IJLT | THE INDIAN JOURNAL OF LAW AND TECHNOLOGY

Volume 17 | Issue 1 | 2021

[Cite as: 17 IJLT, < page no. > (2021)]

NATIONAL LAW SCHOOL OF INDIA UNIVERSITY
BANGALORE

Price: Rs. (in 2 issues)

The mode of citation for this issue of The Indian Journal of Law and Technology, 2020 is as follows:

16 IJLT, <page no.> (2020)

Published by:

Student Bar Association
National Law School of India University
Nagarbhavi, Bangalore – 560072
Website: www.ijlt.in
Email: ijltedit@gmail.com

Distributed exclusively by:

Eastern Book Company
34, Lalbagh, Lucknow - 226 001
U.P., India
Website: www.ebcwebstore.com Email: sales@ebc.co.in

IJLT
WWW.IJLT.IN

THE INDIAN JOURNAL OF LAW AND TECHNOLOGY

Volume 17 | Issue 1 | 2021

IJLT | THE INDIAN JOURNAL OF LAW AND TECHNOLOGY

Volume 17 | Issue 1 | 2021

Contents

ARTICLES

Building Digital Walls and Making Speech and Internet Freedom (or Chinese Technology) Pay for It

An Assessment of the US Government's Attempts to Ban TikTok, WeChat, and Other Chinese Technology

Apratim Vidyarthi & Rachel Hulvey***

Abstract *The Trump Administration's bans on Tik Tok and WeChat were the culmination in a line of escalating moves between the US and China that resulted in the US raising digital walls at home, in contrast to long-standing American foreign policy favouring Internet Freedom. This article examines the rationale cited by the US government for these digital walls, including threats of Chinese government access to American consumer data, the possibility of Chinese censorship on apps used by Americans, Chinese access to American government employees' data and military networks, and the ability of the Chinese government to interfere with American elections and spread disinformation. Our analysis suggests that of these threats, only the threat of access to government employees' data and military networks is sufficiently narrow and acutely rooted in reality so much so that the threat could possibly legally justify banning a foreign technology. However, even that analysis is close and rife with uncertainties.*

More broadly, the tools at the US government's disposal—IEEPA, Congressional lawmaking authority, and CFIUS review—encourage the use of such flimsy rationale and a lack of transparency, which ultimately promotes such broad bans; and the costs of these bans are dear. There may be First Amendment implications, and at the very least, a chilling of speech. There are also significant impacts on American foreign policy, from legitimizing the Chinese strategy of cybersovereignty and government regulation, to the creation of incentives to

* Apratim Vidyarthi: J.D. Candidate, 2022, University of Pennsylvania Law School.
** Rachel Hulvey: Ph.D. Candidate, Political Science, University of Pennsylvania.

Special thanks to Sarah Pierce, who provided guidance, review, and direction in our analysis and made this piece possible. Our gratitude also goes to the editors of the Indian Journal of Law and Technology for their hard work, edits, and advice.

localize data in a manner that might undermine American law enforcement efforts.

Introduction

The Internet is not a series of tubes.[1] Instead, it is a source of information and international communications, a new frontier of warfare, and the eternal source of memes[2]—all untethered to any geographical or earthly border. This analogy of a borderless internet is closely linked with the concept of free speech. In 2010, then-Secretary of State Hillary Clinton outlined the US commitment to internet freedom, including fundamental rights to access information under Article 19 of the Universal Declaration of Human Rights.[3] Expressing optimism towards the potential of technology, Clinton described the internet as a tool that enables democratic expression, echoing US Supreme Court rulings that describe the internet as the "modern public square."[4]

Despite early optimism that the internet is a space that amplifies rights to free expression, Clinton argued that governments present new threats to fundamental rights enshrined in international law, through measures that manipulate the flow of information across borders. Speaking in the language of the Cold War, Clinton described "virtual walls" that are "cropping up in

---

1 'The Daily Show with Jon Stewart: From Here to Neutrality' (*Comedy Central*, 26 October 2009) <https://www.cc.com/video/blvwyz/the-daily-show-with-jon-stewart-from-here-to-neutrality> accessed 24 April 2021.

2 See eg 'Rickroll' (*Know Your Meme*, 2008) <https://knowyourmeme.com/memes/rickroll> accessed 24 April 2021.

3 Daniel Joyce, 'Internet Freedom and Human Rights' (2015) 26 Eur J Intl L 493.

4 *Packingham v North Carolina* 2017 SCC OnLine US SC 72 : 198 L Ed 2d 273 : 137 S Ct 1730, 1737 : 582 US (2017).

the place of visible walls."[5] Government policies that either prevented access to particular websites or otherwise limited the flow of information constituted "a new information curtain . . . descending across much of the world."[6]

Although the US has long worked to prevent the rise of such digital walls abroad, on August 6, 2020, President Trump signed Executive Orders 13942[7] and 13943,[8] banning the popular video social media app TikTok and the Chinese messaging app WeChat respectively, citing national security risks. These bans were the next step in escalating tensions between the US and China. But the bans were also precarious—becoming tied up in courts, where the companies were ultimately granted temporary injunctions while litigation on the merits took place.[9] As of the time of writing, the Trump Administration—like a short TikTok video—has come to an end, and the bans have been revoked.[10]

However, the strategy of such bans is not short-lived, and instead poses serious risks to speech and the structure of the internet. Digital technology is now the primary avenue of expression, and government interference into which digital avenues are available for self-expression raises censorship and freedom of expression concerns regarding the government's interference with speech. While our mental perception of censorship is that a government writes what people within its borders see—whether in Orwell's 1984, The Interview's caricature of Kim Jong Un's cultural censorship, or the "lightly redacted" page 20 of the Mueller Report[11]—the concept of government regulation of speech is no longer so straightforward. Instead, it can be something as subtle as banning apps that are the primary means of communication for millions, under the pretext of security risks, while actually intended as a foreign power tool against foreign adversaries.

These threats to ban technology also hold long-term foreign policy implications. The US Internet Freedom foreign policy was initially designed to

---

5 Hillary Rodham Clinton, US Secretary of State, 'Remarks on Internet Freedom, Address Before the Newseum' (*US State Department*, 21 January 2010) <https://2009-2017.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm> accessed 18 April 2021.

6 ibid.

7 Exec Order No 13942, 85 Fed Reg 48637 (Aug 6 2020).

8 Exec Order No 13943, 85 Fed Reg 48637 (Aug 6 2020).

9 *Tiktok Inc v Trump* 490 F Supp 3d 73, 2020 US Dist. LEXIS 177250 at *26 (DDC 2020) [hereinafter *TikTok v Trump*] (providing an injunction for TikTok); *US WeChat Users All v Trump* 488 F Supp 3d 912 : 2020 US Dist. LEXIS 172816 at *34 (ND Cal 2020) (providing an injunction for WeChat) [hereinafter *WeChat v Trump*].

10 Exec Order No 14034, 86 Fed Reg 31423 (June 9 2021).

11 Special Counsel Robert S Mueller, III, *Report on the Investigation into Russian Interference in the 2016 Presidential Election* (2019) 20 <https://www.justice.gov/storage/report.pdf.> accessed 18 April 2021.

counter the spread of "digital barriers" that block access to information. Solutions blocking foreign technology from use within the US undermine the notion of the Internet as the borderless medium that the US has sought to preserve. Given the importance of democratic values at the heart of US Internet Freedom foreign policy, these bans diminish the ability of the US to pressure other governments to preserve the free flow of data and could have also more detrimental long-term global impacts.

In this article, we outline and evaluate the motivations of the US's recent moves to erect digital walls, in the context of the broader US policy on Internet Freedom. Since the early days of US missionaries, many US efforts abroad attempted to spread liberal values.[12] The internet was seen as a technological means of spreading the ideas of free speech and democratic values globally, through expanded opportunities for uncensored communication. This overarching goal is in tension with the attempted technology bans, which the Trump Administration justified in court as necessary to protect national security and mitigate Chinese government censorship. And for a country that has worked to prevent the rise of digital walls and counter China's "cyber sovereignty" foreign policy, taking actions that block an avenue for free expression borrow from China's playbook and normalises the Chinese approach to governing the internet over the very "borderless" internet the US has invested in protecting.

Section I provides context on the US's Internet Freedom policy, laying the groundwork for why these technology bans are so antithetical to America's long standing commitment to an open internet.

Section II then assesses the variety of risks that the US government has cited in court cases as justifying the TikTok and WeChat bans. The US's alleged risks fall into four categories: Chinese government access to American consumer data, Chinese government censorship on the platforms, risks to government employees' data and government infrastructure, and the platforms' roles in propagating disinformation campaigns and election interference. Overall, the US government failed to clearly outline sufficient harms arising from each of these threats that would justify banning communications tools. Only the threat of access to government employees' data and military networks is sufficiently narrow.

Section III more broadly examines the tools the US can use to block foreign technology, and how the structure of these tools encourages opacity

---

[12] Walter Russell Mead, *Special Providence: American Foreign Policy and How it Changed the World* (Routledge 2013).

and allows for dangerous policies like technology bans to be passed into law. The President's power through the International Emergency Economic Powers Act (IEEPA) is the easiest avenue for pursuing action against foreign firms through executive orders. Congressional statutes can also be used to implement bans on foreign technology, but are foreclosed from punishing individual companies. The executive and Congress also have the joint power to investigate foreign investment in technology companies using the Committee on Foreign Investment in the US (CFIUS) reviews, which provide more discretionary power to the government. Together, these tools provide broad discretionary, opaque, and flexible powers to the government to ban technology. This raises concerns over the ease with which the executive can advance bans of communication tools as a solution.

Section IV examines the cost of such bans. First, there are significant First Amendment and free speech concerns, and a violation of these laws and norms could be akin to soft censorship. Second, such bans have a significant impact on international relations and policy, including calling into question Internet Freedom and hurting the foundations of the internet—effectively an exemplification of Krasner's organized hypocrisy.[13] Finally, such bans also have the potential to drastically impact policies around data localization and create incentives for foreign governments to retaliate and create their own digital walls. Norms for cyber security are currently being negotiated at the United Nations, where the US and China have proposed dramatically different approaches.[14] By borrowing from China's playbook and raising digital walls when threats to US sovereignty are at stake, the US is legitimizing China's norms—the same norms that it has invested resources in countering.

We conclude that the costs of banning communications tools based on intangible, broad risks are not outweighed by the alleged benefits to national security and privacy that arise from these bans. Such bans also raise serious free speech concerns and are not worth the short-term gains the US hopes to achieve. They also legitimize other democratic governments'—such as India's—banning of foreign technology, creating a permission structure for closing avenues of speech and undermining the very unsiloed, open nature

---

[13] See generally Stephen D Krasner, *Sovereignty: Organized Hypocrisy* (1999).

[14] Duncan B Hollis, 'China and the US Strategic Construction of Cybernorms: The Process is the Product' (*Lawfare*, 11 July 2017) <https://www.lawfareblog.com/china-and-us-strategic-construction-cybernorms-process-product-0> accessed 26 April 2021; Christian Ruhl, Duncan Hollis, Wyatt Hoffman & Tim Maurer, *Cyberspace and Geopolitics: Assessing Global Cybersecurity Norm Processes at a Crossroads* (Carnegie Endowment for International Peace 2020) <https://carnegieendowment.org/2020/02/26/cyberspace-and-geopolitics-assessing-global-cybersecurity-norm-processes-at-crossroads-pub-81110> accessed 26 April 2021.

of the internet. The US government has many far-reaching and broad instruments to counter threats beyond banning the technology, and these tools do not create incentives for transparency. It should use these tools in a manner that focuses on a clear process to evaluate whether the risks mitigated by such technology bans are worth the heavy global costs of diminishing Internet Freedom and potentially inspiring other governments to raise digital walls and affect free speech.

I. The US's Internet Freedom Policy and Technology Bans

Over the last three decades, the US has championed the internet as a medium for extending liberalism further than previously imaginable. US Supreme Court rulings describe the internet as facilitating free expression, noting that "anyone with an internet connection" can become "a town crier with a voice that resonates farther than it could from any soapbox."[15] American foreign policy for the internet attempted to extend the same values that promoted domestic speech abroad, championing a "borderless" medium where new modes of communication are possible across countries. The central idea behind this policy was that governments should take a limited role in the regulation of the internet and instead allow technical experts to make decisions to prevent government interference in the operation of a global communications platform.[16]

At the heart of the US Internet Freedom policy is an effort to prevent the rise of strategies that limit the movement of information to within national boundaries. These "digital walls" can take many forms, but the main form involves governments disrupting the openness of the internet through censorship or impounding data within borders and preventing the free movement of information.[17] US officials designed the Internet Freedom foreign policy to preserve a borderless internet, which would, by definition, resist such nationalistic efforts to blockaccess to information, because of its boundlessness. An internet architecture that operated without regard for national borders

---

[15] *Reno v ACLU* 1997 SCC OnLine US SC 82 : 138 L Ed 2d 874 : 521 US 844, 870 (1997).

[16] See, eg, 'Short History of the Internet' (*Internet Society*, February 1993) <https://www.internetsociety.org/internet/history-internet/short-history-of-the-internet> accessed 14 August 2021. The way the internet is governed, through non-profit bodies and groups like ICANN, IETF, IANA (which are all *prima facie* neutral and non-governmental organizations), is the prime example that the US government intended to let the internet govern itself. See, eg , Stuart Minor Benjamin & James B Speta, *Telecommunications Law and Policy* (2015) 537-44.

[17] Jack Goldsmith & Tim Wu, *Who Controls the Internet?: Illusions of a Borderless World* (2006) 23.

extended the possibilities for global communication and speech, ensuring that every individual could access information without regard to where they are located.[18] And strategies like China's Great Firewall are exactly the restrictions the US designed its internet foreign policy to avoid.

The first wave of US foreign policy surrounding the internet questioned the ability of governments to implement digital walls, with President Bill Clinton infamously arguing that trying to regulate the internet would be like "trying to nail Jello to the wall."[19] Years later, Secretary of State Hillary Clinton argued that policies that prevent access to information are as repressive as the Berlin Wall: these efforts only serve to divide societies and limit liberalism.[20] The US invested in efforts to aid activists who were attempting to rise up against repressive states, including circumvention tools that could be used to evade censorship.[21] Of course, in addition to normative impulses to extend liberalism, American companies also benefitted immensely from the light regulation of the private sector, allowing technology giants like Facebook and Google to grow and prosper globally.[22] But even the lack of regulation of these companies is in part justified by the government's desire to not govern speech and content on the internet, both at home and abroad.[23]

After the initial laissez-faire, non-governmental approach to letting the internet develop, emerging policies by foreign governments have called into question the vitality of the US's vision of a borderless internet.[24] Governments have responded to digital threats as they have physical threats: by leveraging the tools of territorial sovereignty and the long-standing power of the state to regulate activity within its borders.[25] Although literature has surveyed China's power to bring the internet under national control, even liberal democracies are, by necessity, shifting, acknowledging the need to implement digital border control strategies to address national security concerns. New emerging threats like election interference and online propaganda now motivate democracies to raise digital walls; for example, in the case of misinformation, governments seek to preserve the smooth transition of power and

---

[18] Joyce (n 3) 493.

[19] 'User Clip: Clinton on Firewall and Jello' (*C-SPAN*, 8 March 2000) <https://www.c-span.org/video/?c4893404/user-clip-clinton-firewall-jello> accessed 24 April 2021.

[20] Clinton (n 5).

[21] See, eg, James Ball, 'Online Tools to Skirt Internet Censorship Overwhelmed by Demand' *The Washington Post* (21 October 2012).

[22] Anupam Chander, 'How Law Made Silicon Valley' (2013) 63 Emory L J 639.

[23] See, eg, Emily Bazelon, 'Free Speech Will Save Our Democracy' *The New York Times* (13 October 2020) <https://www.nytimes.com/2020/10/13/magazine/free-speech.html>.

