Introduction

Bilyana Petkova and Tuomas Ojanen

FUNDAMENTAL RIGHTS PROTECTION ONLINE: CURATION V. REGULATION?

Technology has transformative power—and it is generally a power for good. Thanks to our increased connectivity, knowledge transfer is cheaper and more accessible than ever before. With the outbreak of the coronavirus pandemic in 2020, online teaching and videoconferencing substituted for in-person meetings. Moreover, the virtual environment allowed for broader audiences to follow various events. While many believe that virtual interactions cannot fully replicate the physical world, not least since blue-collar jobs remain firmly rooted in the physical, the quick takeaway from the global health crisis (still ongoing at the moment of writing) is that this one issue did not make the world stop spinning: Physical contacts could in many cases be creatively and effectively replaced by use of the internet. The internet has also ostensibly created preconditions for unprecedented democratization of the public sphere—possibly a true “marketplace of ideas,” or at least an open forum for the exchange of information providing the means for individuals to seek, receive, and impart ideas, regardless of frontiers. By enhancing access to information and freedom of speech, the internet has also become a significant source of citizen empowerment and engagement, transforming the role of citizens, both in their private and their public lives.

In spite of all the excitement, however, will today’s technical infrastructure lead to an actual democratization of knowledge spurring a possible decrease in social inequalities? Isn’t the marketplace of ideas an imperfect market, just as any other? Can it give rise to the proliferation of disinformation and lead to new forms of censorship; can it inflict grave harm? Through the prism of fundamental rights, this book aims to engage with the broader questions framing the debate on online content curation while also looking at the legal nuts and bolts underpinning it. For the purposes of the book, the notion of fundamental rights primarily denotes rights enshrined in the European Convention on Human Rights and the Charter of Fundamental Rights of the European Union in Strasbourg, as seen in light of the case law of the two European Courts: the

European Court of Human Rights and the Court of Justice of the European Union in Luxembourg. Along with national constitutional law, these two European systems of rights protection shape fundamental rights online in Europe and have ripple effects beyond.¹ While most chapters focus on the regulation of internet intermediaries in Europe, a few of our authors also engage with human rights enshrined in the US Constitution or protected by international law instruments such as the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights. Speech curation impacts on a number of fundamental rights, but the most commonly affected ones are privacy and freedom of expression (or freedom of speech, as it is called in the American constitutional vocabulary). The European Court of Human Rights has consistently referred to the importance of freedom of expression as underpinning democracy, and in this way as essential for the protection of all of the rights and freedoms set out in the Convention: “Freedom of expression constitutes one of the essential foundations of a democratic society, one of the basic conditions for its progress and for each individual’s self-fulfilment.”² Based on the EU Charter, the Court of Justice of the European Union has in turn emphasized the centrality of privacy and data protection for ensuring the freedom of the mind, especially taking into account the technological context: “the fact that data are retained and subsequently used without the subscriber or registered user being informed is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance.”³ Further, one of the editors of this volume has further analyzed the importance of privacy and data protection for the EU’s nascent constitutional

¹ As per Article 52(3) of the EU Charter of Fundamental Rights, insofar as the rights in the Charter correspond to rights guaranteed by the European Convention on Human Rights, the meaning and scope of those rights, including limitations, are the same as those laid down in the Convention. Hence, the regulation of internet intermediaries by the EU and its Member States must comply to the level of fundamental rights protection guaranteed by the Convention but, as provided in the last sentence of Article 52(3) of the EU Charter, the EU is always allowed to provide more extensive “fundamental rights protection online.” See Charter of Fundamental Rights of the European Union OJ C 326, 26.10.2012.

² See, for example, *Lingens v Austria*, 1986; *Sener v Turkey*, 2000, *Thoma v Luxembourg*, 2001; *Maronek v Slovakia*, 2001; and *Dichand and others v Austria*, 2002, referred to in Toby Mendel, “A Guide to the Interpretation and Meaning of Article 10 of the European Convention on Human Rights,” available at: [<https://rm.coe.int/16806f5bb3>] (accessed 19 September 2020).

³ Joined cases C-293/12 e C-594/12, *Digital Rights Ireland Ltd*, ECLI:EU:C:2014:238, para 48; see also Case C-362/14 *Maximillian Schrems v Data Protection Commissioner*, ECLI:EU:C:2015:650; Case C-131/12 *Google Spain v. Agencia Española de Protección de Datos (AEPD)* and Mario Costeja González, ECLI:EU:C:2014:317.

identity.⁴ Other rights caught in the crossfire of intermediary regulation could be the right not to be discriminated against, the freedom to conduct business, and the right to property, notably intellectual property.

