c) The period for which the personal data are kept does not exceed that which would enable the achievement of the purpose so specified.

[6] See Principle III of the OECD Privacy Principles; and Principle 5 of the APEC Privacy Framework.

[7] See Principle UN Data Protection Principle and Rights ("Everyone [...] has the right to know whether information concerning him is being processed and to obtain it in an intelligible form, without undue delay or expense, and to have appropriate rectifications or erasures made in the case of unlawful, unnecessary or inaccurate entries and, when it is being communicated, to be informed of the addressees") and Art. 8e of the modernized version of Convention 108 ("Any person shall be entitled: [...] to obtain, upon request, as the case may be, rectification or erasure of such data"). See also Opinion 15/2011 of the Article 29 Working Party on the definition of consent, p. 9

[8] See article 15 of the proposed EU data protection regulation.

[9] Given the importance of data about past platform user behaviour for the provision of personalised search results, it appears unnecessary, as a matter of principle, to apply data retention periods exceeding those foreseen for search engines. Thus, the criterion of 180 days is based on the recognition by the Article 29 Working Party that search engines do not need, in principle, to store data for longer than 6 months- beyond which period, retention should be "comprehensively" justified on "strict necessity" grounds. See Art. 29 WP Opinion 1/2008 on data protection issues related to search engines, p. 19

[10] See Annex 1, definition p): "Legitimate Law"

[11] One example of such functionality is the recently added cross-device tracking feature of Google Analytics. See https://support.google.com/analytics/answer/3234673?hl=en

[12] See e.g. art 7, Directive 95/46/EC of the European Parliament and of the Council 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

[13] See e.g. Google's Terms of Services (http://www.google.com/intl/en/policies/terms) stating that "The rights you grant in this license are for the limited purpose of operating, promoting, and improving our Services, and to develop *new* ones" (as of 15 January 2015).

[14] For the development of this principle, see the decision by the German Constitutional Court in the so called "census" decision. BVerfGe 65, 1, available at http://www.datenschutz-berlin.de/gesetze/sonstige/volksz.htm

[15] See Convention 108, art. 8 a)

[16] See Principle VII d) of the OECD Privacy Principles, Principle II of the UN Data Protection Principles & Rights, and art. 8 d) of Convention 108.

[17] See Convention 108, art. 8 c)

[18] This is a corollary of the right to one's own identity, which forms integral part of the right to privacy

[19] See Opinion 15/2011 of the Article 29 Working Party on the definition of consent, p.33

[20] See article 8 b) of Convention 108

[21] See article 8 f) of Convention 108, and Part IV of the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data

[22] See Article 29 WP Opinion (WP225/14) on the implementation of the Court of Justice of the European Union Judgment on "Google Spain and Inc v. Agencia Española de Proteccion de Datos (AEPD) and Mario Costeja Gonzalez", C-131/12; available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf

[23] This is, once again, in respect of the individual's right to identity, see supra note 15. The exception for public interest purposes is intrinsic to the notion of right to informational self-determination. In part, it refers to the

notion of "public figures" which was specified in Resolution 1165 (1998) of the Parliamentary Assembly of the Council of Europe on the Right to Privacy; it is also specifically addressed through the relevant human rights jurisprudence (see e.g. Von Hannover v. Germany (no.2), 2012) and most recently, through the Art. 29 Working Party's Guidelines on the Implementation of the Court of Justice of the European Union Judgment on "Google Spain and Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González " C- 131/12

[24] *Ibidem*

[25] See Guiding Principles, Part II, section B, para. 21. The Google transparency report is a role model in this field. See http://www.google.com/transparencyreport/

[26] In Sweden, for example, journalistic products such as newspapers, even if privately owned, abide by specially designed laws that grant them a special legal status because of their potential for free speech.

[27] See Council of Europe, Recommendation CM/Rec(2011)7 of the Committee of Ministers to member states on a new notion of media, para. 6

[28] *Ibidem*

[29] On that regard, the Johannesburg Principles on National Security, Freedom of Expression and Access to Information provide further guidance on how and when restrictions to freedom of expression may be exercised.