[24] 'The Internet's New Borders' (*The Economist*, 9 August 2001*)* <https://www.economist.com/leaders/2001/08/09/the-internets-new-borders> accessed 9 August 2021.

[25] Goldsmith & Wu (n 17).

trust in elections, or in the case of cybercrime, to prevent attacks on national industries.

On this new frontier, although some governments are slowly shifting slightly towards China's vision of territorial control, the US has held fast to ideas privileging free information flow. For example, the US government decries data localization laws—strategies that impound data within national borders—as harmful to the concept of internet freedom. The government also uses international trade agreements to preserve a zone of free data flows between signatories.[26] Although more democracies are implementing content moderation to address threats of terrorism, the US broadly[27] adheres to the principle that information flows should remain unadulterated by governments. Another example is the US government's eschewing of intermediary liability laws that require platforms to remove illegal content or face sanctions in all instances except in the case of sex trafficking.[28]

In contrast to this history of American policies upholding the free flow of data and speech, a ban on Chinese communication tools flies in the face of Internet Freedom and broader norms of liberalism that privilege free expression and the right to access information regardless of territorial boundaries. The effort constitutes a puzzling attempt by the architect of Internet Freedom to implement policies it has continuously derided abroad, in the process affecting First Amendment rights that prevent the government from making laws that abridge "the freedom of speech, or the press."[29] Although the US has attempted to prevent the rise of digital walls, counterintuitively, it went against decades of attempts to preserve liberalism online. So, what are the motivations for this about-face, and are these rationales credible?

II. Assessing the Legal Justifications for These Technology Bans

Although the US has advocated against foreign efforts to impose digital walls, the government cites characteristics of Chinese technology as threats damaging enough to national interests to justify banning Chinese communication

---

[26] Vipal Monga and Telis Demos, 'U.S. Banks Want Freer Flow of Data in Nafta Pact' *The Wall Street Journal* (2 November 2017) <https://www.wsj.com/articles/u-s-banks-want-freer-flow-of-data-in-nafta-pact-1509624001> accessed 9 August 2021.

[27] Even so, this broad policy is often inconsistent, for example, with the PRISM program.

[28] Aja Romano, 'A New Law Intended to Curb Sex Trafficking Threatens the Future of the Internet as We Know it' (*Vox*, 13 April 2018) <https://www.vox.com/culture/2018/4/13/17172762/fosta-sesta-backpage-230-internet-freedom> accessed 9 August 2021.

[29] US Const amend I.

tools. This section describes the alleged threats the US government has cited *in court and legally* as a rationale for banning Chinese technology, ranging from consumer privacy to preventing China from conducting censorship across borders.[30] We then analyse what kinds of harms these threats bring, and to whom these harms are posed. This assessment is based on five categories of harm central to cybersecurity law: harms to confidentiality, integrity, availability of information, systems, and networks.[31] Each of these harms may be to individuals, companies, or national security.[32] Finally, we assess whether these harms are based on retrospective threats or prospective ones.[33]

We then offer a rough legal estimation of whether the burden of bans based on each threat is worth the risk or liability if each threat materialized, by assessing the risk of an unaddressed remedy and the utility of implementing a remedy—effectively a derivation of the Learned Hand formula the Second Circuit used in *United States v Carroll Towing Co*, but here in the context of cybersecurity.[34] The Learned Hand formula is used to determine whether an act is negligent. Where the burden of adequate precautionary measures (B) is less than the liability or harm arising out of a potential injury (L), multiplied by the probability of that injury (P), the tortfeasor is negligent unless they implement the precautionary measure. The formula, $B < P * L$, amounts to a risk versus utility trade off.[35]

The US's articulated threats fall into two categories: broad concerns about the influence on consumers and the public (such as access to user data and censorship); and specific national security concerns (such as access of federal government users' data, corporate decision making influenced by adversarial nations, and election interference and the creation of disinformation campaigns). Narrower threats are easier to associate with harms and parties affected, whereas broader threats are either hard to verify as extant, or so broad that those threats are no different from threats associated with most digital technologies. How the US government positions the threat, both in breadth and in the potential harm, shapes whether the benefits of a ban in

---

[30] We take this legal approach because other justifications offered for these bans are less concrete, less substantiated (if at all), and less relevant when it comes to whether these bans would have ultimately survived the legal system.

[31] Jeff Kosseff, 'Defining Cybersecurity Law' (2018) 103 Iowa L Rev 985, 1010.

[32] ibid.

[33] ibid.

[34] Scott J Shackelford, Andrew A Proia, Brenton Martell & Amanda N Craig, 'Toward a Global Cybersecurity Standard of Care: Exploring the Implications of the 2014 NIST Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices' (2015) 50 Texas Intl L J 305, 315.

[35] ibid. For the original analysis, see *United States v Carroll Towing Co*, 159 F 2d 169, 173 (2d Cir 1947).

mitigating the threat outweigh the expense of free speech protections and internet freedom under US law.

Using the Learned Hand approach to assessing legal justifications, our conclusion is that narrowly defined risks indicate acute potential harm, which might be better suited as a rationale that would withstand First Amendment scrutiny. Since the US government has cited only one acute potential harm, there may be other underlying foreign policy concerns that motivate these digital walls, which will be discussed in Section IV.

A. Privacy Concerns in Access to Consumer Data

The US government fears that China will use data collected by apps to surveil American consumers. This fear has been exacerbated by growing suspicion between the US and China, with the US alleging that the Chinese government can use Chinese technology to access American consumer data, which may implicate confidentiality and data integrity, and harm consumers. Nonetheless, given the ambiguous nature of the threat as defined by the government both in court and in executive orders, mitigating such a broad risk to privacy through a technology ban is not worth the consequences to speech and internet freedom.

First, in the executive orders banning TikTok and WeChat, the Trump Administration noted that "India recently banned the use of TikTok and other Chinese mobile applications . . . [asserting] that they were 'stealing and surreptitiously transmitting users' data in an unauthorized manner to servers which have locations outside India.'"[36] More directly, in addressing WeChat, the executive order notes that "WeChat automatically captures vast swaths of information from its users. This data collection threatens to allow the Chinese Communist Party to access Americans' personal and proprietary information."[37]

The government elaborated on these claims in court cases that arose immediately after the executive orders were signed into law. In *TikTok Inc v Trump*, the government alleged that the Chinese government was "building massive databases of Americans' personal information" to "further its intelligence-gathering and to understand more about who to target for espionage, whether electronically or via human recruitment."[38] In *Huawei Techs USA Inc v United States*, the government alleged that Chinese "cyber activity"

---

[36] Exec Order No 13942 (n 7).
[37] Exec Order No 13943 (n 8).
[38] *TikTok v Trump* (n 9) [8].

could lead to the exploitation of American networks which have Chinese telecommunications equipment embedded within them.[39] More broadly, the government also alleges that Chinese government officials embedded in private Chinese technology companies create an opening for these officials to more directly sway the companies into providing the Chinese government access to American consumer data.[40] Even individuals have raised lawsuits in American courts alleging harm from Chinese surveillance through WeChat.[41]

These broad alleged risks implicate issues of data confidentiality and integrity, and this threat is likely real, judging by recent changes in Chinese law that grant the government broad authority to access data. For example, the number of Chinese Communist Party (CCP) members in management positions in a company, combined with laws like the 2017 Chinese National Intelligence Law (which the US alleges allows Chinese authorities to "take control of any China-based firm's facilities and communications equipment")[42] affect whether data remains confidential and whether it remains unaltered by anyone other than the end-users.[43]

Further, Article 14 of the Chinese National Intelligence Law states that national intelligence institutions "may request that relevant organs, organizations, and citizens provide necessary support, assistance, and cooperation."[44] This broad-based authority is not new, and has teeth: Byte Dance, TikTok's parent company, has previously cooperated with the Chinese government in shutting down one of its media platforms, reflecting the power of the National Intelligence Law in its influence over company operations.[45] The

---

[39] *Huawei Techs USA Inc v United States* 440 F Supp 3d 607, 622 (ED Tex 2020) [hereinafter *Huawei v United States*].

[40] *TikTok v Trump* (n 9) *5 (stating the government's allegations that "TikTok's foreign ownership and data collection pose a risk that the Chinese Communist Party can 'access . . . Americans' personal and proprietary information—potentially allowing China to track the locations of Federal employees and contractors, build dossiers of personal information for blackmail, and conduct corporate espionage.'") See also *Huawei v United States* (n 39) 622 (stating that the government alleges that "large Chinese companies—particularly those 'national champions' prominent in China's 'going out' strategy of overseas expansion—are directly subject to direction by the Chinese Communist Party, to include support for PRC state policies and goals.").

[41] See, eg, *Citizen Power Initiatives for China v Tencent America LLC* Docket No. 21CV375169 (Cal Super Ct 2021).

[42] *TikTok v Trump* (n 9) [9].

[43] ibid.

[44] 'China's Intelligence Law and the Country's Future Intelligence Competitions' (*Government of Canada*, 17 May 2018) <https://www.canada.ca/en/security-intelligence-service/corporate/publications/china-and-the-age-of-strategic-rivalry/chinas-intelligence-law-and-the-countrys-future-intelligence-competitions.html> accessed 18 April 2021.

[45] Jiayang Fan, 'Why China Cracked Down on the Social-Media Giant Bytedance' (*New Yorker*, 19 April 2018) <https://www.newyorker.com/news/daily-comment/

US alleges that "[Chinese] laws can compel cooperation from ByteDance, regardless of whether ByteDance's subsidiaries are located outside the territory of [China]," implying that the law impacts foreign-operated companies.[46] But the scope of authority the Chinese law provides is unclear, as is how that authority impacts user data in practice—and thus leaves ambiguous to what extent confidentiality and integrity are implicated.[47]

Recent American policy may also affect the US government's perception of the risk of access to consumer data, and the harms arising from it. The passage of the Clarifying Lawful Use of Overseas Data (CLOUD) Act, which created a mechanism to demand access to data held on servers in foreign territory for the purpose of law enforcement investigations, allows US government warrants to extend beyond US borders.[48] The Snowden disclosures also revealed a sweeping effort to gather and access foreign nationals' information, reflecting a strong signals intelligence apparatus that had the capacity

---

why-china-cracked-down-on-the-social-media-giant-bytedance> accessed 18 April 2021.

[46] *TikTok v Trump* (n 9) [8] - [9].

[47] We also note here a tangential threat: the Chinese government's coercion of companies to enforce domestic policies. However, it is hard to tell when these companies' acts abroad are done at the behest of government force, and there is inadequate information to determine whether this threat implicates access to consumer data at all. See nn 45 and 57 (exemplifying Chinese government acts that censor and shape domestic business policy of tech giants and their users). The line between broad corporate policy being shaped by government policy and specific corporate decisions being forced by individual government actors embedded in an organization is hard to discern, given the opacity of decision making within Chinese firms.

The problem is exacerbated when we examine the decisions made by Chinese-owned firms and those that are mostly privately owned. For example, Chinese state-owned companies are often used as a tool of coercion in Chinese foreign policy. Ketian Vivian Zhang, 'Chinese Non-Military Coercion – Tactics and Rationale' (*Brookings*, 22 January 2019) <https://www.brookings.edu/articles/chinese-non-military-coercion-tactics-and-rationale/> accessed 18 April 2019 (noting an incident where a Chinese state-owned company bought a Norwegian hydro company in order to get access to Norwegian expertise in deepwater drilling). But privately-owned companies are more in line with the broad goal of having indigenous companies "be globally competitive," and it is unclear what low-level decisions are enforced by Chinese government officials. ibid.

Despite this opacity, there are still reasons to be concerned: in 2016, 68% of China's private companies had party bodies, as did 70% of foreign enterprises. Richard McGregor, 'How the State Runs Business in China' *The Guardian* (25 July 2019) <https://www.theguardian.com/world/2019/jul/25/china-business-xi-jinping-communist-party-state-private-enterprise-huawei> accessed 18 April 2021. While most of these party bodies are used to influence business decisions, it is unclear if such decisions include access to, and therefore harm, US consumer data—or whether another threat, such as censorship, is implicated. ibid.

[48] See, eg, Jennifer Daskal, 'Law Enforcement Access to Data Across Borders: The Evolving Security and Rights Issues' (2016) 8 J National Security L and Policy 473; Jennifer Daskal, 'Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0' (2018) 71 Stanford L Rev Online 9–16; Jean Galbraith, 'Congress Enacts the Clarifying Lawful Overseas Use of Data (CLOUD) Act, Reshaping US Law Governing Cross-Border Access to Data' (2018) 112 American J Intl L 487.

to breach data confidentiality and integrity.[49] Thus, the threat of "access to consumer data" may indicate American discomfort with a Chinese surveillance apparatus similar to that of the US's in reach.[50]

Even assuming the threat of Chinese government access to consumer data is real, it is ambiguous what tangible harms arise from Chinese access to American consumer data. American companies like Facebook and Google gather enormous data profiles of their users, and may also affect data confidentiality and integrity. The US government also routinely accesses consumer data, both through due process[51] and by buying consumer data.[52] Why, and at what point, a foreign company's (and potentially a foreign government's) access to domestic consumer data poses more danger than a congruent access by a local company or the US government are both unclear. Both domestic and foreign companies' access to US data may have national security impacts, given that foreign governments can theoretically force American companies to hand over data. Transparency about the kinds of threats that Chinese companies uniquely pose by accessing American consumer data may provide credibility to the threat of an outright technology ban.

Even assuming the existence of the threat of access to consumer data by the Chinese government in a manner that implicates national security, mitigating this threat using a foreign technology ban would create more costs (burden, or B in Learned Hand terms) than benefits from prevented harms (P*L). The costs of such an action are massive. First, since it is widely known that the US government occasionally accesses consumer data, and that

---

[49] See generally 50 USC § 1881(a), commonly known as Section 702 of the Foreign Intelligence Surveillance Act, for an example of the US government's ability to access foreign consumer data. The relevant procedural mechanism is the FISA court, which holds such surveillance accountable, though there is significant debate—beyond the scope of this paper—about whether these courts actually enforce accountability.

[50] Henry Farrell and Abraham L Newman, 'Weaponized Interdependence: How Global Economic Networks Shape State Coercion' (2019) 44 International Security 42.

[51] See, eg, Barton Gellman & Ashkan Soltani, 'NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Documents Say' *The Washington Post* (30 October 2013) <http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html> accessed 24 April 2021.

[52] See, eg, Byron Tau & Michelle Hackman, 'Federal Agencies Use Cellphone Location Data for Immigration Enforcement' *The Wall Street Journal* (7 February 2020) <https://www.wsj.com/articles/federal-agencies-use-cellphone-location-data-for-immigration-enforcement-11581078600> accessed 24 April 2021. See generally 50 USC § 1881(a), commonly known as Section 702 of the Foreign Intelligence Surveillance Act, for an example of the US government's ability to access foreign consumer data. The relevant procedural mechanism is the FISA court, which holds such surveillance accountable, though there is significant debate—beyond the scope of this paper—about whether these courts actually enforce accountability.

American companies construct data profiles, foreign governments could use the same cudgel of "access to consumer data" to bar American companies, causing financial harm. Relatedly, other nations (such as India) may find this a useful signal to allege broad and ambiguous threats to raise digital walls, barring not just American and Chinese companies, but companies from other countries that are pretextually adversarial. There are few benefits to balance these significant costs: while the US would prevent one avenue of accessing consumer data in the short run, the Internet has few borders. The Chinese government would not find it difficult to buy American consumer data—as the American government does[53]—or use other mechanisms (like cyberattacks) to access such data, effectively not reducing the harm from this threat. In Learned Hand terms, the burden (B) incurred in implementing a ban is much higher than the (admittedly likely) liability arising from the Chinese government accessing American consumer data.

In sum, "access to consumer data" is a broad and nebulous threat. It implicates *consumer* data confidentiality and integrity. But how that associates with national security, despite Chinese policy changes that increase government access to Chinese company operations, is not outlined in a legally satisfactory way. Even if such a threat exists, the costs of mitigating it using a technology ban outweigh the benefits of curtailing the threat.