While data travels faster than ever before to our electronic devices and across various databases, the risks associated with the rapid flow of information have grown exponentially. On the individual level, think of incitement to hate speech, dissemination of information violating personal privacy, and the multiplication of other reputational damages in the digital age, or infringements on intellectual property rights. Once, changing one's physical address was enough to remedy harassment in the wake of unwanted publicity or defamation. And copyright enforcement was of a different nature before the dawn of YouTube. Today, the digital trail that we leave, and the sheer speed of information flows, render conventional remedies obsolete. On the level of the political system, think of fake news, Cambridge Analytica, and cybersecurity warfare, all of which endanger the very foundation of democracy. In short, to rein in new technologies' potential, we must think about whether and how to regulate them: through industry-wide codes of conduct, other soft or hard law mechanisms, co-regulation, or perhaps through Code⁵ itself. We should think hard so as not to overregulate, lest we stifle innovation; but we should think harder so as not to underregulate, lest we lose our personal freedoms.

This volume focuses specifically on topics related to fundamental rights protection online connected to content or other speech curation. Content curation is a neologism we transpose from the museum context into the sphere of online intermediaries. It is hopefully an apt one as it aims to capture curation by both public and private actors and therefore goes beyond the binary dynamic created by terms like "regulation" and "moderation," which in turn imply predominance of either public or private actors, respectively, over the process of curation. As Hans Ulrich Obrist incisively notes:

The current vogue for the idea of curating stems from a feature of modern life that is impossible to ignore: the proliferation and reproduction of ideas, raw data, processed information, images, disciplinary knowledge and material products that we are witnessing today. This is hard to overstate. But though the explosive effects of the Internet have now become very obvious, they are only the leading edge of a larger change that has been occurring for about a hundred years ... The exponential increase in the amount of data created by human societies is a basic fact of our time.⁶

⁴ Bilyana Petkova, "Privacy as Europe's First Amendment" (2019) 25 *European Law Journal*.

⁵ Lawrence Lessig, *Code: and Other Laws of Cyberspace* (Basic Books 2000).

⁶ Hans Ulrich Obrist, *Ways of Curating* (Penguin 2014) at p 23.

The ready availability of content and the sheer amount of information in existence makes the work of the speech curator all the more significant and difficult. How to sift through all the data in order to make sense of it? How to weasel out misinformation or simply illegal content? Should yet new categories of illegal content be created? The very etymology of the word *curare*—to take care of—is, again, as Obrest helpfully observes, a proxy for “cultivating, growing, pruning and trying to help people and their shared contexts to thrive.”⁷ In an online environment, the “curator” is the user; however, it can also be the intermediary (platform) that curates content through either artificial intelligence (AI) or a—more or less—trained personnel of content moderators; in some cases the curator is a judge or an administrative agency, and yet in others likely a combination of all of the above. Although implicit in our title is an emphasis on regulation—and therefore public control over intermediaries—we do not want to lose sight of the bigger picture, which is both empirically and normatively richer; a picture in which intermediaries indeed exercise significant private powers over content, perhaps by “cultivating, growing, pruning” and hopefully “trying to help people and their shared contexts to thrive.”⁸

Another caveat is the very choice of use of the term “intermediary.” Although throughout the book we use “platform” and “intermediary” interchangeably, in the title of the collection and overall, most of our authors give preference to the word “intermediary.” An intermediary, as Fowler notes, is, “even with concrete sense of go-between or middleman or mediator, a word that should be viewed with suspicion and resorted to only when it is clear that every more ordinary word comes short of the need.”⁹ In the traditional sense of the word, an intermediary might be an agent that mediates between parties that do not necessarily agree. It is therefore difficult to accept that online intermediaries are mere conduits of information even if there is a perceived need to think of them as such. Going back to the transposed neologism of museum curation, one could see, with Obrist, the same tension, or at least get the impression that museum and gallery curators have come to compete with artists for primacy in the production of meaning or aesthetic value in the same way as intermediaries are sometimes seen today to compete for revenues with news outlets and creators.¹⁰ Be that as it may, we acknowledge the inherent tension in the term while maintaining it, as it is also the choice of the European legislator in

⁷ *ibid* at p 25.

⁸ *ibid*.

⁹ HW Fowler, *A Dictionary of Modern English Usage: The Classic First Edition* (OUP 1926) at p 281.

¹⁰ *Supra* n 5 at 33.

the e-Commerce Directive.¹¹ Over the period in which this book goes to print, the e-Commerce Directive is likely to be subjected to amendments and reenacted.¹² For years, the Directive has served as a bedrock for the intermediary liability regime in the European Union, providing a safe harbor to intermediaries under conditions. It is, however, not with nostalgia that we write about it on its 20th anniversary, but rather with an eye to revealing the rationale behind the conception of the regime on intermediary liability exceptions in Europe, as well as in an attempt to trace back how the regime has functioned so far, allowing the emergence of parallel new legislative and judicial carve-outs in the Member States and on the EU level.

Online curation is moreover perhaps a more accurate description of the phenomena connected to online content since the familiar “to regulate or not to regulate” is hardly fitting the multiplicity of online intermediaries today. Different problems might require different solutions and a one-size-fits-all approach is hard to find when intermediaries range from those serving as a link between retailers and end users, such as Amazon; to those that pool friends’ preferences and interests, such as Facebook; or those that simply serve as home-sharing or ride-hailing platforms, such as Airbnb and Uber. Despite the convergence around targeted advertising, of relevant consideration is also the specific business model of each platform. Although the e-Commerce Directive applies to intermediaries across the board,¹³ since we are focused on online speech the intermediaries discussed in this book are primarily news outlets, search engines, and social media.