[30] See Manila Principles on Intermediary Liability, 3.b; available at https://www.manilaprinciples.org/

[31] See the Global Network Initiative Principles on Freedom of Expression and Privacy; available at https://globalnetworkinitiative.org/principles/index.php

[32] See for instance, those provided by CommonTerms (see www.Commonterms.org) and Aza Raskin (see http://www.azarask.in/blog/post/privacy-icons/)

[33] Recommendation CM/Rec(2014)6 of the Committee of Ministers to member States on a guide to human rights for Internet users – Explanatory Memorandum, para. 90

[34] Council of Europe Recommendation CM/Rec(2014)6 of the Committee of Ministers to member States on a guide to human rights for Internet users – Explanatory Memorandum, para. 95

[35] See Declaration of the Committee of Ministers on protecting the dignity, security and privacy of children on the Internet. Decl-20.02.2008/2E

[36] See Council of Europe Recommendation CM/Rec(2012)3 of the Committee of Ministers to member States on the protection of human rights with regard to search engines, para. II.8

[37] See EU Directive 95/46/EC, Article 2(h)

[38] See Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, 16 May 2011, A/HRC/17/27

[39] See e.g. Protocol No. 12 to the Convention for the Protection of Human Rights and Fundamental Freedoms

[40] See Council of Europe, Committee of Ministers" Recommendation 97(20) on "hate speech"

[41] In the case of restriction to freedom of expression, the legitimate purpose shall be one of those set out in article 19, paragraph 3, of the Covenant, namely (i) to protect the rights or reputations of others, or (ii) to protect national security or of public order, or of public health or morals. While no specific legitimate objectives have been identified by the Special Rapporteur to evaluate restrictions to privacy, the test devised in the Report is roughly equivalent, requiring that measures encroaching upon privacy be taken on the basis of a specific decision by a State authority expressly empowered by law to do so, usually the judiciary, for the purpose of protecting the rights of others. See 2011 Report, para. 59
See Explanatory Report of the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("Convention 108"), para. 28

[42] See e.g. Council of Europe, Recommendation CM/Rec(2014)6 of the Committee of Ministers to member States on a guide to human rights for Internet users – Explanatory Memorandum

[43] See the Opinion 4/2007 of the Article 29 Working Party on the concept of personal data, according to which "a person is identifiable if, on the basis of any means likely reasonably to be used either by the data controller or by any other person, he or she can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity".

[44] See U.S. National Institute of Standards and Technology (NIST), NIST's Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), available at: http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf. See also the Opinion 4/2007 of the Article 29 Working Party on the concept of personal data, according to which "a person is identifiable if, on the basis of any means likely reasonably to be used either by the data controller or by any other person, he or she can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity".

[45] In the case of restriction to freedom of expression, the legitimate purpose shall be one of those set out in article 19, paragraph 3, of the Covenant, namely (i) to protect the rights or reputations of others, or (ii) to protect national security or of public order, or of public health or morals. While no specific legitimate objectives have been identified by the Special Rapporteur to evaluate restrictions to privacy, the test devised in the Report is roughly equivalent, requiring that measures encroaching upon privacy be taken on the basis of a specific decision by a State authority expressly empowered by law to do so, usually the judiciary, for the purpose of protecting the rights of others. See 2011 Report, para. 59.

This book was produced by FGV Direito Rio,
composed with the font family Gotham, in 2017.

The **Authors** of the analyses featured in this volume are (in alphabetical order): Luca Belli, David Erdos, Maryant Fernández Pérez, Pedro Augusto Francisco, Krzysztof Garstka, Judith Herzog, Krisztina Huszti-Orban, David Kaye, Emily B. Laidlaw, Orla Lynskey, Lofred Madzou, Joe McNamee, Julia Reda, Marc Tessier, Natasha Tusikov, Rolf H. Weber, Nicolo Zingales, Célia Zolynski.

This book is the **Official 2017 Outcome** of the **UN IGF Dynamic Coalition on Platform Responsibility (DCPR)**, which is a multistakeholder group fostering a cooperative analysis of online platforms' responsibility to respect human rights, while putting forward solutions to protect platform-users' rights. This book offers responses to the DCPR's call for **multistakeholder dialogue**, made ever more pressing by the diverse and raising challenges generated by the *platformisation* of our economy and, more generally, our society. The analyses featured in this book critically explore the human rights dimension of the digital platform debate, subsequently focusing on the governance of personal data and, lastly, suggesting new solutions for the new roles played by online platforms.

This volume includes the **Recommendations on Terms of Service and Human Rights**, which were elaborated through a multistakeholder participatory process, facilitated by the DCPR. In accordance with the UN Guiding Principles on Business and Human Rights, the Recommendations provide guidance for terms of service that may deemed as "responsible" due to their respect of internationally agreed human rights standards.

> "*This volume seeks to capture and offer thoughtful solutions for the conundrums faced by governments, corporate actors and all individuals who take advantage of – or are taken advantage of within – the vast forums of the digital age. [...] This is a volume for all stakeholders.*"
>
> **David Kaye,**
> United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression

> "*This volume takes a broader perspective on platform responsibility, critically examining both legal obligations and political pressure on platforms to employ voluntary measures with regard to the actions of their users [...], in order to promote competition, maintain the rule of law and safeguard the rights of users.*"
>
> **Julia Reda,**
> Member of the European Parliament

Agência Brasileira do ISBN
ISBN 978-85-9597-014-4
9 788595 970144