B. Foreign Censorship in the US

In addition to threats to consumer data, the US government contends that the CCP could use its influence and legal apparatus to "[censor] content that the [CCP] deems politically sensitive."[54] Such concerns are grounded in truth and implicate data integrity and access to information. The threat of censorship is a prospective threat to consumers and national security. But because allegations of censorship are broad, and the kinds of censorship which tangibly harm American consumers and the government are unclear, the impacts to speech and digital walls outweigh the benefits of fighting censorship through censoring a foreign technology.

US government concerns about censorship have to do with both censorship of the content American users consume and create, as well as the coverage of politically charged foreign policy issues, such as "content concerning protests in Hong Kong and China's treatment of Uyghurs and other Muslim minorities."[55] In addition, the US government is concerned about the

---

[53] ibid.
[54] *TikTok v Trump* (n 9) *5.
[55] *Marland v Trump* 498 F Supp 3d 624 : 2020 US Dist LEXIS 177129 at *7 (ED Pa 2020).

"censorship of critiques about the Chinese government," which is effectively propaganda for the Chinese government.[56]

These allegations of censorship are grounded in historical truth. The Chinese government has a history of censorship on the internet, including on apps and websites that are used beyond its borders.[57] Scholars have described extraterritorial instances of censorship and the reach of online policies that extend beyond national boundaries.[58] Also, American firms have been criticized for bending to the will of the Chinese government, affecting users globally. For example, the Chinese government may have pressured Apple to remove HKmap.live, an app that was used to track police activity by pro-democracy protestors in Hong Kong.[59] More subtly, the Chinese government has pressured American airlines to remove references to Taiwan from their websites globally.[60] While such censorship is tied to economic pressure, it nonetheless indicates the Chinese government's approach to speech not just domestically, but globally.

China can also censor speech beyond its borders by demanding that Chinese firms globally remove particular information. American officials claim that TikTok globally implements demands from the Chinese government to scrub inappropriate or illegal content from the platform.[61] Documented accounts

---

[56] *WeChat v Trump* (n 9) *3-4.

[57] See, eg, Min Jiang, 'Chinese Internet Business and Human Rights' (2016) 1 Business Human Rights J 139 ("Authorities have also cracked down on WeChat, asking it to remove politically 'harmful' posts and accounts."). WeChat, for example, censors users regardless of their geographic location. Eileen Guo, 'Censored by China, under Attack in America: What's Next for WeChat?' (*MIT Technology Review*, 30 October 2020), <https://www.technologyreview.com/2020/10/30/1011450/wechat-censored-china-under-attack-in-america/> accessed 18 April 2021 (noting that "American WeChat users aren't necessarily subject to the same levels of Chinese internet policing" but that "most content is still subject to the Chinese Communist Party's rules").

[58] See, eg, Jennifer Daskal, 'Borders and Bits' (2018) 71 Vanderbilt L Rev 179, 217 n 131 (examining the difficult and nebulous problem of US-based users who are promoting democracy, and being censored, in China); Jennifer Daskal, 'Speech Across Borders' (2019) 105 Virginia L Rev 1605, 1607 (discussing how China opposed big technology companies like Facebook and Twitter from shutting down pro-China propaganda accounts).

[59] Louise Matsakis, 'Apple's Good Intentions Often Stop at China's Borders' (*WIRED*, 17 October 2019), <https://www.wired.com/story/apple-china-censorship-apps-flag/> accessed 18 April 2021.

[60] Sui-Lee Wee, 'Giving in to China, US Airlines Drop Taiwan (in Name at Least)' *The New York Times* (25 July 2018) <https://www.nytimes.com/2018/07/25/business/taiwan-american-airlines-china.html> accessed 18 April 2021.

[61] Drew Harwell & Tony Romm, 'Inside TikTok: A Culture Clash Where US Views about Censorship Often were Overridden by the Chinese Bosses' *The Washington Post* (5 November 2019) <https://www.washingtonpost.com/technology/2019/11/05/inside-tiktok-culture-clash-where-us-views-about-censorship-often-were-overridden-by-chinese-bosses/> accessed 18 April 2021 (reporting that "former employees claimed attempts to persuade Chinese teams not to block or penalize certain videos were routinely ignored,

of messages disappearing and users being blocked from accessing WeChat and TikTok have been reported by users who make posts critical of the Chinese government.[62] Both history and American allegations indicate the ability of the Chinese government to impact both American consumer access to data about foreign events as well as the integrity of conversations and data on Chinese apps.

Thus, although the Chinese government's history of censorship on these applications is clear, the US government's allegations leave unsaid the harm to consumers and national security when such data integrity and access to information is impacted. This is because what constitutes censorship under the US's claims is unclear, especially given that some forms of speech regulation may be considered acceptable censorship. For example, American websites moderate content that users post, including Facebook, Twitter, and Google.[63] While most of this content moderation is not government-mandated, technology companies are liable when users post copyrighted content,[64] hate speech that incites violence,[65] and false advertising,[66] reflecting the government's role in shaping speech online. Without clarification of the harms of censorship, this threat, like Chinese access to consumer data, remains broad and unsophisticated. But such a broad allegation may still be politically credible, since a foreign censor seems far more dangerous than domestic regulation of speech, much of which seems either reasonable or within control.

---

out of caution about the Chinese government's restrictions and previous penalties on other ByteDance apps").

62 Jeanne Whalen, 'Chinese Censorship Invades the US via WeChat' *The Washington Post* (7 January 2021) <https://www.washingtonpost.com/technology/2021/01/07/wechat-censorship-china-us-ban/> accessed 18 April 2021; See also Amanda Aronczyk, 'Nervous TikTok' (*National Public Radio* 13 January 2021) <https://www.npr.org/2021/01/13/956558906/nervous-tiktok> accessed 18 April 2021 (starting at 8:14, discussing instances where TikTok videos describing Chinese treatment of Uighurs were "shadow banned," and the creators of these videos had their accounts suspended).

63 See, eg, Kate Conger, 'Facebook, Google and Twitter C.E.O.s Return to Washington to Defend their Content Moderation' *The New York Times* (28 October 2020) <https://www.nytimes.com/2020/10/28/technology/facebook-google-and-twitter-ceos-return-to-washington-to-defend-their-content-moderation.html> accessed 18 April 2021.

64 See, eg, the Digital Millennium Copyright Act, which requires that internet companies block access to material that infringes on copyright, in exchange for liability protection. Pub L No 105-304 112 Stat 2860 (Oct 28 1998).

65 See, eg, *Elonis v United States* 192 L Ed 2d 1 : 575 US ___ (2015) (finding that in order to hold the plaintiff liable for threatening statements made about his ex-wife on Facebook, the plaintiff would have had to have the right *mens rea* or intent to harm the wife).

66 See, eg, *Casper Sleep Inc v Mitcham* 204 F Supp 3d 632, 640 (SDNY 2016) (a case between an online mattress retailer and an online mattress reviewer, who falsely advertised his impartiality of mattress reviews).

Even so, the use of "censorship" as a threat that justifies banning a foreign technology may create significant consequences (burden, or B in Learned Hand terms) that outweigh the escaped liability (P*L) of preventing some censorship. First, the broad threat of censorship could set precedent allowing the government to ban other apps where foreign governments play a role in regulating American users' speech, but do not *prima facie* censor speech. For example, the German government outlaws the "use of symbols of unconstitutional organizations" like the Nazi party, outside of the contexts of "art or science, research, or teaching."[67] If the German government prevented a German citizen from talking about the Nazi party with an American person, using a German app, that could be painted as censorship.[68] Second, as with access to consumer data, such a threat/action pair could bring scrutiny to American practices of content moderation and self-regulation, with foreign governments chafing at the US government's definition of what constitutes acceptable censorship (i.e. content moderation). This could lead to foreign governments pressuring American companies to follow a content moderation regime in line with the foreign government's values. Finally, by banning technologies, the US risks leaving in dark those users in China and elsewhere who could still communicate with American users and read messages that escape censorship. The soft power of communication—both through messages received and open channels of communication—is inherently undervalued.

These costs—the Learned Hand formula's burden—are not outweighed by the value of the prevented liability, even if it is all but certain that the Chinese government is engaging in online censorship through these apps. For one, the amount of censorship that is currently taking place seems low compared to the value brought in having some access to communication with more than a billion users. By banning apps, the US government is doing the Chinese government's work by strengthening the bubble in which Chinese citizens live. A ban raises the burden, B, incurred by the US, by strengthening Chinese censorship. Further, the CCP's current controlled information ecosystem is already frowned upon globally. A ban would indicate that the US government is comfortable with controlling the information ecosystem at home, legitimizing the Chinese policy (and perhaps encouraging other

[67] 'Strafgesetzbuch § 86a' (*German Law Archive*, 13 November 1998) <https://germanlawarchive.iuscomp.org/?p=752> accessed 18 April 2021.

[68] Especially, as it stands, speech about Nazis, even in the public arena, is considered protected by the First Amendment. See, eg, *National Socialist Party of America v Village of Skokie* 1977 SCC OnLine US SC 113 : 53 L Ed 2d 96 : 432 US 43 (1977) (reversing an Illinois state court's decision to provide an injunction against the NSPA's (a neo-Nazi organization) request for a permit to march in Skokie, reasoning that the display of Nazi logos were not fighting words that were not protected by the First Amendment).

countries adversarial to China, like India, to enact their own technology bans), instead of the status quo.

Thus, the idea of "censorship" as a threat is broad and nebulous. It implicates consumer data integrity and access to information, and may tangentially impact national security. Yet, how substantial this threat is, given the undefined contours of "censorship," is unclear. These uncertainties indicate that the small benefit of preventing Chinese censorship by banning Chinese technology may not be worth the costs of retaliation, scrutiny, and loss of communication with foreign users.

C. Risks to US Military and Government Employees

All governments are animated by a desire to protect national security. An explicit and tangible risk to US national security, as opposed to a general threat to consumers, is the potential for the Chinese government to access federal employees' data and disrupt government infrastructure. The history of Chinese cyberattacks on US government data indicates that this risk to government systems and networks has significant harms to national security, and warrants some policy response.

President Trump's Executive Order 13,942 found that TikTok's data collection could allow "China to track the locations of Federal employees and contractors [and] build dossiers of personal information for blackmail."[69] In addition, the government claims that its networks "face significant information security risks, including the threat of unauthorized access, use, disclosure, disruption, modification, or destruction of government information" and that "the development of Internet of Things (IoT) is placing these government networks further at risk" from technology companies stationed in adversarial countries.[70] The National Security Agency (NSA), among other intelligence agencies, has already stated that Chinese "state-sponsored cyber actors . . . exploit computer networks of interest that hold . . . political and military information."[71]

This risk is serious enough that the federal government has taken steps in the past to prevent foreign software and hardware from being used by government employees and on government networks. The government stopped software from Kaspersky Labs (a Russian software company) from being

---

[69] Exec Order No 13942 (n 7).

[70] *Huawei v United States* (n 39) 640.

[71] National Security Agency, 'Cybersecurity Advisory' (*US Department of Defense*, October 2020) <https://media.defense.gov/2020/Oct/20/2002519884/-1/-1/0/CSA_CHINESE_EXPLOIT_VULNERABILITIES_UOO179811.PDF> accessed 18 April 2021.

used on its networks, indicating that this perceived risk was due to the connection with Russia.[72] Further, the threat from China is not speculative, given the history of Chinese-origin hacks and attacks towards government workers and agencies. For example, in 2015, the Social Security Numbers (SSNs) and other records of 21.5 million past, present, and prospective federal employees were stolen.[73] While the government did not directly confirm that the Chinese government was behind the attacks, then-Director of National Intelligence James Clapper identified China as the "leading suspect,"[74] and later, a Chinese national was arrested by the FBI in connection with the hacks.[75] Among other attacks are those on the US Navy and its industrial partners.[76] In addition to creating vulnerabilities in infrastructure and defence systems, the information collected could be used for blackmail or to obtain bargaining advantages when the Chinese government possesses sensitive personal information about American officials.

Similarly, Congress also articulated this risk in its CFIUS review of Grindr, the LGBTQ dating app that was previously owned by a Chinese investment firm. CFIUS warned that data collected about American citizens—especially information about sexual preferences or HIV status—could be used to blackmail American officials and military personnel.[77] The review led to

---

[72] 115 PL 91 § 1634 (2017) (prohibiting the use of products and services developed by Kaspersky Lab, a cybersecurity company headquartered in Russia). The language in § 1634 was then effectively reused when banning Huawei products being used on government networks in 115 PL 232, § 889 (2018) (prohibiting the use of "[t]elecommunications equipment produced by Huawei Technologies Company or ZTE Corporation.").

[73] 'Cybersecurity Incidents' (*Cybersecurity Resource Center at US Office of Personnel Management*) <https://www.opm.gov/cybersecurity/cybersecurity-incidents/> accessed 11 November 2021.

[74] Kristin Finklea et al, Cong Rsch Serv, R44111, Cyber Intrusion into US Office of Personnel Management: In Brief (2015) <https://fas.org/sgp/crs/natsec/R441

[75] Devlin Barrett, 'Chinese National Arrested for Allegedly Using Malware Linked to OPM Hack' *The Washington Post* (24 August 2017) <https://www.washingtonpost.com/world/national-security/chinese-national-arrested-for-using-malware-linked-to-opm-hack/2017/08/24/746cbdc2-8931-11e7-a50f-e0d4e6ec070a_story.html> accessed 18 April 2021.

[76] Gordon Lubold & Dustin Volz, 'Navy, Industry Partners are 'Under Cyber Siege' by Chinese Hackers, Review Asserts' *The Wall Street Journal* (12 March 2019) <https://www.wsj.com/articles/navy-industry-partners-are-under-cyber-siege-review-asserts-11552415553> accessed 18 April 2021.

[77] David E Sanger, 'Grindr is Owned by a Chinese Firm, and the U.S. is Trying to Force it to Sell' *The New York Times* (28 March 2019) <https://www.nytimes.com/2019/03/28/us/politics/grindr-china-national-security.html> accessed 18 April 2021; See also James Fontanella-Khan & Yuan Yang, 'Grindr Sold by Chinese Owner After US National Security Concerns' *Financial Times* (7 March 2020) <https://www.ft.com/content/a32a740a-5fb3-11ea-8033-fa40a0d65a98> accessed 18 April 2021.

the company agreeing to limit transfers of data to China and basing its headquarters in the US.[78]

Unlike the previous two harms, harms to government employees and infrastructure are narrow and well defined, and in light of the history of Chinese and foreign cyberattacks against US government infrastructure, clearly impact national security. Of course, not all national security threats justify passing policies that may affect civil liberties. The policy response should depend on the nature of the threat. One framework for categorizing these threats is to determine whether they are non-significant, significant, or an act of war.[79] This categorization depends on the "actual and anticipated effects of any cyber incident, including injury, damage, and death."[80] At the very least, prior Chinese cyber-attacks are not non-significant, since they have resulted in significant data theft,[81] the theft of intellectual property,[82] and the risk of damage to physical infrastructure.[83] The kind of threat the US government is alleging is rooted in reality, and not the sort of edge case that is difficult to pinpoint, unlike generalized harms arising from access to consumer data or nebulous notions of censorship. This kind of threat justifies some response.

---

78 ibid; See also CFIUS discussion, s III.C.

79 Nicole Softness, 'How Should the U.S. Respond to a Russian Cyber Attack', (2017) 12 Yale J Intl Affairs 99, 106.

80 ibid 107.

81 See, eg, Ryan Lucas 'Chinese Hackers Charged in Alleged Cyber-Theft of 145 Million Americans' Data' (*NPR*, 10 February 2020) <https://www.npr.org/2020/02/10/804501991/chinese-hackers-charged-in-alleged-cyber-theft-of-145-million-americans-data> accessed 18 April 2021.