Given the complexity of the topic, it further makes sense to point out what remains beyond the scope of this collection. Speech curation is without any doubt global but, as already alluded to with the centrality we give to the intermediary regime of the e-Commerce Directive, the book is in effect primarily focused on the European Union and its Member States. This is without prejudice to the fact that we also devote space to the constitutional layer of freedom of speech and the regime on intermediary liability exemptions in the United States, as well to the treatment of intermediaries on the international

¹¹ 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 (“Directive on electronic commerce”) OJ L 178, 17.7.2000, p 1–16 [hereafter E-commerce Directive].

¹² Reform of the EU liability regime for online intermediaries: Background on the forthcoming Digital Services Act, available at: [[www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_IDA\(2020\)649404](http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_IDA(2020)649404)] accessed 30 April 2020.

¹³ However, whereas the Court of Justice of the European Union (CJEU) considered Airbnb to fall within the scope of the e-Commerce Directive (Case C-390/18, ECLI:EU:C:2019:1112), the Court has so far excluded Uber from its remit (C-434/15, EU:C:2017:9811; C-320/16, EU:C:2018:221).

plane. Alongside the case law of the European Court of Human Rights, which sets minimum standards of fundamental rights protection in Europe and which we thereby understand as a legal order interlocking the European one rather than as an international law system, we discuss legislative and judicial developments in Germany, France, and Italy. In a Union of 27 states, it is hard to be exhaustive: We focus on Germany and France because they were the first countries to enact legislative initiatives that address the problem of disinformation, and on Italy because of the contradictory decisions of lower courts that culminated in an important recent case of the Italian Supreme Court. Although of vital importance, we also do not address the intersection of intermediary liability and competition law, or that of data protection and intermediary liability. This is not to undermine their importance but rather to acknowledge the fact that these angles merit separate attention. Foundational work regarding data protection and intermediaries in connection to the “right to be forgotten” has already been laid down by Robert Post.¹⁴ Furthermore, with one notable exception, the perspective we offer is mostly that of European academics. For an exclusively American account of the problems we discuss, worth mentioning is the work of Jack Balkin,¹⁵ Danielle Citron,¹⁶ Jennifer Dascal,¹⁷ and Kate Klonick.¹⁸ We grant that future iterations would do well to include the points of view of scholars from the Middle East, Asia, and the Global South. We moreover acknowledge the limitations of the current volume, which is no more than a snapshot in an unfolding debate; the questions we discuss are therefore constantly in need of being reopened and updated,¹⁹ due to changes in the

¹⁴ Robert Post, “Data Privacy and Dignitary Privacy: Google Spain, the Right to be Forgotten, and the Construction of the Public Sphere” (2018) 67 *Duke Law Journal* 981.

¹⁵ Jack Balkin, “How to Regulate (and Not Regulate) Social Media,” keynote address given at the Association for Computing Machinery conference on Computer Science and Law (2019), available at: [https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3484114] (accessed 19 September 2020).

¹⁶ Danielle Citron, “Cyber Mobs, Disinformation, and Death Videos: The Internet as It Is (And As It Should Be)” *Michigan Law Review* (forthcoming 2020).

¹⁷ Jennifer Dascal, “Google Inc. v. Equustek Solutions Inc” (2019) 112 *American Journal of International Law* 4; “Speech across Borders” (2019) 105 *Virginia Law Review* 1605.

¹⁸ Kate Klonick, “The New Governors: The People, Rules, and Processes Governing Online Speech” (2018) 131 *Harvard Law Review* 1598. See also Thomas Kadri and Kate Klonick, “Facebook v. Sullivan: Public Figures and Newsworthiness in Online Speech” (2020) 93 *Southern California Law Review* 37.

¹⁹ For example, the future research agenda on intermediaries would need to include empirical insights on the newly established Facebook Oversight Board, social media’s reputation scoring for fake news and disinformation campaigns during the coronavirus pandemic. Regarding Facebook’s Oversight Board, see Kate Klonick, “Creating Global

public debate and the legal sphere. Finally, the collection does not discuss at length important recent cases not only on delisting in the context of the “right to be forgotten” but also on defamation and copyright—instead, in the last part of this introduction we offer a schematic segue to a judicial deconstruction of content curation connected to the contextual and jurisdictional puzzles revealed in these cases.

ONLINE CONTENT ACROSS CONTEXTS AND JURISDICTIONS

In the first part of the book, we theorize with regard to the questions framing the debate on intermediaries. The book opens with a chapter by Oreste Pollicino unpacking some of the reasons behind the transatlantic divide. He holds that even in cases that are similar or identical, different balances will be struck, and different solutions will be found—in some cases, very different—based on the judicial framing. Judicial framing in relation to new technologies will in turn vary based on the role of the State in authoritarian or democratic systems, on the constitutional specificities of Europe and the United States, and on the willingness of judges to adapt familiar concepts to the digital world as opposed to entrenched insistence on parallels to the analogue world. Importantly, Oreste moves on to point out that judicial framing relies on metaphors. He shows that one such metaphor—that of the “marketplace of ideas”—is wrongly transferred to the context of fake news. A metaphor implies knowledge transfer across domains (from the Greek *meta*-pherein, to “carry over”). When US Justice Holmes introduced the metaphor of a marketplace of ideas to the domain of free speech, the liberal state and competition in the market were at their best. Similarly, when the US Supreme Court borrowed the same metaphor to call the internet the “new marketplace of ideas,” the internet market, in its genesis period, was absolutely free and not in any way affected by dominant positions, or, even worse, by monopolies and oligopolies. Far from being a free market, today the digital market is characterized by economic concentrations and the strength of (a few) private powers. Against this background, for Oreste, if fake news is arguably the most significant and pervasive source failure in the marketplace of ideas, the intervention of public powers could not be excluded, because the target domain of the metaphor—namely, the digital market—has changed since the US Supreme Court defined the internet as a “new free marketplace of ideas.”

Governance for Online Speech: The Development of Facebook’s Oversight Board,” *Yale Law Journal* (forthcoming 2020).

The last chapter in Part I of the book discusses the so-called filter bubble phenomenon from a human rights perspective. Christoph Bezemek starts from the premise that the digital revolution has failed to keep its promise to provide an open forum for the exchange of information and the cherished ideal of a true marketplace of ideas. Many fear that established gatekeepers have been replaced by algorithms that operate based on the users' existing preferences, thereby safely giving them the comfort of what is known and expected instead of confronting them with alternative thought and positions. Christoph argues that, instead of bringing down the gatekeepers of speech-institutionalized media, the information society brought new gatekeepers which may act more effectively (and more secretly) than their predecessors. Even if technology enables alternative voices and sources of information, these may never reach us through the filter bubble. From a fundamental rights perspective this poses problems not only for freedom of expression but also for the individual's pursuit of self-fulfillment inherent to the right to privacy. Ultimately, however, although state intervention is possible, for Christoph primary responsibility for bursting the bubble rests with the individual.

In Part II we delve into a sample of national regulatory approaches, looking into the legislative history and the intellectual debate surrounding various European and US legislative initiatives. Thomas Wischmeyer starts this debate by stating that constitutional democracies traditionally entrust courts rather than administrative agencies with the regulation of speech. Proposals to involve bureaucrats in speech regulation are quickly dismissed as government censorship. However, with the massive proliferation of harmful speech on the internet, the judicial system is less and less capable to enforce legal standards online. Against this backdrop, a debate has emerged as to whether or not to authorize an administrative agency with the online enforcement of free speech principles as defined by constitutional law and interpreted by the courts. In 2017, the German legislator led this idea to fruition and enacted the "Network Enforcement Law," which gives the federal bureaucracy the power to evaluate and assess the internal speech policies of major online platforms. Thomas's chapter analyzes the Enforcement Act and asks whether the new law adequately distributes the responsibility for preventing harmful speech between three major stakeholders: intermediaries, the administration, and courts. While the German law has its weaknesses, Wischmeyer's conclusion is that its general approach is overall convincing.

Next, Kamel Ajii shows how, for French President Emmanuel Macron, "All speech is not worth the same." This statement synthesizes the spirit and substance of the bill Macron proposed (and later enacted) to fight fake news during elections. The interference in electoral campaigns both in the United States and in France and the risk of divisiveness within society urged the French government to legislate. But how can lawmakers protect the electoral

process while preserving freedom of expression and of the press? The French bill created duties of cooperation and loyalty on social media companies, and an emergency procedure that can result in a takedown injunction within 48 hours. Ajji's chapter reports the legislative debates regarding the regulation of fake news and introduces the notion of artificial information, which conceptualizes the key aspects of this threat to democracy. He then examines the proposal's provisions regarding platforms, before suggesting paths to reduce the spread and effects of artificial information while preserving pluralistic expression online.

The final chapter of Part II is by Mark MacCarthy, who argues that the US Congress should consider legislation to regulate the content moderation practices of platforms. Failure to act will leave platform users unprotected. But a law requiring content rules against the most salient kinds of harmful platform content, including hate speech, terrorist material, and disinformation campaigns, would not pass constitutional muster under the First Amendment. In contrast, a consumer protection approach to content moderation might be effective and pass First Amendment scrutiny. The Federal Trade Commission (FTC), on its own or with authorization from Congress, could treat the failure to establish and maintain a procedurally adequate content moderation program as an unfair practice. This would effectively require platforms to have a content moderation program in place that contains content rules, enforcement procedures, and due process protections including disclosure, mechanisms to ask for reinstatement, and an internal appeals process, but it would not mandate the substance of the platform's content rules. It would respond to strict First Amendment scrutiny as a narrowly crafted requirement that burdens speech no more than is necessary to achieve the compelling government purpose of preventing an unfair trade practice. In addition, or alternatively, the FTC might be authorized to use its deception authority to require platforms to say what they do and do what they say in connection with content moderation programs. The FTC would treat failure to disclose key elements of a content moderation program as a material omission, and the failure to act in accordance with its program as a deceptive or misleading practice. Its First Amendment defense would rest on the compelling government interest in preventing consumer deception. Finally, MacCarthy notes that an additional advantage of this consumer protection approach is that it does not require controversial modifications of the US Section 230 of the Communications Decency Act immunities for platforms, which have in turn been the bedrock of the US intermediary liability regime.