82 See, eg, Jeffrey B Jones, 'Confronting China's Efforts to Steal Defense Information' (*Belfer Center for Science and International Affairs, Harvard Kennedy School*, 2020) <https://www.belfercenter.org/sites/default/files/2020-05/ChinaStealing.pdf> accessed 18 April 2021 (noting that Chinese theft of intellectual property "is costing industry in the range of $180 billion to as high as $540 billion per year" due to cyber espionage). See also Erica D Borghard & Shawn W Lonergan, 'Chinese Hackers are Stealing US Defense Secrets: Here is How to Stop Them' (*Council on Foreign Relations*, 11 March 2019) <https://www.cfr.org/blog/chinese-hackers-are-stealing-us-defense-secrets-here-how-stop-them> accessed 18 April 2021.

83 See, eg, Adam Clark Estes, 'Chinese Army Hackers are Trying to Bring Down US Infrastructure, After All' (*The Atlantic*, 18 February 2013) <https://www.theatlantic.com/international/archive/2013/02/chinese-army-hackers-are-trying-bring-down-us-infrastructure-after-all/318215/> accessed 18 April 2021; Kim Zetter, 'Solar Winds Hack Infected Critical Infrastructure, Including Power Industry' (*The Intercept*, 24 December 2020) <https://theintercept.com/2020/12/24/solarwinds-hack-power-infrastructure/> accessed 18 April 2021; David E Sanger, Julian E Barnes & Nicole Perlroth, 'Preparing for Retaliation Against Russia, US Confronts Hacking by China' *The New York Times* (7 March 2021) <https://www.nytimes.com/2021/03/07/us/politics/microsoft-solarwinds-hack-russia-china.html> accessed 18 April 2021.

However, responding to the threat to government systems and networks through a technology ban may not be worth the costs to speech and internet freedom. The burden B, or cost in the Learned Hand formula, is one to civil liberties. Assessing the value of this burden is entirely subjective, and therefore difficult to estimate.[84] But US courts and the government are generally comfortable with abridging civil liberties—especially those related to the First Amendment—during wartime or when serious national security risks are involved. For example, in *Schenck v United States*, the Supreme Court upheld a statute that ambiguously forbade speech "advising or teaching the duty . . . or propriety of overthrowing" the government.[85] More recently, in *Holder v Humanitarian Law Project*, the Court upheld provisions of the Material Support Statute, which forbade Americans from providing legal services or even advocacy training to any organization the State Department designated as a terrorist organization—including, controversially, the Kurdistan People's Party.[86] The Court has also upheld the Patriot Act, which allows for surveillance of non-US persons when related to national security.[87] Beyond the First Amendment, the Court has upheld bans on movement and immigration during wartime, first in *Korematsu v United States* (where the Court upheld forced internment of Japanese-American citizens),[88] and recently in *Trump v Hawaii* (where the Court upheld the travel ban against some Muslim countries).[89] In short, in scenarios such as US-China cyber hostilities, civil rights may not be valued highly by courts.

On the other side of the Learned Hand equation is the liability and probability of harm (P*L). The probability of a cyberattack that leverages data or application infrastructure is not insignificant, given the escalating pattern of Chinese cyberattacks. The liability, or cost of harms, is high, ranging from intellectual property theft to damage to critical infrastructure. Even assuming the abstract harm to civil rights is high, the cost on the other side is likely higher, given the risk of damage and death arising from escalating cyberattacks. Simply put: the risk to government employees and infrastructure is real, and the harms avoided *may* outweigh the costs to civil liberties.

---

[84] In fact, courts are hesitant to provide compensatory damages in § 1983 claims (generally claims where the government violates constitutional rights and plaintiffs sue the government), where the award focuses on the abstract value of the constitutional right at issue. See, eg, *Memphis Community School Distt v Stachura* 1986 SCC OnLine US SC 148 : 91 L Ed 2d 249 : 477 US 299, 308 (1986) (noting that "the abstract value of a constitutional right may not form the basis for § 1983 damages").

[85] 1919 SCC OnLine US SC 62 : 63 L Ed 470 : 249 US 47 (1919).

[86] *Holder v Humanitarian Law Project* 2010 SCC OnLine US SC 75 : 561 US 1, 9-10 (2010).

[87] See, eg, Susan N Herman, 'The USA Patriot Act and the Submajoritarian Fourth Amendment' (2006) 41 Harvard Civil Rights-Civil Liberties L Rev 67, 78.

[88] 1944 SCC OnLine US SC 135 : 89 L Ed 194 : 323 US 214 (1944).

[89] 138 S Ct 2392 : 585 US __ (2018).

Even with this close calculus, a narrower approach to securing government networks may be more beneficial in the long run. Especially given limited political capital and the difficulty of a systemic approach to improving government cybersecurity, a ban on foreign technology could be passed in lieu of improving government cybersecurity infrastructure, leaving vulnerabilities such as those that led to the latest Russian hacking of US government systems unaddressed.[90] There is also incentive to develop a more targeted remedy: if the government articulates the risk of a foreign technology this narrowly, remedies that impact speech will likely have to be as narrowly-tailored as possible, so as to minimally infringe upon First Amendment rights of users.[91] Finally, while the Court has been amenable to abridging civil rights during wartime, setting a precedent, through a technology ban, of policy that abridges an avenue of speech is a dangerous path, and one that should be trod upon only when other options are exhausted.

To sum up, the threat to government workers and infrastructure is a clearly articulated threat that falls neatly within the framework of cybersecurity law, impacting systems and networks. This clearly implicates national security, and the threat is substantial—and perhaps the costs of such a threat are higher than the burdens on civil liberties. But, while addressing such risks through a technology ban may well be worth some cost to speech and internet freedoms, there are better ways of mitigating such a risk that provide more protections to speech and civil rights.

D. Chinese Election Interference and Disinformation Campaigns

Finally, the US government contends that there is a risk "of disinformation campaigns that benefit the [Chinese government], such as when TikTok videos spread debunked conspiracy theories about the origins of the 2019 Novel Coronavirus."[92] Both Democratic and Republican elected officials have also expressed concern that TikTok is a "potential target of foreign influence campaigns, like those carried out during the 2016 election." This indicates that disinformation campaigns pertaining to elections may be a risk incurred due to the use of TikTok.[93] Such risks implicate data integrity and access

---

[90] David E Sanger, Nicole Perlroth & Julian E Barnes, 'As Understanding of Russian Hacking Grows, So Does Alarm' *The New York Times* (2 January 2021) <https://www.nytimes.com/2021/01/02/us/politics/russian-hacking-government.html> accessed 18 April 2021.

[91] See s IV.A

[92] *TikTok v Trump* (n 9) 5.

[93] 'Letter from Charles E. Schumer and Tom Cotton to Joseph Maguire' (*United States Senate*, 23 October 2019) <https://www.democrats.senate.gov/imo/media/doc/10232019%20TikTok%20Letter%20-%20FINAL%20PDF.pdf> accessed 18 April 2021.

to information, in a manner that prospectively impacts national security. But evidence of the Chinese government engaging in election interference is scant. Evidence of Chinese disinformation campaigns is part reality, part myth.[94] And the harm from such campaigns has only begun to be realized. Like the threat of censorship, without a clear understanding of what kinds of election interference and disinformation are being propagated, it is impossible to assess the actual dangers to national security, and difficult to understand whether a technology ban is the most effective approach, or at least one worth the costs to free speech and internet freedom.

Admittedly, social media platforms are vessels for propagating disinformation and exacerbating election interference campaigns.[95] The Russian government used Facebook, Twitter, YouTube, and Instagram in its 2016 election interference campaign.[96] Also, in the 2020 election, Facebook and Twitter, among others, have been in the spotlight for the intensity and volume of disinformation—especially pertaining to elections—that courses through their networks.[97] Given this, it is possible that TikTok, as a major social media platform in the lead-up to the 2020 election, was a vessel for disinformation. However, the extent to which the Chinese government used the platform to impact the 2020 election is unclear, especially at the time of writing. Additionally, the primary source of election interference in 2016 was Russia, and the Mueller Probe and Congress took significant steps to uncover proof of this interference. In contrast, claims about Chinese interference in American elections through a disinformation campaign are unsubstantiated or even decried, and proof about such interference is unlikely to be forthcoming without such an investigation.[98] Nonetheless, the broad

---

[94] Dustin Volz, 'U.S. National Security Adviser Says China Targeting 2020 Election' (*The Wall Street Journal,* 9 August 2020) <https://www.wsj.com/articles/u-s-national-security-adviser-says-china-targeting-2020-election-11597007831> accessed 9 August 2021. Note that "Mr O'Brien's comments were met with skepticism by other officials familiar with the matter. While China has an active interest in the election, the U.S. doesn't currently have intelligence showing that Beijing is directly trying to hack election-related systems, the officials said."

[95] Hunt Allcott & Matthew Gentzkow, 'Social Media and Fake News in the 2016 Election' (2017) 31 J Econ Persp 211, 212 (discussing that "the most popular fake news stories were more widely shared on Facebook than the most popular mainstream news stories" and that "115 pro-Trump fake stories . . . were shared on Facebook a total of 30 million times").

[96] See generally Select Committee on Intelligence, US Senate, *(U) Report* (Vol 2, Committee Print 2020) <https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf> accessed 18 April 2021.

[97] Alex Webb, 'Disinformation Threatens Other Elections After US Voting Ends' *Bloomberg* (3 November 2020) <https://www.bloomberg.com/news/articles/2020-11-03/election-2020-disinformation-on-facebook-twitter-looms-after-polls-close> accessed 18 April 2021 (discussing that "disinformation, propaganda, and fake news are as big a problem elsewhere as they are in the US" on Facebook, Twitter, and Alphabet).

[98] Volz (n 94).

allegation that TikTok *could* be used to sow disinformation and impact elections likely implicates data integrity and access to information, but only because TikTok is just another social media platform where disinformation and election interference are common occurrences.

There is also some truth to the allegation that TikTok plays a role in spreading disinformation—as does all social media. However, the threat of disinformation spread is broad, and the threshold for the kinds and amounts of disinformation that threatens data integrity and access to information in a manner that harms national security has not been clearly articulated by the government. A significant amount of Russian government-backed disinformation (amongst others) flows through Facebook, Twitter, and other American companies. Yet, the government has not taken steps towards curbing disinformation on domestic platforms, indicating that some amount of disinformation may be acceptable and not worth disrupting, given the-side-effect of affecting speech and other civil liberties.

Even assuming that the threat of Chinese disinformation and election interference exists in a well-articulated, clear form, the costs (B) of addressing this threat are not worth the prevented liability (P*L). Without a clear rule about how disinformation on TikTok is more harmful than those on domestic platforms and what harms must be mitigated, the US government opens American platforms to retaliation in foreign countries. Further, a foreign technology ban because of disinformation originating from China will not stop Chinese disinformation campaigns from permeating domestic platforms, without parallel regulation of domestic companies like Facebook and Twitter. Instead, such a technology ban may have the perverse consequence of reallocating disinformation resources to Facebook and other social media platforms that have larger user bases than TikTok, increasing the strength of these foreign campaigns.

In sum, there is some evidence of Chinese disinformation campaigns, but little to none of the Chinese election interference. Nonetheless, the American government's articulation of this threat is not well defined. While the threat impacts data integrity and access to information in the context of national security, the magnitude of this threat is unclear. The little benefit of mitigating this threat through a foreign technology ban is not worth the cost of shifting disinformation onto more widely-used platforms like Facebook.

III. The Methods of Raising Digital Walls in the US

Given that the US has framed the issue as a threat to security interests and sovereignty, there is a broad array of tools at the government's disposal. To

combat the aforementioned risks posed by foreign technology companies, the US government has used three main tools:[99] the IEEPA, which is used by the President to handle threats that may cause national emergencies; Congressional statutes that can protect privacy by preemptively imposing sanctions on companies that may cause harm; and CFIUS review, which is a tool jointly employed by the President and Congress to investigate foreign investments in technology companies. Together, these tools give the executive and the legislature broad power, albeit subject to some constraints, to act against technology companies, even if the risks are not yet rooted in reality. We provide a brief overview of these tools and assess the broader structural problem: that such blunt, powerful tools create incentives to enact such technology bans, even at the expense of civil liberties and undermining existing US Internet Freedom policy.

A. IEEPA

IEEPA authorizes the President to approach "unusual and extraordinary threat[s] . . . . to the national security, foreign policy, or economy of the United States" that originate from outside the US, by allowing the President to declare a national emergency regarding that threat.[100] Concerning foreign companies like TikTok, the Act authorizes the President to "investigate . . . , regulate . . . , or prohibit . . . transactions involving any property in which any foreign country or a national thereof has any interest . . . subject to the jurisdiction of the United States . . . ."[101] However, the act forbids the President from exercising such authority over "any postal, telegraphic, telephonic, or other personal communication, which does not involve a transfer of anything of value. . .", or "the importation from any country . . . of any information or informational materials, including . . . news wire feeds."[102] Finally, the IEEPA also grants broad authority to the President when dealing with economic or industrial espionage occuring in cyberspace, allowing the President to "block and prohibit all transactions in all property and interests in property" against *persons* who are engaging in economic or industrial espionage in cyberspace of intellectual property of US persons.[103]

Thus, the IEEPA effectively grants the President a strong, albeit conditional, power to regulate foreign corporations that pose a danger to the US, but creates exceptions for personal communications technologies. Presidents

[99] This list is not a comprehensive one, but only outlines the main tools that fit within the limited scope of this paper.
[100] 50 USC § 1701(a).
[101] 50 USC § 1702(a)(1)(B).
[102] 50 USC § 1702(b)(3).
[103] 50 USC § 1708(b).

Trump and Obama have exercised the authority accorded to them by the IEEPA thrice to address cybersecurity threats stemming from Chinese companies. President Obama signed Executive Order 13,694 to target persons engaging in "malicious cyber-enabled activities" through sanctions, including individuals who use computers to harm critical infrastructure, cause a disruption to the internet, or conduct online theft.[104] President Trump then signed Executive Order 13,848, which sanctions individuals conducting foreign interference in the US elections by "materially assisting . . . or providing technological support . . . ."[105] It also allows the executive branch to exclude a company's alien corporate officers from the US.[106] Finally, the most prominent Executive Order is 13,873, which addresses securing information and communications technology and services by allowing the executive branch to prohibit the transfer or installation of foreign technologies that pose a threat to national security.[107] This final order was the basis for the Executive Orders issued to address threats posed by TikTok[108] and WeChat.[109]

Taken together, the IEEPA enables the President, who acts alone through executive orders, to target individuals and companies known to be maliciously impacting the US through communication technologies. However, the President must first declare a national emergency before he can exercise authority under the IEEPA.[110] Additionally—and most importantly—the President cannot regulate personal communications or informational materials.[111]

Despite these minor controls, the wording of the three aforementioned Executive Orders indicates that this tool can have a broad scope, and at the least can be used to hamper the operations of foreign companies on US soil, without the President having to truly articulate and "prove" in court the risks to privacy and national security. This means there is little incentive to elaborate on how the privacy concerns pertaining to consumer data, censorship, and disinformation campaigns mentioned are tied to national security. Further, since cyberattacks are often unattributable, and can use technology without the consent of the user (e.g. through a Distributed Denial

---

[104] Exec Order No 13694, 80 Fed Reg 18077 (Apr 1 2015).
[105] Exec Order No 13848, 83 Fed Reg 46843 (Sept 14 2018).
[106] ibid.
[107] Exec Order No 13873, 84 Fed Reg 22689 (May 17 2019).
[108] Exec Order No 13942 (n 7).
[109] Exec Order No 13943 (n 8).
[110] *Marland v Trump* (n 55) 13.
[111] ibid. In at least one other case, the courts have specifically prevented the President from regulating communications apps because the President is not allowed to regulate "personal communication[s]." *United States Wechat Users Alliance v Trump* 20-cv-05910-LB 2020 US Dist LEXIS 197776 at 3-4 (ND Cal 2020).

of Service attack), Executive Orders provide the flexibility to sanction individuals who may be indirectly or vaguely associated with attacks, under the guise of national security.[112] Finally, and most critically, IEEPA's breadth creates a structure for the President to "prohibit" technology,[113] rather than take the narrower approach of addressing the underlying risks. For example, since IEEPA can be used to ban technology—and can be done unilaterally by the executive—it may be an easier solution than more targeted solutions that protect consumer privacy or prevent disinformation.

B. Congressional Statutes

The legislative branch also has considerable power in this arena: Congress can pass legislation that targets corporations that it considers a threat to national security. However, Congress cannot pass bills that specifically punish a single entity, known as bills of attainder.[114] Statutes that legislatively determine guilt, whether retrospective or prospective, are considered invalid.[115] Courts look at whether statutes are a legitimate regulation of conduct, which is allowed; or whether they are punishment, which is prohibited.[116] Even so, statutes which target a single company can still be legitimate if there are "legitimate justification[s]."[117]

An example of a legitimate statute is the 2019 National Defense Authorization Act, which prohibited regulatory and government agencies from procuring telecommunications equipment from Chinese companies Huawei, ZTE, Hytera Communications, Hangzhou Hikvision Digital

---

[112] Attribution is difficult because "[c]omputer networks are not designed to facilitate attribution, and hostile actors exploit this weakness to hide their true identity." Eric F Mejia, 'Act and Actor Attribution in Cyberspace: A Proposed Analytic Framework' (2014) 8 Strategic Studies Q 114, 121-22.This can be done through a variety of methods, including spoofing, host laundering, and attacks spread over months. ibid. Attribution is further complicated if attackers use methods like a Distributed Denial of Service Attack (DDoS), which use networks of bots—hijacked computers that, unknown to the user, are involved in malicious attacks—to shut down websites or online services. See, eg, Michael Gervais, 'Cyber Attacks and the Laws of War' (2012) 30 Berkeley J Intl L 525, 555-56. Because the laws of international relations and war, and the laws of cyberspace are so orthogonal, it seems almost impossible to identify persons engaging in "malicious cyber-enabled activities" or providing "technological support" for election interference.

[113] 50 USC § 1702(a)(1)(B).

[114] US Const art I, § 9, cl 3. See also *Nixon v Administrator of General Services* 1977 SCC OnLine US SC 152 : 53 L Ed 2d 867 : 433 US 425, 476 (1977) (noting that retrospective statutes include those that "[inflict] deprivations on some blameworthy or tainted individual in order to prevent . . . future misconduct.").

[115] *United States v Brown* 1965 SCC OnLine US SC 123 : 14 L Ed 2d 484 : 381 US 437, 458-59 (1965).

[116] *Nixon*, 1977 SCC OnLine US SC 152 : 53 L Ed 2d 867 : 433 US 425, 476 (n 114).

[117] ibid 472 & 477.

Technology Company, and Dahua Technology Company.[118] The statute was ruled to be constitutional because the government had the nonpunitive purpose of securing "the federal government's information systems," which included protecting the government's networks from the risk of Internet of Things (IoT) devices.[119] China's history of attacking government networks, including through private contractors, provided a rationalization for such a risk.[120] A similar risk from Russian government cyberattacks was used as justification for prohibiting the use of Kaspersky Lab products by the American government.[121] Note however in both these cases that Congress only limited the *federal government* from using or purchasing the selected companies' products, and did not prohibit private citizens from buying from these companies.

Put simply, Congress can target companies it considers risky, especially if there is a history of attacks originating from the countries of origin. However, the noted limitations—nonpunitive actions and the need for legitimate justification—effectively require Congress to provide well-articulated risks, *unlike* the ones in Section II, before implementing technology bans and raising digital walls. And the limitations and statutory precedent indicate a preference for narrower policy solutions, like preventing the federal government from buying foreign technology, rather than an all-inclusive ban. But history may not be an indicator of the future. Given Congress' broad statutory power,[122] especially in the realm of national security, and given the established risks in the domain of cyberspace, Congress may chart a new path forward and engage in broader technology bans. But given the cumbersome nature of Congressional action, combined with Congressional gridlock, statutory action is the least likely of the three, even though it is the one that creates the most precedent and potential for narrow policy approaches.

C. CFIUS Review

The Congressional Committee on Foreign Investment in the US, or CFIUS, conducts reviews that focus on the national security implications of foreign

---

[118] John S McCain National Defense Authorization Act for Fiscal Year 2019 § 889 PL 115-232 (2018).

[119] *Huawei v United States* (n 39) 639-40.

[120] ibid 641. This history of attacks is also what lends legitimacy to the risk to federal employees and government infrastructure that the government has articulated in the TikTok and WeChat bans, noted in s II.C.

[121] National Defense Authorization Act for Fiscal Year 2018 § 1634 PL 115-91 (2017). See also *Kaspersky Lab Inc v United States Department of Homeland Security* 909 F 3d 445 (DDC 2018) (upholding the restriction under *Nixon* and finding that the targeting of Kaspersky products was not a violation of the bill of attainder clause).

[122] See, eg, US Const art I, § 8, cls 10-16.

investments in American companies or operations. The committee's focus is on ensuring that American technology is not transferred to countries that pose national security risks, as opposed to focusing on day-to-day operational decisions made by companies.[123] Broadly, CFIUS reviews look at transactions where a foreign government has a "substantial interest," and then the committee conducts national security risk assessments and creates potential protective measures to prevent impacts to national security.[124] The review's scope has recently expanded with the Foreign Investment Risk Review Modernization Act of 2018, which allows for CFIUS review to focus on "critical technolog[ies]" and "critical infrastructure."[125] The act also focuses on Chinese investment in the US.[126] Generally, however, the CFIUS review is "highly secretive."[127]

The CFIUS review has been used recently to examine Chinese investment into American hardware and software companies. In 2016, due to national security concerns, President Obama blocked Chinese company Grand Chip Investment from acquiring a controlling interest in the American assets of German company Aixtron, a semiconductor coating manufacturer.[128] This was only the third time a President had used CFIUS review to prevent foreign investment, indicating the extraordinary circumstances and importance of Aixtron's assets in the US.[129] The next time a President used the review was in 2017, when President Trump blocked a Chinese investment firm from acquiring Lattice Semiconductor, again for national security concerns.[130] However, national security concerns are not limited to China; in 2018, President Trump blocked the acquisition of Qualcomm, a semiconductor maker, by Broadcom, which is based in Singapore.[131]

---

[123] Cong Rsch Serv, RL33388, The Committee on Foreign Investment in the United States (CFIUS) 1 (2020).

[124] ibid 14.

[125] ibid 2.

[126] ibid 11.

[127] See, eg, David E Sanger, 'Grindr is Owned by a Chinese Firm, and the US is Trying to Force it to Sell' *The New York Times* (28 March 2019) <https://www.nytimes.com/2019/03/28/us/politics/grindr-china-national-security.html> accessed 19 April 2021 (noting that CFIUS is "a highly secretive panel").

[128] Exec Order Regarding the Proposed Acquisition of a Controlling Interest in Aixtron SE by Grand Chip Investment GMBH 81 Fed Reg 88607 (Dec 2 2016).

[129] The first Presidential use of CFIUS was by President George H.W. Bush, who voided the sale of aircraft parts maker Mamco Manufacturing to a Chinese state-owned aircraft company. The second was by President Obama, who ordered Chinese investors to divest from wind farm projects located near a US Navy Weapons systems training facility. See n 123 at 21.

[130] Exec Order Regarding the Proposed Acquisition of Lattice Semiconductor Corporation by China Venture Capital Fund Corporation Limited 82 Fed Reg 43665 (Sept 13 2017).

[131] Exec Order Regarding the Proposed Takeover of Qualcomm Incorporated by Broadcom Limited 83 Fed Reg 11631 (Mar 12 2018).

And, presidential action is not needed to prevent foreign investment into domestic companies. In 2019, Congress initiated a CFIUS review of Chinese firm Beijing Kunlun Tech's acquisition of Grindr, the popular LGBTQ dating app. The review may have been triggered by access to US officials and government contractors' app data, including users' location data,[132] and the review caused the Chinese firm to divest itself of the app.[133] A similar concern over data privacy caused CFIUS to block a merger between MoneyGram, a money transfer company, and Ant Financial, a Chinese e-payments company.[134]

While secretive, the history of CFIUS review and presidential orders using CFIUS review indicates that Congress and the Executive find the review an easy, opaque, and effective method of blocking the sale of companies that may be of national security concern. The use of the review in the past decade indicates that the sale of American technology companies to Chinese or China-proximate companies could pose a national security concern, but does not provide insight into what risk specifically, beyond the vague notion of "access to personal data," exists. This is problematic, especially if policymakers and lawyers want to shed light on the reasoning behind American motivations for digital walls. On the other hand, CFIUS review (without 'the') is generally used to protect existing companies from receiving foreign investors, rather than outright and proactive bans. Thus, the use of this tool may be to indirectly prevent the growth of home-grown technologies, rather than preventing foreign companies from establishing or continuing a US presence. Still, this subtle form of creating an "investment wall" is an extension of digital walls, and the lack of process transparency is troubling.

IV. The Implications of Digital Walls

Questions of borders and digital walls implicate free speech, both domestically and globally.[135] US internet users will be denied a communication platform, which may have implications concerning the First Amendment. Additionally, global implications that must be considered include how such technology bans will undermine the US Internet Freedom policy and how

---

[132] Sarah Bauerle Danzman & Geoffrey Gertz, 'Why is the US Forcing a Chinese Company to Sell the Gay Dating App Grindr?' *The Washington Post* (3 April 2019) <https://www.washingtonpost.com/politics/2019/04/03/why-is-us-is-forcing-chinese-company-sell-gay-dating-app-grindr/?utm_term=.799ee5be1f32> accessed 19 April 2021.

[133] ibid.

[134] Ana Swanson & Paul Mozur, 'MoneyGram and Ant Financial Call Off Merger, Citing Regulatory Concerns' *The New York Times* (2 January 2018) <https://www.nytimes.com/2018/01/02/business/moneygram-ant-financial-china-cfius.html> accessed 19 April 2021.

[135] *Who Controls the Internet* (n 17) 150.

such bans may undermine the borderless technical foundations of the internet, lending support for the Chinese vision of the internet.

A. First Amendment and Free Speech

If the government aims to ban apps entirely, as in the case of WeChat and TikTok, courts may consider the consequences relating to the First Amendment implications. The First Amendment prevents the government from making laws that "[abridge] the freedom of speech, or that of the press."[136] Banning apps like WeChat that serve as "public square[s]"[137] raise First Amendment concerns, and the government must satisfy heightened scrutiny for the ban to be upheld by courts. In court, this requires assessing whether the abridgement of speech is narrow enough and sufficiently justified by government need. Where a law regulates speech in a content-neutral manner, the government must satisfy some requirements of intermediate scrutiny i.e., the law must be "(1) narrowly tailored, (2) serve a significant governmental interest unrelated to the content of the speech, and (3) leave open adequate channels of communication."[138] When the law regulates speech in a manner that is content-based (i.e. discriminates against a specific viewpoint), strict scrutiny applies.[139] Strict scrutiny requires the government to prove that the restriction "furthers a compelling interest and is narrowly tailored to achieve that interest."[140]

It is unclear whether banning an app is content-neutral or content-based. For example, banning an app is a time, place, and manner restriction that prohibits *all* speech at a given place (the app), and such regulation requires intermediate scrutiny.[141] At the same time, certain apps have specific types of content, so banning the app could be content-based. For example, WeChat's content focuses on Chinese-language speakers and relays issues and information pertinent to Chinese speakers. Courts have not adequately considered this problem, to determine whether such a ban is content-neutral or

---

[136] US Const amend I.

[137] *WeChat v Trump* (n 9) 26-28.

[138] ibid (citing *Ward v Rock against Racism*, 1989 SCC OnLine US SC 140 : 105 L Ed 2d 661 : 491 US 781, 791 [1989]).

[139] See, eg, *Reed v Town of Gilbert* , 192 L Ed 2d 236 : 576 US 155, 172 (2015).

[140] See, eg, *Ward v Rock against Racism* 1989 SCC OnLine US SC 140 : 105 L Ed 2d 661 : 491 US 781, 791 (1989) ("the government may impose reasonable restrictions on the time, place, or manner of protected speech, provided the restrictions" satisfy intermediate scrutiny).

[141] ibid.

content-based. Nonetheless, at minimum, intermediate scrutiny applies—and even this would be hard for the government to satisfy.[142]

The narrowness prong of the test is averse to outright bans on an app, especially where the ban may be incongruent with the government's assessment of potential risk. For example, in *US WeChat Alliance v Trump*, the Trump Administration tried to ban downloads of WeChat due to national security concerns, one of which was that the app was being downloaded on government devices.[143] The court found that "barring WeChat from government devices" is a narrowly tailored alternative to an outright ban, which it did not deem to be sufficiently narrow.[144] Thus, the government's assessment and allegation regarding the risks it faces plays a critical role in determining whether the solution—banning an app—is legally permissible.[145] In the cases assessed in this paper, the risks defined by the government have varied.[146] If the actual risks are to consumer data and censorship, then an app ban, regulation, or changes to the app may be as "narrow" as possible and may fulfil the second prong of the test, i.e., the requirement that the ban must have a significant relation to a governmental interest *unrelated* to the speech itself (in this case, protecting American consumers). However, if the risks are primarily to government employees, then a narrowly tailored solution preventing government employees from downloading that app on government devices may be the only permissible one, and the second prong of the test may not even be reached. Either way, since issues concerning election interference, foreign control of apps, and data access are in flux and have

---

[142] The picture is further complicated by the question of whether the speech considered is political or commercial. See, eg, *Buckley v Valeo* 1976 SCC OnLine US SC 16 : 46 L Ed 2d 659 : 421 US 1, 25 (1976) (applying strict scrutiny to political speech); *Central Hudson Gas & Electric Corpn v Public Service Commission* 1980 SCC OnLine US SC 139 : 65 L Ed 2d 341 : 447 US 557, 566 (1980) (applying intermediate scrutiny to commercial speech). It is unclear whether an app ban falls in the category of political speech, or of commercial speech, and courts have not conducted adequate analysis on this. See, eg, *TikTok v Trump* (n 9) 26, where the court assesses a ban on WeChat in terms of strict scrutiny.

[143] *WeChat v Trump* (n 9) 28.

[144] ibid.

[145] Note also that courts are deferential to the government's definition of risks, especially in issues about national security. Effectively, the government's narrative in defining the risk might be taken at *prima facie* value. For example, in *Holder v Humanitarian Law Project* 2010 SCC OnLine US SC 75 : 561 US 1, 33-34 (2010) the Court deferred to the government's claims about risks arising from providing designated terrorist organizations legal support, stating that "evaluation of the facts by the Executive, like Congress's assessment, is entitled to deference." See also *Ziglar v Abbasi*, 137 S Ct 1843 : 582 US ___ (2017) where the court noted that the separation of powers prevented the Court from questioning the Executive's decisions in the realm of national security. The Court ruled similarly in *Hernandez v Mesa* 206 L Ed 2d 29 : 140 S Ct 735 589 US_(2020), 740-42 regarding the Executive's role in international law.

[146] See s II.

not been extensively litigated in the courts, it remains to be seen whether the government could curtail speech in favour of national security.

If the first prong is fulfilled, it is likely that the second prong—significant governmental interest unrelated to the content of the speech—will also be fulfilled. This is because the risks being cited in Section II have to do with national security, election integrity, and the like, which are unrelated to the content of the speech, and directly related to the existence of the app.

The third prong—adequate alternate channels of communication—plays a subtler role. In *WeChat*, the plaintiffs alleged that their app—which is the primary app for Chinese-speaking and Chinese-American users—had no "viable substitute platforms."[147] In WeChat's case, this is true: no other Chinese language communications app has as broad a user base, nor serves as many functions, as WeChat does.[148] However, TikTok, as an app, is less unique and more substitutable, and in pending litigation, courts have not assessed whether banning TikTok would leave open no alternative means of communication.[149]

The specific factors that courts use to define "substitutability" in the context of digital technologies are unclear.[150] Apps and technology companies advertise their uniqueness, and depending on the level of granularity, apps and platforms can look distinct or homogenous. Facebook, Twitter, TikTok,

---

[147] *WeChat v Trump* (n 9) 27.