Part III is about the European regulatory landscape. Sophie Stalla-Bourdillon and Robert Thorburn attempt to unveil "the scandal of intermediary" by stressing the hybrid nature of internet intermediaries that can play both a passive and an active role. They argue from this assessment that the use of binary and

exclusive oppositions in EU law, such as “active/passive” and “general monitoring/monitoring in a specific case,” has created confusion inasmuch as the “both/and” dispensation has not been acknowledged. Further, this chapter aims to reconstruct a regulatory approach based on the premise that intermediation implies hybridity. It therefore argues that if internet intermediaries are hybrid, the legal response in order to confine the increasing powers of actors performing intermediary activities can only be hybrid and plural. In particular, the authors suggest that the legal response should move away from, or go beyond, the traditional civil liability question “When do internet intermediaries have sufficient evidence to be vicariously liable?” It should rather focus upon intermediaries’ own acts, with a view to confining their regulatory power, even if regulatory modalities are necessarily mixed. Finally, Stalla-Bourdillon and Thorburn critically comment upon the evolution of intermediary liability in the EU, making the case that the e-Commerce Directive should remain a cornerstone of the EU legal framework.

Building on Sophie Stalla-Bourdillon and Robert Thorburn’s chapter, Alberto Miglio observes that through the gateway of the preliminary ruling procedure, the Court of Justice of the European Union has become a major actor in shaping the legal regime of online intermediaries within the EU. This has not proven an easy task to accomplish, due to the sheer heterogeneity of businesses that may be labeled as “intermediaries,” but also to the fragmentation of the legislative framework: Whereas the 2000 e-Commerce Directive grants intermediaries exemptions from liability with a view to encouraging the online dissemination of information, other pieces of legislation require Member States to make injunctive relief available against intermediaries for the purpose of protecting intellectual property rights. In reviewing the Luxembourg Court’s case law on the matter, Alberto’s chapter addresses the uncertain boundaries of liability exemptions and critically discusses the Court’s reliance on a balancing test between competing rights.

In the final chapter devoted to European law, Teresa Quintel and Carsten Ullrich discuss the EU soft law measures related to intermediaries. For Teresa and Carsten, social media have increasingly come to the attention of policy makers, not least because they provide an important stage for “fake news” or “disinformation” and “hate speech.” The pressure to take more responsibility over content hosted by social media has grown, with the EU relying mostly on non-binding, self-regulatory agreements. These measures have raised concerns regarding freedom of expression, because they require large online platforms to adjudicate on the legality of content. An alternative solution, explored by the authors, would require platforms to apply a risk-based approach to the prevention and removal of illegal content. The norms and standards of such approach would be based on the concept of duty of care and be subject to reg-

ulatory oversight. It is suggested that the current EU self-regulatory proposals lack democratic legitimacy and need to be replaced by co-regulatory solutions.

Keeping in mind the intertwining elements between the European Convention on Human Rights and European law, in Part IV we move to the international law landscape. First, Marta Maroni explores recent developments related to the liability of internet intermediaries for user-generated content as developed by the European Court of Human Rights in the cases *Delfi v Estonia* (2015) and *MTE v Hungary* (2016). Marta offers an analysis of the legal arguments deployed by the Court, drawing attention in particular to the question of anonymity and how anonymity might challenge the role of law in granting remedies. These issues influenced the Court's ruling in *Delphi*, whereby the Court opted for designing a more regulated environment at the expense of affording a broader understanding to freedom of expression. Maroni thus argues that delegating to private powers judgment as to what should count as freedom of expression, as well as the protection of the right to private companies, risks reducing freedom of expression to a mere "technicality," further neglecting the normative complexity of the right and hampering the internet's position as a pluralistic environment.

We conclude with a chapter firmly anchored in international law, by Lea Heasman. The author starts from the premise that internet intermediaries operating across borders struggle to find the balance between their obligations under national law when such diverge from international law standards. Like multinational companies in other sectors, online intermediaries seem to have been granted impunity for human rights violations on an international scale partly due to the fact that the horizontal effect of human rights is not recognized under international law. Lea's chapter focuses on non-binding principles such as "corporate responsibility" and "due diligence" established under the auspices of the United Nations and the Organization for Economic Cooperation and Development (OECD). It argues that the OECD and the Council of Europe's recent non-binding regulatory initiatives that apply specifically to the protection of freedom of expression and privacy in the field of online platforms largely build on the UN Guiding Principles, and that requiring intermediaries to follow due diligence procedures (putting a human rights policy in place, conducting impact assessments, and offering grievance mechanisms) is the way forward.