[148] See, eg, 'Number of monthly active WeChat users from 2nd quarter 2011 to 3rd quarter 2020' (*Statista*, 1 December 2020) <https://www.statista.com/statistics/255778/number-of-active-wechat-messenger-accounts/https://www.statista.com/statistics/255778/number-of-active-wechat-messenger-accounts> accessed 31 December 2020.

[149] *Marland v Trump* (n 55) 24.

[150] Antitrust law, which provides criteria for which products are substitutable, is unhelpful. In *Brown Shoe Co v United States* 1962 SCC OnLine US SC 114 : 8 L Ed 2d 510 : 370 US 294, 325 (1962), the Supreme Court focused on seven factors, most of which are price-related: (1) industry or public recognition of separate markets; (2) a product's peculiar characteristics and uses; (3) unique production facilities; (4) distinct customers; (5) distinct prices; (6) sensitivity to price changes; and (7) specialized vendors. Unfortunately, in the case of apps which are free, only factors (2) and (4) are relevant here, and indicate that WeChat may not be substitutable. But courts have yet to address substitutability in the context of social media and app-based technology, so looking at antitrust law may not provide adequate guidance, especially given the balancing test-nature of antitrust regulation in this area. See, eg, Wilson C Freeman & Jay B Sykes, Cong RschServ, R45910, Antitrust and "Big Tech" 25-32 (2019) <https://fas.org/sgp/crs/misc/R45910.pdf> accessed 16 August 2021. It becomes even more unclear because where a market is two-sided (e.g. video streaming, where one side is the viewer and the other the producer), the two sides may disagree about whether alternative platforms are substitutable. Erik Hovenkamp, Platform Antitrust [2019] 44 J Corp L 713, 730. Here, it is unclear whether WeChat is part of a two-sided market, but it could be: on one side are users who have access to a free internet ecosystem (American users); and on the other side are users whose only choice of communication with those abroad is WeChat (Chinese users).

Instagram, and Snapchat are all social media platforms. However, the specific features of Instagram—including the ability to send videos and disappearing pictures—make it a feasible substitute for Snapchat. Instagram and Snapchat's video-sharing features may also make them substitutes for TikTok. Yet TikTok's user base and content discovery functions (such as search features and algorithms that power its feed) are different from those offered on Instagram and Snapchat. Which features are considered and how broadly or narrowly a platform's purpose or functionality is defined will impact whether the platform is considered substitutable. Additionally, the size and demographic of the user base may also play a role. If American WeChat users are forced to migrate to another communication app like WhatsApp or Signal, but users in China are unable to use such apps, or those receiving messages are not on the new apps, then the new apps may not be perfect substitutes for the banned app. To sum: even if the ban is narrow and related to a governmental interest, it may not satisfy heightened scrutiny if the ban also does not provide an alternate channel of communication.

Beyond the tests applied to courts, there are other impacts to speech that are concerning. First, temporary injunctions that oscillate based on courts' decisions may have a chilling effect on speech on these platforms. Users may fear that such platforms may not be around for long, causing migration to other platforms, fragmentation of user bases, or cessation of usage altogether. Especially on platforms like TikTok, where users have monetized their presence, uncertainty may reduce the attractiveness of the public forum.[151] If a user's primary viewership, network, or identity is built around one platform, users may be disincentivized from developing content on these platforms if the government can ban, threaten, or slow these apps down in courts. Second, the government could use data privacy, data access, disinformation, and national security as pretexts for banning or curtailing the usage of an app. Indirectly, this might be content-neutral, which lowers scrutiny.[152] However, by targeting specific types of apps—for example, primarily Chinese-speaking (WeChat); primarily used by younger users (TikTok); or those that focus on a specific demographic or theme—the government might be intentionally or unintentionally curtailing content-specific speech.

---

[151] See, eg, Louise Matsakis, 'TikTok is Paying Creators. Not All of Them are Happy' (*WIRED*, 10 September (Sept 10, 2020), <https://www.wired.com/story/tiktok-creators-fund-revenue-sharing-complaints/> accessed 19 April 2021. *Cf* Taylor Lorenz, 'What if the U.S. Bans TikTok' *The New York Times* (10 July 2020), <https://www.nytimes.com/2020/07/10/style/tiktok-ban-us-users-influencers-taylor-lorenz.html> accessed 19 April 2021 (noting that users are feeling "anxiety," including for users whom "TikTok is their livelihood.").

[152] See, eg, *Reed v Town of Gilbert* 192 L Ed 2d 236 : 576 US 155, 166 (2015) (noting that content neutral laws are subject to a "lower level of scrutiny").

Again, the risks articulated above could be pretextual and could help frame a technology ban as a time/place/manner restriction, rather than one that aims at specific types of speech, lowering the type of scrutiny courts apply.

Ultimately, courts are yet to determine the factors considered in the First Amendment context when looking at app bans. But even the threat of such bans may come at the price of uncertainty and chilled speech, especially if users switch away from these platforms in the face of threats to ban communication tools.

B. Undermining Internet Freedom, Human Rights, and American Foreign Policy

American efforts to ban Chinese technologies play into the Chinese "cyber sovereignty norms" that support China's territorial vision of the internet, where each government plays a central role in shaping the governance of the internet within national boundaries. Instead of is opposed to allowing private actors to manage the flow of data and the ability of information.[153] Although China does not actively export "digital authoritarianism," other governments can gravitate towards these tools through emulation.[154] For the US—a government that has taken a hands-off approach to internet regulation—emulating China's approach of asserting a strong role for government officials to ban communications tools flies in the face of long-standing norms and protections. One of the main issues is that the US is not just blocking foreign technology agnostic to its origins; rather, it is specifically excluding *Chinese* technology as tensions between the two countries escalate.

In fact, given the nebulous, broad, and unclear risks defined in Section II, these technology bans may also have a more compelling, non-legal justification: great power politics intended to compete with growing Chinese cyber power, resulting in a homegrown digital wall that emulates Chinese strategy. The US has concerns about national security regarding China's ability to gain intelligence benefits from controlling the exchange of global technology.[155] In the US, for instance, the government benefits from the dominance of American technology firms and the government's ability to demand data

---

[153] Rogier Creemers, 'China's Conception of Cyber Sovereignty : Rhetoric and Realization' in Dennis Broeders and Bibi van den Berg (eds), *Governing Cyberspace: Behavior, Power and Diplomacy* (2020) 107.

[154] Matthew S Erie and Thomas Streinz, 'The Beijing Effect: China's' Digital Silk Road' as Transnational Data Governance' (2021) New York University J Intl L & Politics (JILP), Forthcoming.

[155] Farrell & Newman (n 50).

from firms for domestic and national security purposes.[156] The strategic vantage point that the US perceives China to be gaining is instilling fear that China will gain an upper hand to bargain with. This threat is heightened when foreign technology is used by US military or government officials, raising fears of blackmail and extortion.

Despite these concerns, US efforts to impose bans on communication technology may lead to more serious long-term consequences. These efforts play into Chinese "cyber sovereignty norms" that support China's vision of the internet, which promotes an alternative vision to the US Internet Freedom policy.[157] Since the dawn of the internet, dictators have viewed the internet as a potential threat to power. The Arab Spring served as a painful reminder for many leaders that communications tools could be used by organized opposition against the regime. China argues that governments should be able to control the internet, acceding to the demands of national security. But with these technology bans, the US has borrowed from China's toolkit in order to address security and sovereignty concerns by blocking access to a communications platform. Combined with other Western countries' shift to a more reasonable regulatory regime that penalizes technology companies (both foreign and domestic) for competitive and online harms,[158] the US's heavy-handed regulatory approach of banning technologies does much to normalize China's approach to internet governance.

These efforts have serious global consequences. First, American actions matter as cybersecurity norms continue to develop and the US and China compete to establish norms for internet governance.[159] China's vision is one that strongly supports state sovereignty and territorial control over information flows.[160] The US government, on the other hand, supports a vision of a "borderless"[161] internet, where limited government interventions support

---

[156] Alan Z. Rozenshtein, 'Surveillance Intermediaries' (2018) 70 Stanford L Rev 99. Of course, these demands are made through the courts and with sufficient legal protections for those subject to the surveillance.

[157] Creemers (n 153).

[158] See, eg, Australia's negotiations with Facebook about paying news outlets for hosting their links on the Facebook platform. Jason Scott and Vlad Savov, 'Australian Law Could Force Facebook, Google to Strip Content' (*Bloomberg*, June 22, 2021) <https://www.bloomberg.com/news/articles/2021-06-23/australia-s-online-safety-bill-forces-platforms-to-strip-content> accessed 16 August 2021.

[159] Laura De Nardis, *The Global War for Internet Governance* (Yale University Press 2014).

[160] Cai Cuihong, 'China and Global Cyber Governance: Main Principles and Debates' [2018] 42 Asian Perspective 647; Creemers (n 157).

[161] 'Senior State Department Official on State Department 2019 Successes on Cybersecurity and 5G Issues' (*United States Department of State*, 9 January 2020) <https://2017-2021.state.gov/senior-state-department-official-on-state-department-2019-successes-on-cybersecurity-and-5g-issues/> accessed 25 April 2021.

and uphold global free speech protections. These differences are reflected in preferences for the application of existing human rights law as well as whether internet governance should be located in multistakeholder institutions (preferred by the US) versus multilateral institutions (preferred by China). Processes within the UN, supported by the US, aim to develop norms for cybersecurity and establish a common understanding.[162] US efforts to ban communications tools normalize the "cyber sovereignty" policy and could undermine US efforts at the UN to codify internet freedom norms into international agreements and processes.

Second, for a government that has promoted the free flow of information, US attempts to block communications tools create permissive space for other governments to implement similar bans. Goldsmith describes the failure of the internet freedom foreign policy as animating from the hypocrisy of US strategies.[163] One arm of the diplomatic core promotes free speech values and the right to access content, whereas more recent policies have undercut the message by blocking Chinese communication tools. Despite being a nation that strongly privileges free speech at home and abroad, these current American efforts diminish the reach of original foreign policies designed to limit digital walls and preserve a zone of openness and information exchange.

Because of the hypocritical policy that fuels justification for the Chinese approach to dealing with cybersecurity threats, other democratic governments may follow suit and adopt bans of their own to mirror US policy. This hypothesis is supported by theories of legal diffusion, which suggest that policy decisions are not made independently. As governments adopt particular legislation, their counterparts take note.[164] Emulation occurs when governments adopt policies in a "follow the leader" approach, with policymakers considering laws from the largest or richest countries as standards that should be emulated.[165] An example of this is India's policy concerning Chinese apps. After a border clash with China, India retaliated by preventing

---

[162] Martha Finnemore and Duncan B Hollis, 'Constructing Norms for Global Cybersecurity' [2016] 110 American J Intl L 425.

[163] Goldsmith & Wu (n 17).

[164] Beth A Simmons & Zachary Elkins, 'The Globalization of Liberalization: Policy Diffusion in the International Political Economy' [2004] 98 American Political Science Rev 171–189; Frank Dobbin, Beth A Simmons & Geoffrey Garrett, 'The Global Diffusion of Public Policies: Social Construction, Coercion, Competition, or Learning?' [2007] 33 Annual Review of Sociology 449–472; Beth A Simmons, Frank Dobbin & Geoffrey Garrett, 'Introduction: The International Diffusion of Liberalism' [2006] 60 Intl Org, <http://www.journals.cambridge.org/abstract_S0020818306060267> accessed 19 April 2021; Zachary Elkins, Andrew T Guzman & Beth A Simmons, 'Competing for Capital: The Diffusion of Bilateral Investment Treaties, 1960–2000' [2006] 60 Intl Org 811.

[165] Dobbin, Simmons, and Garrett, ibid 452.

an estimated 200 million users from accessing TikTok.[166] Other governments are also beginning to probe into the practices of TikTok: leaders from Japan's Liberal Democratic Ruling Party launched efforts to restrict access to TikTok and other Chinese-owned apps to protect personal information.[167]

The US vision has long been one of the dominant approaches to internet governance. As the architect of the internet, the US was able to instil preferences into many international institutions and forums.[168] Internet Freedom is also reflected in some multilateral decisions. Seeking to advance Article 19 protections of the Universal Declaration of Human Rights that guarantees that everyone enjoys the right to "to seek, receive and impart information and ideas through any media and regardless of frontiers," the UN Human Rights Council and General Assembly agreed that offline rights apply online.[169] Other victories include the Internet Freedom Coalition. In 2011, fourteen countries endorsed a declaration protecting human rights and fundamental freedoms online.[170] More recently, President Biden organized a partnership of "techno-democracies"[171] designed to prevent China from "setting the rules and shaping the norms that govern the use of technology."[172] However, these efforts are undermined by US domestic responses—including ones that are no longer in effect, like President Trump's technology bans[173]—that implicitly support a "cyber sovereignty" approach and devi-

---

[166] Raymond Zhong & Kai Schultz, 'With India's TikTok Ban, the World's Digital Walls Grow Higher' *The New York Times* (30 June 2020) <https://www.nytimes.com/2020/06/30/technology/india-china-tiktok.html> accessed 19 April 2021. We note that this happened around the same time that the Trump Administration banned TikTok, though who thought of the idea first is unclear. Even so, the US policy affirms and justifies the Indian policy.

[167] Jennifer Hassan & Ruby Mellen, 'It's not just the United States: These Governments also see TikTok as a Problem.' *The Washington Post* (18 September 2020) <https://www.washingtonpost.com/world/2020/08/03/its-not-just-united-states-these-governments-see-tiktok-growing-problem/> accessed 19 April 2021.

[168] Kal Raustiala, 'Governing the Internet' [2016] 110 American J Intl L 491 (specifically referring to US dominance over ICANN, the organization that handles the assignment of domain names).

[169] n 3. See also David Kaye, 'The Limits of Supply-Side Internet Freedom' (*Knight First Amendment Institute,* 2018) <https://knightcolumbia.org/content/limits-supply-side-internet-freedom> accessed 29 March 2021.

[170] 'Launch of Internet Freedom Coalition at "Freedom Online" Conference' (*U.S. Department of State*, 13 December 2011) <//2009-2017.state.gov/r/pa/prs/ps/2011/12/178667.htm> accessed 29 March 2021.

[171] Jared Cohen & Richard Fontaine, 'Uniting the Techno-Democracies' (*Foreign Affairs*) <https://www.foreignaffairs.com/articles/united-states/2020-10-13/uniting-techno-democracies> accessed 18 March 2021.

[172] David Ignatius, 'Opinion | Biden's Ambitious Plan to Push Back against Techno-Autocracies' *The Washington Post* (11 February 2021) <https://www.washingtonpost.com/opinions/bidens-ambitious-plan-to-push-back-against-techno-autocracies/2021/02/11/2f2a358e-6cb6-11eb-9ead-673168d5b874_story.html> accessed 18 March 2021.

[173] Among the myriad reasons that even an obsolete and undone policy undermines the overall Internet Freedom message are the potential transitory nature of US foreign policy, which

ate from long-standing efforts designed to instead design international collaboration to support free expression.

C. Data Storage and Localization

Another major issue within the Internet Freedom and cyber sovereignty debate is the concept of data localization. Data localization undermines the notion of an open internet through technical means, by requiring that companies store particular types of information within national borders.[174] The US government has sought to prevent the diffusion of data localization policies, even codifying clauses that prohibit data localization within major trade agreements.[175]

Continued scrutiny about foreign access to US user data, exacerbated by technology bans, may motivate companies to store user data in the US. A major concern driving these US government technology bans is the ability of hostile foreign governments like China to access US user data.[176] However, companies claim that their data is not stored in China, but elsewhere; in TikTok's case, the company claims its data is stored on servers in the US and Singapore.[177]

But given the borderless nature of the internet, significant issues arise. First, it is unclear whether foreign nations or governments are prohibited from accessing data if that data is stored in the US. In TikTok's case, even though it claimed that its data was stored in the US and Singapore, the company noted that its information could still be shared with its China-based

---

subsequent Presidents can easily change without significant Congressional approval; the signals sent to anti-democratic countries that create a permission structure for technology bans to take place; the uncertain investment atmosphere that may dissuade foreign companies from bringing their technology to the US; and the difficulty of undoing technology bans that have already gone into effect, like those in India.

[174] Anupam Chander & Uyên P Lê, 'Breaking the Web: Data Localization vs. the Global Internet' (2014) Emory L J, Forthcoming; Anupam Chander & Uyên P Lê, 'Data Nationalism' (2014) 64 Emory L J 677.

[175] Michael Giest, 'Data Rules in Modern Trade Agreements: Toward Reconciling an Open Internet with Privacy and Security Safeguards' (*Centre for International Governance Innovation,* 2018) <https://www.cigionline.org/articles/data-rules-modern-trade-agreements-toward-reconciling-open-internet-privacy-and-security> accessed 23 April 2021; Agam Shah & Jared Council, 'USMCA Formalizes Free Flow of Data, Other Tech Issues' *The Wall Street Journal* (29 January 2020) <https://www.wsj.com/articles/cios-businesses-to-benefit-from-new-trade-deal-11580340128> accessed 23 April 2021.

[176] See s II.A.

[177] Robert McMillian, Liza Lin & Shan Li, 'TikTok User Data: What Does the App Collect and Why are U.S. Authorities Concerned?' *The Wall Street Journal* (7 July 2020) <https://www.wsj.com/articles/tiktok-user-data-what-does-the-app-collect-and-why-are-u-s-authorities-concerned-11594157084> accessed 19 April 2021.

parent company, ByteDance, and other affiliates.[178] Second, logistical issues arise for users who travel: is data stored in the US based on whether the user is in the US, whether the server is in the US, or whether the user is a US person? Additionally, when a non-US person communicates with a US person, whose location controls where the data is stored?

Effectively, how the law defines "US person" may define how much data is stored in the US. If a "US person" includes not just citizens and those located in the US, but anyone using a US-based server, such a definition will be overinclusive, capturing more than just people physically located in the US. Further, a broad definition of a US person or storage of more than just US users' data in the US may lead to reciprocity by foreign states: other states may incentivize companies to store data pertaining to domestic users locally, and may do so in an over inclusive manner. This would harm the privacy of US users by allowing their data to be stored in other countries and be accessed by foreign governments without due process, and harm the privacy of foreign users by encouraging their home governments to store data locally, making it easy for them to access such data. Of course, this assumes that US users' data stored at home is more private than data stored abroad. In some cases—especially where "abroad" includes authoritarian countries or those with invasive governments, like China—this is evident. In other cases, this claim is subjective. However, having US users' data stored in the US provides more easily accessible courts where privacy concerns can be litigated and allow consumers to deal with a government that is at worst translucent,[179] but whose practices are familiar.[180]

The costs of such implications go beyond financial (including aggregation and efficiency losses) and logistical considerations. If data of non-US users is stored abroad, that may have a roundabout impact on national security, leaving data not stored on cloud servers, but on local servers, more difficult to reach by warrants like those considered in *United States v Microsoft*

---

[178] ibid.

[179] For example, the US's Freedom of Information Act requests provide Americans with the ability to access what kind of information the government collects about them. See 5 USC § 552.

[180] Another example of a familiar and somewhat transparent process is the stringent process required for the government to get a warrant to wiretap (including the monitoring of electronic communications) a suspect. The government must provide a variety of information, including the identity of the officer making the application, detailed reasoning for why the wiretap is required, a limited period of time for when the wiretap can be implemented, and must ensure that the minimum amount of information is intercepted. See generally 18 USC § 2518. Of course, the government's mass national security surveillance programs after the Snowden program have shown the possibility that at least metadata is collected without due process. But generally speaking, where detailed information beyond metadata is collected, the process requirements indicate that some modicum of privacy may be preserved.

Corp.[181] Additionally, data localization may facilitate the ability of foreign governments to surveil their own citizens, by creating one local honeypot where data can be found, rather than creating jurisdictional hurdles. There may also be enhanced scrutiny of US data standards and surveillance practices if the definition of US users is overbroad and includes non-US persons, and could have reciprocity impacts. Finally, while some US trade agreements ban data localization (such as the US-Mexico-Canada Agreement), actions against companies that access US user data where data localization is not in place may effectively create de facto data localization by incentivizing companies to store their data locally for fear of punishment, without explicitly saying so legally.[182]

The issue of data localization is one that courts and policymakers have yet to completely comprehend. However, current technology embargoes and actions may bring about the need to tackle this issue head-on or risk creating the perverse incentives and side-effects of a de facto data localization law.

V. Conclusion

The saga of the TikTok ban and the Trump Administration are both in the past, even if temporarily. But while the administration was fleeting, the American strategy of banning foreign technologies, especially in light of the tense US-China relationship, may be unlikely to disappear. The threats that the US government presented to justify these bans—Chinese access to American consumer data, Chinese censorship, and Chinese election interference and disinformation campaigns—are vague and ill-defined. But the threat of Chinese disruption to the US government's functionality is evident in light of the current cybersecurity and threat context. Despite this significant and well-articulated risk, the strategic costs of such bans, the impacts on speech and international relations, and the cost of precedent do not justify using the hammer of bans on foreign technology bans on problems that do not look like nails. And the lack of transparency in what these threats entail and how the decision-making process played out procedurally raise questions about the necessity and benefit of such bans.

We note that this article is a brief glimpse into the complex, arcane logic and the corresponding balancing act of foreign technology bans in the US.

---

[181] 2018 SCC OnLine US SC 72 : 138 S Ct 1186 : 584 US ___ (2018).

[182] See, eg, Michael Geist, 'How the USMCA falls Short on Digital Trade, Data Protection, and Privacy' *The Washington Post* (3 October 2018) <https://www.washingtonpost.com/news/global-opinions/wp/2018/10/03/how-the-usmca-falls-short-on-digital-trade-data-protection-and-privacy/> accessed 19 April 2021.

More work is required to create a holistic picture that incorporates not just the speech and international relations implications of such bans, but also the heavy costs to the data economy and the intelligence sector. Given the Indian government's ban on Chinese apps, future work could discuss the Indian government's even blunter approach to technology bans, which have been successfully implemented and have not been invalidated in courts. Notably, unlike the US, the Indian government does not have the shackles of an Internet Freedom policy to be beholden to. And the constraints and protections of the First Amendment do not apply in Indian law. These different circumstances, in combination with China's proximity and nearby military threat, may create a different set of costs and benefits. Additionally, the US's past technology bans could justify technology bans in other democracies, like in India.

Clearly, the Indian context is different, since the bans have been implemented. This raises a whole host of curious questions. Given these bans, what kinds of speech, if any, have been stifled? Have other countries, including China, retaliated by banning Indian technology? What kinds of justifications are considered legitimate in the Indian context, and do they mirror those used in the American context? These questions were beyond this paper's scope, but answering them might help create a more complete framework for categorizing threats, understanding their magnitude, assessing their validity, and highlighting how such bans are perceived by other countries that are also threatened by Chinese cybersecurity prowess.

Ultimately, however, from an American policy and legal perspective, the consequences of these bans are far-fetched and damaging. That the Biden Administration has not pursued them further provides us with some time to assess the harms, and pursue more targeted policies that do not affect speech, encourage censorship, and undermine Internet Freedom.

Encryption in India: Preserving the Online Engine of Privacy, Free Expression, Security, and Economic Growth

Greg Nojeim & Namrata Maheshwari***

Abstract *This article argues that the traceability mandate imposed in India by the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 undermines encryption and negatively impacts cybersecurity as well as the fundamental right to privacy. In doing so, it explains how the traceability requirement fails the necessity and proportionality test laid down by the Indian Supreme Court in the Puttaswamy judgment, wherein it held that the right to privacy is a fundamental right under the Constitution of India. Further, the article makes a case for why encryption is important for protecting privacy, free expression, and other human rights, and also for bulwarking the economy, preserving democracy, and ensuring national security.*

Part I of the article provides a background on how encryption works and the purpose it serves in the digital era. Part II analyzes the trajectory of encryption policy in India and the relevant legal frameworks. Thereafter, Part III explains the traceability mandate under the New Intermediary Guidelines and its effect on encryption, and consequently, the impact on cybersecurity and the right to privacy. It assesses whether it meets the requirement of necessity and proportionality as set out by the Supreme Court. Finally, Part IV explains that encryption should be protected and encouraged because it guards against unwarranted surveillance and preserves privacy and expression,

* Greg Nojeim is a Senior Counsel and Co-Director of the Security and Surveillance Project at the Center for Democracy & Technology, an NGO with offices in Washington, D.C. and Brussels.

** Namrata Maheshwari is Asia Pacific Policy Counsel at Access Now, an international non-profit organisation, and former Consultant with the Center for Democracy and Technology. She is an India qualified lawyer.

The authors would like to thank Ankit Kapoor, BA.LLB (Hons.) student at NLSIU, for his assistance with the preliminary research for this article.

is a crucial tool to protect human rights in the digital age, strengthens national security, and benefits the economy.

Introduction

One of the strongest statements in favour of privacy against government intrusion was made by the former Prime Minister of the United Kingdom, William Pitt, in 1763: 'The poorest man may in his cottage, bid defiance to all the forces of the Crown. It may be frail, its roof may shake; the wind may blow through it; the storm may enter; the rain may enter, but the King of England may not enter; all his force dares not cross the threshold of the ruined tenement.'[1] Centuries later, while the protection of privacy against government surveillance remains a work in progress, encryption serves as a veritable gatekeeper of the online sphere that houses the most sensitive and private information of individuals, communities, corporations, and the state alike.

Despite the positive impact of encryption on privacy, security, and the economy, the Indian government proposes to weaken encryption and imperil users' rights while jeopardising the security of data online.[2] This article aims to contribute to the encryption debate in India, and globally, by showing that proposals that have the effect of weakening encryption and communications security should be rejected because they will not achieve the desired objectives and would instead severely hamper privacy, free expression, and cybersecurity, and cause significant damage to the economy.

---

[1] William Pitt, Speech on the Excise Bill (1763) (quoted in *Miller v United States* 1958 SCC OnLine US SC 131 : 2 L Ed 2d 1332 : 357 US 301, 307 (1958)).

[2] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

Section I of this article provides background information about encryption. Section II elucidates the trajectory of encryption policy in India by providing an overview of the important developments pertaining to encryption over the last three decades. Section III analyses changes to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, which impose a requirement that communications carried on certain messaging services be traceable to their source. It shows that a traceability mandate would weaken encryption, fail to accomplish the goal of stopping the spread of fake news, and would not meet the requirements of the proportionality test the Supreme Court recently established when it held that the right to privacy is a fundamental right under the Indian Constitution. Finally, Section IV preceding the conclusion makes a case for protecting and encouraging encryption because of its importance for privacy in the face of rampant surveillance, the necessity for upholding human rights, and a positive correlation with national security and economic growth.

I. Background on Encryption

In the digital era, the amount of sensitive data stored electronically grows, and will continue to grow exponentially.[3] Medical and biometric records, bank account details, private communications, and location information are only a few of the many examples of such data that is now more easily accessible than ever before.[4] The concomitant effects of this trajectory are serious concerns pertaining to privacy[5] and online security.[6] The COVID-19 pandemic has created new demands for digital data, both by forcing many schools and workplaces into remote settings and by fostering technologies to fight the disease. This in turn has aggravated associated privacy concerns[7]

---

[3] Thomas Alsop, 'Data Storage - Statistics & Facts' (*Statista*, 23 June 2020) <https://www.statista.com/topics/3150/data-storage/#dossierSummary__chapter1> accessed 12 November 2020.

[4] Eva-Maria Schomakersa, Chantal Lidyni
, Dirk Müllmannb & Martina Zieflea, 'Internet Users' Perceptions of Information Sensitivity – Insights from Germany' (2019) 46 Intl J Info Management 142, 143-148.

[5] ibid.

[6] Terrence Berg, 'The Changing Face of Cybercrime', (2007) 86 Michigan Bar J 18.

[7] Elizabeth Beattie, 'We're Watching You: COVID-19 Surveillance Raises Privacy Fears' (*Al Jazerra*, 3 April 2020) <https://www.aljazeera.com/news/2020/4/3/were-watching-you-covid-19-surveillance-raises-privacy-fears> accessed 2 November 2020; For updates on global responses to the covid-19 pandemic that raise privacy related concerns, *see*: 'Tracking the Global Response to COVID-19' (*Privacy International*) <https://privacyinternational.org/examples/tracking-global-response-covid-19> accessed 12 November 2020, and Andrej Zwitter & Oskar J. Gstrein, 'Big Data, Privacy and COVID-19 – Learning from Humanitarian Expertise in Data Protection' (2020) 5 J Intl Humanitarian Action <https://jhumanitarianaction.springeropen.com/articles/10.1186/s41018-020-00072-6> accessed 12 November 2020.

and enhanced the importance of tools such as encryption to secure data and protect individuals, governments, and the economy.

Encryption preserves data privacy and security. It is the method in cryptography[8] by which information is 'locked' and rendered unintelligible to an unauthorized recipient, and the authorized recipient possesses a 'key'[9] that decrypts the message and converts it into plain text.[10] In other words, encryption scrambles readable text or files in a way that only the sender and the intended recipient can comprehend the content. It protects data from unauthorized access and preserves the authenticity and privacy of information online, and protects users in a range of ways. As Philipp Rogaway puts it, 'cryptography rearranges power: it configures who can do what, from what.'[11] By ensuring that users retain autonomy over who accesses their data, encryption re-balances the power of users with the power of other parties that typically have more. Most banking applications and credit card payment terminals use encryption and it is broadly used across most communication platforms.[12]

Encryption protects both stored data and data in transit.[13] One of the most secure forms of encryption is end-to-end encryption ('**E2EE**'). E2EE

---

[8] *The American Heritage Dictionary of English Language* (4th edn, Houghton Mifflin Co. 2000) 439. Herein, cryptography is defined as '1. The process or skill of communicating in or deciphering secret writings or ciphers. 2. Secret writing.'

[9] An encryption key is a string of numbers. The longer the string, the stronger the encryption. Typically, when using encryption software, the user's password activates the key. There are two methods of employing such keys – symmetric encryption, also known as private key encryption; and asymmetric encryption, also known as public key encryption. Private key encryption entails the use of the same key to encrypt and decrypt content. Whereas public key encryption requires a public key, known to the public, to encrypt and a private key, known only to the individual using encryption, to decrypt. It is considered virtually impossible to break strong public key encryption without acquiring the private key. Branden M. Palfreyman, 'Lessons from the British and American Approaches to Compelled Decryption' (2007) 75(1) Brooklyn L Rev 345, 350-352; Lawrence Lessig, *Code and Other Laws of Cyberspace* (Basic Books 1999) 36; 'A Deep Dive on End-to-End Encryption: How Do Public Key Encryption Systems Work?' (*Surveillance Self-Defense*, 29 November 2018) <https://ssd.eff.org/en/module/deep-dive-end-end-encryption-how-do-public-key-encryption-systems-work> accessed 12 November 2020.

[10] Gulshan Rai, RK Dubash, & AK Chakravarty, 'Cryptography Technology and Policy Directions in the Context of NII' (1997) Information Technology Group, Department of Electronics Cyberlaw Series 3, Version 1 <https://web.archive.org/web/19990506205823/http:/www.allindia.com:80/gov/doe/cryplaw.htm> accessed 12 November 2020.

[11] Philipp Rogaway. 'The Moral Character of Cryptographic Work' (Asiacrypt, Auckland, December 2015).