DECONSTRUCTING JUDICIAL SPEECH CURATION

The chapters in this book clearly testify to the fact that for some time now, the law has been unsettled as to how to treat intermediaries. Whether in the American or in European doctrinal understanding, intermediaries have been

classified as mere conduits of information,²⁰ as quasi-state actors that accomplish a role similar to that of a traditional public square,²¹ as broadcasters like other electronic media (television or radio),²² or as speakers and publishers with own freedom of speech rights.²³ Of course, the crux of the matter is that intermediaries often want to have it both ways—to be treated as something akin to mere conduits of information, and therefore not incurring any liability, *while* enjoying full free speech constitutional rights akin to those of the free press. The contradiction is evident, among others,²⁴ in the dissent of Judge Sajó in the *Delphi*²⁵ case. Sajó argued that the news portal in that case should not incur liability, even though it was an “active” intermediary, as it was not the publisher of the offensive speech at stake. At the same time, he argued that the news portal was pursuing journalistic activities and was therefore covered by the right to freedom of expression under the European Convention on Human Rights.

Time will tell if the problem of forum shopping between regimes of intermediary liability safe harbors and fundamental rights can be avoided by embracing the dual character of intermediaries,²⁶ and thereby affording the same platform different legal treatment according to the circumstances of the case. Although unrelated to freedom of speech offshoots, it seems that at least in the case of alleged trademark and trade secrets infringements, this is what happened to Google in two court decisions in Europe and Canada respectively,

²⁰ Although perhaps somewhat old-fashioned in the wake of algorithmic news (and other information) ranking, the idea that intermediaries are only the “cables” or “pipes” through which information flows freely still finds expression in the law. Under EU law, this is expressed by the idea of a “passive” intermediary, discussed in this volume in the chapters by Marco Bassini and Sophie Stalla-Bourdillon and Robert Thorburn, as well as by Alberto Miglio.

²¹ Robert Post is adamant in defending the role of intermediaries for the development of (a global?) public sphere, *supra* n 13.

²² See Kate Klonick, “The New Governors: The People, Rules, and Processes Governing Online Speech” (2018) 131 *Harvard Law Review* 1598 (summarizing the relevant case law).

²³ *ibid.* Note that under EU law, the question translates into a debate about the horizontal effect of the EU Charter of Fundamental Rights.

²⁴ In a US courtroom, Facebook claimed that it is the publisher and that decisions regarding what to publish and what not to publish belong to the platform, since its publisher discretion should be protected as a free speech right. See “Is Facebook a Publisher? In Public It Says No, But in Court It Says Yes”, *The Guardian*, available at: [www.theguardian.com/technology/2018/jul/02/facebook-mark-zuckerberg-platform-publisher-lawsuit?CMP=share_btn_link] (accessed 19 September 2020).

²⁵ *Delfi v Estonia* ECHR 2015–II 319, dissenting opinion of Judge András Sajó. See also the chapter by Marta Maroni in this volume.

²⁶ See the chapter by Stalla-Bourdillon and Thorburn in this volume.

whereby the platform was first found not to infringe European trademark law by displaying trademarks as keyword search terms,²⁷ but in a later judgment was mandated in Canada to deindex from its search results websites posted by a company infringing upon trade secrets.²⁸

In any event, if an intermediary is found liable regardless of the legal ground, a court would likely proceed by offering the same remedy to the aggrieved party, that is, the delisting of the contested piece of information. Delisting seems to be a logical remedy regardless of the subject matter of the infringement, which could range from intellectual property rights to data protection to defamation to disinformation. The Court of Justice of the European Union first deployed delisting in *Google Spain*,²⁹ where the remedy meant removal from search results while preserving the information at the original source. The European Court of Human Rights has been equally reluctant to demand erasure in the context of balancing freedom of expression and privacy rights. Accordingly, the Court emphasized the importance of digital archives and refused a request to anonymize former convicts' names.³⁰ In obiter dicta, however, the ECtHR, referring to *Google Spain*, alluded to the possibility of delisting as a remedy for the aggrieved party. The Court recalled that a publisher of a web page is distinct from a search engine in that it could benefit from the journalistic derogation of the EU General Data Protection Regulation while the search engine could not. Ultimately, the Strasbourg Court suggested that individuals seek remedy from the search engine, not the web publisher, since the legitimate interests at stake as well as the consequences for the data subject's privacy may be different.³¹ Be that as it may, the first step in a court's analysis would be to decide whether delisting would also imply erasure. And as much as the two European courts have been consistently careful in preserving the availability of information in the sense of news items, that threshold might be necessarily different when the contested information is defamatory

²⁷ Joined cases C-236/08 to C-238/08, *Google France SARL and Google Inc. v Louis Vuitton Malletier SA, Google France SARL v Viaticum SA and Luteciel SARL and Google France SARL v Centre national de recherche en relations humaines (CNRRH) SARL and Others*, EU:C:2010:159, discussed in further detail in the chapters by Stalla-Bourdillon and Thorburn and Miglio in this volume.

²⁸ *Google Inc. v Equustek Inc.* [2017] Supreme Court of Canada; see also *Equustek Inc. v Jack*, Supreme Court of British Columbia [2018].

²⁹ *Supra* n 2, Case C-131/12 *Google Spain v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, ECLI:EU:C:2014:317.

³⁰ *L. and W.W. v Germany*—60798/10 and 65599/10, ECHR judgment of 28 June 2018.

³¹ *ibid* at para 97. The ECtHR used rather emphatic language: “the original publisher of the information, whose activity is generally at the *heart of what freedom of expression* is intended to protect”: emphasis ours.

in nature or hate speech, or related to intellectual property infringements or disinformation.

The last step in a court's analysis would likely consist of defining the geographical scope of the remedy, and it is on that point that passions ignite. The three options before a judge would be a domain-limited remedy, a location-limited remedy or a global injunction.³² In the first scenario, the court could seek to issue an injunction ordering the intermediary to remove offending material from, say, its French or German domain (for example, google.fr or google.de), but not from its other domains. The second option consists in a court issuing an injunction ordering the intermediary to filter out users based on location (for example, in Europe) and remove any offending material for those users only, regardless of which Google domain they visit (google.fr/de or google.com). The third option is to simply order global delisting, requiring Google to issue a global injunction removing offending material across all of its domains and for all of its users worldwide.

The question arises as to whether the geographical scope of the injunction should be determined by the subject matter of the infringement. In the aforementioned case, the Canadian court mentioned that global injunctions have been given for violations as varied as those related to sexual images of children, copyright, and hate speech.³³ The starting point for defending the granting of global injunctions must be the effectiveness of the remedying measure. For instance, not unlike in the Canadian example, in the recent case of a former Austrian politician from the Green Party who, in the context of the refugee crisis in Europe, was called on social media a "lousy traitor," a "corrupt oaf," and a "member of a fascist party,"³⁴ the alternative to a global injunction for the aggrieved politician would have been to seek injunctions jurisdiction by jurisdiction—surely not the most human rights-friendly way of enforcing rights. Next to intellectual property and hate speech, the question on the geographical scope of remedies arose again in the context of the "right to be forgotten," whereby the French data protection authority sought a global injunction for a violation of that right under EU law.³⁵ Instead, Google insisted on a location-limited remedy within EU borders. In both the Austrian and the French preliminary references, the Luxembourg Court did not impose a global

³² Andrew Keane Woods, "Litigating Data Sovereignty" (2018) 128 *Yale Law Journal* 328.

³³ *Supra* n 27; *Google Inc. v Equustek Inc.* [2017] Supreme Court of Canada, paras 848–49.

³⁴ Case C-18/18, *Glawischnig-Piesczek v Facebook Ireland Ltd.*, ECLI:EU:C:2019:458, paras 12–15.

³⁵ Case C-507/17 *Google LLC v Commission nationale de l'informatique et des libertés (CNIL)* ECLI:EU:C:2019:772.

injunction based on EU law but left the door open for the national courts of EU Member States to do so if they deemed it so appropriate under national law.³⁶ This “federalist” stance of the Court was likely dictated by the fact that in both cases, the EU judges needed to interpret directives rather than regulations (the e-Commerce Directive and the pre-General Data Protection Regulation regime,³⁷ respectively; the e-Commerce Directive moreover explicitly allows for injunctions to be imposed by EU Member State courts).

The most important, and perhaps most sensible,³⁸ argument against global injunctions intertwines a procedural and a substantive element. On the procedural side, there is the worry that a global injunction would not be enforced in some jurisdictions; on the substantive side, the problem is said to stem from the disputed universality of fundamental rights. In the sense of procedure or judicial methodology, one could observe an interesting twist in the use of the term judicial comity. Whereas judicial comity could be, and was for years, arguably understood as the willingness of judges to rely on or at least respect foreign law precedent in their judicial decision-making, recently judicial comity has been evoked by platforms in favor of judicial restraint and “non-interference.” The substantive prong of the argument, related to the procedural one, holds that not all countries interpret qualified rights such as privacy and freedom of speech in the same fashion.³⁹ Whereas in European states sensitivities about hate speech go back to the shared experiences of World War II, in the US freedom of speech is afforded a high threshold of content neutrality that is only tabled for judicial debate in the context of incitement to violence. Similarly, the “right to be forgotten,” originally rooted in the French “droit à l’oubli,” is not a concept that enjoys universal recognition—more to the point, in some cases when it does, it can easily be hijacked as an excuse by authoritarian

³⁶ *ibid* at para 72.

³⁷ Commission Regulation 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 (General Data Protection Regulation), and repealing Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

³⁸ “Most sensible” meaning that typically opposition comes in the form of simplistic, ill-masked libertarian and deregulatory refrain that pits any sort of injunction that any court issues against a platform as endangering the holy ideal of freedom of speech that can easily become a proxy for a platform’s own commercial interest. On the danger of using the metaphor of marketplace of ideas, see Oreste Pollicino’s chapter in this volume.

³⁹ Embedded in European jurisprudential thought, the justification of the Advocate General’s Opinion in the CNIL case that only absolute rights should merit extraterritorial application is yet further proof of cultural relativism: see Case C-507/17 *Google LLC v Commission nationale de l’informatique et des libertés (CNIL)* ECLI:EU:C:2019:15.

states in order to restrict dissident freedom of speech in ways thought impermissible by both European and American democracies.⁴⁰ Finally, the same difficulty would arise in the hypothetical case of imposing a global injunction for fake news, since democratic states that explicitly create a new category of proscribed speech outlawing disinformation are still in the minority (see France, for example).⁴¹ As for the EU, the tendency of converting soft into hard law measures, exemplified by the voluntary Code on Hate Speech with intermediaries followed by a legislative proposal on a Terrorist Content Regulation,⁴² opens the possibility for a potential future transformation of the current soft law arrangement on fake news—the Code on Misinformation with the platform—into a legally binding legislative act. Further fueling this line of argument, authoritarian regimes have started enacting cybersecurity and other legislation that, under the rubric of fake news, serves as a pretext to severely restrict freedom of speech.

Finally, apart from ideological and cultural objections as to what should count and what should not count as permissible speech across jurisdictions, critics also point to the technical difficulty of using AI-powered tools to remove speech from social media. Specifically, the critique goes, what could be taken by AI as offensive material could turn out to be merely satire; hence, for example, enforcing the Luxembourg Court's recent judgment concerning the Austrian politician that required Facebook to remove not only "identically worded" but also "equivalent" defamatory speech could lead to unintended global censorship. This seems hardly to be at issue for illegal copyright or other intellectual property rights infringements, however: the strongest substantive pushback for global injunctions in that category comes instead from resisting Google's (or any other platform's) role as a third party in a dispute between two other parties and thereby questioning the resulting akin-to-strict-liability implications for the platform. A final point follows here regarding resistance to the imposition on the intermediary of a legal regime resembling strict liability in tort: no matter how controversial strict liability might be in this as in any other field, reframing the issue as one of free speech could be misplaced. Rather, the friends and foes of strict liability would do well to argue on its merits the pros and cons of applying to intermediaries, in certain limited cases, such an approach.

⁴⁰ "Expungement" however is well established in US law—for criminal records, for financial records, and for juvenile records. The two approaches are not so far apart. We are grateful to Marc Rotenberg for that remark.

⁴¹ See the chapter by Kamel Ajjai in this volume tracing the process of enacting the French law on disinformation.

⁴² See the chapters by Teresa Quintel and Carsten Ulrich in this volume.

To summarize, it would seem that whereas the accountability of intermediaries is perceived as a problem in both the United States and the European Union, consistent with its political economy, the US is not planning to undertake a major reform of the intermediary liability safe harbors under Section 230 of the Communications Decency Act. Often rubberstamped by US judges, content curation is therefore outsourced to the platforms that usually act according to so-called community standards centered on an expansive reading of the US First Amendment's free speech provision. The consequence is that regardless of the legal context, such a reading tends to afford delisting as a remedy confined to a certain jurisdiction. Instead, courts in the EU and Canada are grappling with their public power mandates that imply affording due relief to the injured party, even if global delisting in carefully chosen cases might come at the expense of engaging in endless jurisdictional quagmires. Simultaneously, the authors in our volume show that influential EU states such as France, Germany, and Italy are on the one hand demanding the involvement of public oversight bodies in the process of content curation, while on the other they are contemplating new limitations to free speech in the wake of new challenges to the democratic state such as disinformation campaigns, terrorist threats, and the need to preserve intellectual creativity. The findings of this book point to the need—triggered by EU Member States, the judgments of the European courts in Luxembourg and Strasbourg, and international law developments—for the EU to proceed with an overhaul of the EU intermediary liability regime, demanding more responsibility from the platforms while trying not to impose undue burden upon them. As a result, what might seem as a head-on collision between private and public power in the speech curation endeavor may produce beneficial friction. Since only a handful of cases will reach the courts, for the foreseeable future the bulk of speech curation will remain in the hands of platforms. But the pressure coming from public law institutions may spur intermediaries to consider constant updates to their operational community standards, including—importantly—a requirement for transparency regarding the sources of political advertisements. Facebook's newly established Oversight Board might need to include public administrators. New business models, such as that of fact-checkers, steadily grow. As a European legal construct, hate speech denotes abusive, denigrating, or harassing speech against a group or an individual's gender; national, racial, or ethnic origin; or religious beliefs. No matter the final outcome of the proposed European legislative framework on banning the dissemination of terrorist speech online, given its potential to cause psychological, dignitary, material, and physical harm, hate speech will remain illegal in most European countries, where Facebook, Google, YouTube, and other intermediaries have millions of subscribers. Perhaps we are not far from seeing the infusion of major platforms' community standards with European and other democratic states'

sensitivities on hate speech and content creators' intellectual property rights. At least insofar as intermediaries' aspirations are to be global speech curators, that might be the legitimate expectation of their users.