[12] James Titcomb, 'What is Encryption, How Does It Work and What Apps Use It?' (*The Telegraph*, 29 March 2017) <https://www.telegraph.co.uk/technology/0/encryption-should-using/> accessed 12 November 2020.

[13] Nate Lord, 'Data Protection: Data In Transit vs. Data At Rest' (*Digital Guardian*, 15 July 2019) <https://digitalguardian.com/blog/data-protection-data-in-transit-vs-data-at-rest>

ensures that no one other than the sender and the intended recipient, including intermediaries such as the communication service provider itself, can view the information exchanged.[14]

Indian law defines encryption as '[t]he process of transforming plain text data into an unintelligible form (cypher text) such that the original data either cannot be recovered (one-way encryption) or cannot be recovered without using an inverse decryption process (two-way encryption).'[15]

India does not currently have legislation dedicated to encryption. It is governed largely by sectoral regulations and the Information Technology Act, 2000[16] ('**IT Act**'). The last few decades have witnessed the evolution of the Indian government's approach to encryption with some recent developments reflecting the government's perception of encryption as an obstacle for government agencies.[17]

II. The Trajectory of Encryption Policy in India

Technology policy on matters pertaining to encryption began taking shape in India in the 1990s.[18] The growth of digital banking, electronic commu-

---

accessed 12 November 2020.

[14] Saurabh Sharma, 'End-to-end Encryption: The Heart of Data Security in Today's Digital World' (*Live Mint*, 5 December 2019) <https://www.livemint.com/opinion/columns/end-to-end-encryption-the-heart-of-data-security-in-today-s-digital-world-11575560730299.html> accessed 12 November 2020.

[15] Information Technology (Certifying Authorities) Rules, 2000, sch V.

[16] Information Technology Act, 2000 ('IT Act').

[17] For instance, the traceability mandate under Rule 4(2) of the Information Technology (Intermediaries Guidelines and Digital Media Ethics Code) Rules, 2021; the report by the ad-hoc committee of the Rajya Sabha recommending that law enforcement agencies should be permitted to break end-to-end encryption to trace the distributor of child pornography on social media, *see*: Neha Alawadhi, 'RS Panel Suggests Breaking Encryption to Curb Child Pornography Distribution' (*Business Standard,* 27 January 2020) <https://www.business-standard.com/article/technology/rs-panel-suggests-breaking-encryption-to-curb-child-pornograhy-distribution-120012600705_1.html> accessed 20 July 2021; and statements by the former Minister of Electronics and Information Technology demanding that the origins of messages on end-to-end encrypted platforms should be traceable, *see*: 'Right to Privacy not for those Who Abuse Internet Platform: Ravi Shankar Prasad' (*The New Indian Express*, 14 October 2019) <https://www.newindianexpress.com/nation/2019/oct/14/right-to-privacy-not-for-those-who-abuse-internet-platform-ravi-shankar-prasad-2047531.html> accessed 17 July 2021.

[18] Bedavyasa Mohanty, 'The Encryption Debate in India' (2019) Carnegie Endowment for International Peace, 2 <https://carnegieendowment.org/files/WP_The_Encryption_Debate_in_India.pdf> accessed 12 November 2020. The Indian Telegraph Act, 1885, and the rules thereunder, on the governance of communications are applicable in the context of encryption, even though they were not specifically framed in that regard. For an overview of laws relating to encryption in India, *see*: 'The Road Ahead for Encryption in India' (2020) NASSCOM-DSCI, 29-36 <https://community.nasscom.in/communities/

nication, online intermediaries, and e-commerce led the Indian government to enact the IT Act. The IT Act established a regulatory framework governing the virtual marketplace[19] and introduced a range of e-commerce and internet-related criminal offences.[20] The Act endorsed the use of Public Key Infrastructure (PKI), a system of encryption used for cybersecurity, for secure exchange of data and money.[21] However, as recognized by the Reserve Bank of India (RBI) while issuing guidelines for internet banking,[22] PKI and other sophisticated encryption tools were not commonly available in India then.[23] As a result, the RBI recommended 128-bit Secure Socket Layer (SSL) encryption as an alternative to PKI and to ensure security in online banking, and the Securities Exchange Board of India recommended this standard as the default for e-commerce.[24]

However, subsequently, encryption policy took a turn that reflected governmental concern that encryption will preclude government access to data. The regulatory framework on encryption is now set out simultaneously in the IT Act, the Indian Telegraph Act, 1885[25] ('**Telegraph Act**') as well as sector-specific regulations.[26] These provisions are aimed at specifying the standard of encryption that may be used, permitting decryption by governmental

---

policy-advocacy/nasscom-dsci-discussion-paper-the-road-ahead-for-encryption-in-india.html> accessed 12 November 2020.

19 Khaitan & Co., 'Digital Business in India: Overview' (*Thomson Reuters Practical Law*, 1 February 2017) <https://content.next.westlaw.com/Document/I910e2c5a3b8d11e598dc8b09b4f043e0/View/FullText.html?transitionType=Default&contextData=(sc.Default)&firstPage=true> accessed 12 November 2020.

20 Subhajit Basu and Richard Jones, 'Indian Information and Technology Act 2000: Review of the Regulatory Powers under the Act' (2005) 19(2) Intl Rev L Comp & Tech, 209, 219.

21 IT Act 2000, s 3.

22 'Internet Banking Guidelines' (*Reserve Bank of India*, 14 June 2001) <https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=414&Mode=0> accessed 12 November 2020.

23 The lack of domestic capacity in respect of cryptographic software in India in the 1990s could largely be attributed to export controls, *see*: Arun Mohan Sukumar, Wassenaar's Web: A Ahreat to Technology Transfer' (*The Hindu*, 29 March 2016) <https://www.thehindu.com/opinion/columns/wassenaars-web-a-threat-to-technology-transfer/article7499748.ece> accessed 12 November 2020.

24 Committee on Internet based Securities Trading and Services, *First Report* (SEBI 2000) 6-7.

25 The Indian Telegraph Act, 1885 is the primary legislation governing communication in India. It gives the Central Government the exclusive privilege of 'establishing, maintaining and working telegraphs'. Under s 3(1-AA), 'telegraph' is defined as 'any appliance, instrument, material or apparatus used or capable of use for transmission or reception of signs, signals, writing, images and sounds or intelligence of any nature by wire, visual or other electro-magnetic emissions, Radio waves or Hertzian waves, galvanic, electric or magnetic means'.

26 For instance, the Department of Telecommunications prohibits the use of bulk encryption, *see*: License Agreement for Unified License Agreement, para 37.1.

agencies, and compelling assistance with decryption so the government can gain access.[27]

The IT Act was amended with effect from 2009 to allow the central government to prescribe the modes or methods for encryption for e-governance and e-commerce.[28] Another amendment authorized the central and state governments to intercept, monitor, or decrypt communications in the interest of national security, sovereignty, defence and for the preservation of public order or investigation of an offence.[29] Service providers and subscribers are obligated to assist government agencies with accessing data in this manner.[30]

In the same year, the government enacted the Information Technology (Procedure and Safeguards for Interception, Monitoring, and Decryption of Information) Rules ('**Decryption Rules**').[31] The Decryption Rules set out the parameters and procedures for decryption. End-to-end encrypted platforms are arguably outside the scope of these rules since 'decryption assistance' is defined as assistance to 'allow access, *to the extent possible*, to encrypted information.'[32] The Decryption Rules empower the government[33] to issue an order for decryption for 'any informationas is sent to or from any person or

---

[27] [1] Pranesh Prakash & Japreet Grewal, 'How India Regulates Encryption' (*Center for Internet & Society*, 30 October 2015) <https://cis-india.org/internet-governance/blog/how-india-regulates-encryption> accessed 12 November 2020.

[28] Information Technology Act, 2000, s 84-A.

[29] Information Technology Act, 2000, s 69. A petition challenging the validity of this section is currently pending before the Supreme Court of India, *see*: *Internet Freedom Foundation v Union of India* (WP(C) No 44 of 2019)(pending). Herein, the petitioners approached the Supreme Court invoking its writ jurisdiction, under Article 32 of the Constitution of India, challenging the constitutionality of s 69 of IT Act and the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009 ('The Decryption Rules') on the grounds that they violate the Right to Equality (art 14), the Right to Freedom of Expression (art 19(1)(a)), and the Right to Privacy (art 21).

[30] Information Technology Act, 2000, s 69.

[31] The Decryption Rules. However, A petition challenging the validity of these Rules is currently pending before the Supreme Court of India, *see: Internet Freedom Foundation v Union of India* (WP(C) No 44 of 2019) (pending). Herein, the petitioners approached the Supreme Court through its writ jurisdiction, under art 32 of the Constitution, challenging the constitutionality of s 69 of IT Act and the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009 ('The Decryption Rules') on the grounds that they violate the Right to Equality (art 14), the Right to Freedom of Expression (art 19(1)(a)), and the Right to Privacy (art 21).

[32] The Decryption Rules, rule 2(g)(i) (emphasis added).

[33] In December 2018, the Ministry of Home Affairs authorized ten security and intelligence agencies to intercept, monitor and decrypt any information in any computer resource in accordance with the IT Act. *see*: Ministry of Home Affairs, Order dated 20 December 2018 <http://egazette.nic.in/WriteReadData/2018/194066.pdf> accessed 18 November 2020, *see*: The Wire Staff, 'Home Ministry Allows 10 Central Agencies to Engage in Electronic Snooping' (*The Wire*, 21 December 2018) <https://thewire.in/government/home-ministry-allows-10-central-agencies-to-engage-in-electronic-interception> accessed 12 November 2020.

class of persons or relating to any particular subject.'[34] The provision, therefore, covers a wide breadth of information and paves the way for non-targeted or indiscriminate decryption orders. Further, the Decryption Rules require that records pertaining to decryption orders be destroyed within a prescribed period of six months[35] which significantly diminishes the scope for review of the government's exercise of such unilateral power. The government often invokes national security to justify decryption orders.[36]

The first time encryption was openly portrayed as antithetical to national security in India was against the backdrop of the 2008 terror attacks in Mumbai. The government had previously threatened to block Research In Motion (RIM) from the Indian market[37] since the government could not monitor content shared on RIM's BlackBerry devices.[38] The news that those involved in the terror attacks had used BlackBerry devices[39] further intensified the government's antagonistic stance against encryption.[40] After protracted negotiations, RIM agreed to locate BlackBerry servers in India and enabled the government to intercept data of individual users sent over its messaging service, but not corporate customers' data sent over the BlackBerry Enterprise Server systems.[41] The outcome reduced users' privacy resulting from the concern that encryption poses a threat to national security. It is worth noting that intelligence officials were of the view that existing surveillance mechanisms had in fact gleaned sufficient information regarding the

---

[34] The Decryption Rules, rule 9.

[35] The Decryption Rules, rule 23. This provision is often invoked to reject applications under the Right to Information, 2005, regarding the number of decryption orders issued by the government.

[36] The Decryption Rules were framed under s 69, IT Act, which authorizes the central and state governments to intercept, monitor or decrypt communication in the interest of national security, sovereignty, defense and for preservation of public order or investigation of an offence.

[37] 'India Threatens to Shut Down BlackBerry Services' (*Voice of America News*, 11 August 2010) <https://www.voanews.com/east-asia/india-threatens-shut-down-blackberry-services> accessed 12 November 2020.

[38] Because RIM was a device manufacturer, restrictions on encryption standards applicable to telecommunication companies under license agreements were not applicable to RIM.

[39] Damien McElroy, 'Mumbai attacks: Terrorists Monitored British Websites using BlackBerry Phones' (*The Telegraph*, 28 November 2008) <https://www.telegraph.co.uk/news/worldnews/asia/india/3534599/Mumbai-attacks-Terrorists-monitored-coverage-on-UK-websites-using-BlackBerry-phones-bombay-india.html> accessed 12 November 2020.

[40] Sahil Makkar & Shauvik Ghosh, 'India Renews Threat to ban BlackBerry Services' (*LiveMint*, 29 July 2010) <https://www.livemint.com/Home-Page/H0ZmePNYWQk7Tv6NkNAefK/India-renews-threat-to-ban-BlackBerry-services.html>accessed 12 November 2020.

[41] Apurva Chaudhary, 'BlackBerry's Tussle with Indian Govt Finally Ends; BB Provides Interception System' (*Medianama*, 10 July 2013) <https://www.medianama.com/2013/07/223-blackberrys-tussle-with-indian-govt-finally-ends-bb-provides-interception-system/> accessed 12 November 2020.

preparation for the attack; agencies merely failed to put the pieces together.[42] Therefore, the need for creating backdoors to amplify surveillance capabilities and its value to investigations is questionable.

Seven years later, the central government made its first attempt to create a comprehensive policy on encryption. It released a draft National Encryption Policy in 2015[43] and withdrew it within two days in response to severe criticism from a range of stakeholders regarding concerns of privacy and state overreach. The draft had several problematic provisions.[44] For instance, it required users and businesses to retain plain text copies of encrypted communications for 90 days, triggering grave cybersecurity concerns. Further, the government could specify the key length and algorithm to be used in encryption technologies for all users and businesses, leaving no room for users to choose stronger standards, or for businesses to innovate and adopt security measures. An addendum was issued[45] with the aim of mitigating some of the damage. However, a revised draft of the encryption policy has not yet been released.

Most recently, and arguably most problematically, encryption has been in the spotlight in India owing to the notification of the Information Technology (Intermediaries Guidelines and Digital Media Ethics Code) Rules, 2021 ('**New Intermediary Guidelines**') which alter the intermediary liability regime in India.[46] These guidelines mark an important moment in the country's journey on technology policy and may be indicative of greater regulation of encryption, influenced by its perceived hindrance to enabling government access to data. The implementation will impact the economy of the world's largest democracy, and determine in part whether technology strengthens or impedes fundamental rights and freedoms.

---

[42] <https://www.nytimes.com/2014/12/22/world/asia/in-2008-mumbai-attacks-piles-of-spy-data-but-an-uncompleted-puzzle.html>.

[43] Draft Encryption Policy 2015.

[44] 'FAQ: Legal Position of Encryption in India' (*SFLC.in*, 11 November 2017) <https://sflc.in/faq-legal-position-encryption-india> accessed 12 November 2020; Nandita Mathur, 'What was the Draft Encryption Policy and Why it was Withdrawn?' (*LiveMint*, 22 September 2015) <https://www.livemint.com/Politics/RZtAGhM6IjDBWujiK6ysEP/What-was-the-encryption-policy-and-why-it-was-withdrawn.html> accessed 12 November 2020.

[45] The addendum exempted mass use encryption products used in web applications, social media sites, and social media applications such as WhatsApp, Facebook, Twitter etc.; SSL/TLS encryption products used in Internet-banking and payment gateways; and SSL/TLS encryption products being used for e-commerce and password-based transactions.

[46] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

III. The Intermediary Liability Rules: Traceability and the Challenge to Encryption

The New Intermediary Guidelines supersede the Information Technology (Intermediaries guidelines) Rules, 2011, which set out the guidelines that intermediaries were bound to follow under the IT Act. Non-compliance with such guidelines would render intermediaries ineligible for protection under the 'safe harbour' provision – section 79 of the IT Act – which exempts intermediaries from liability for third party content as long as the stated conditions are fulfilled. Because of the extremely limited extent to which social media platforms can moderate user content when it is encrypted end-to-end, strong protection against liability for users' statements on social media platforms is essential to their operation, and to their users' rights to express themselves.

A draft of an amendment to the guidelines that intermediaries are bound to follow was first introduced in 2018 ('**Draft Intermediaries Guidelines**').[47] The Draft Intermediaries Guidelines proposed to impose a new traceability requirement that would severely undermine encryption and jeopardise privacy and security. Online intermediaries[48] such as messaging services and social media networks would be obligated to assist the government with identifying the source of any content when required by the government. This would also have a negative impact on the right to freedom of expression as the threat of losing protection from liability would compel companies to over-comply, to the absolute detriment of users.

When the Draft Intermediaries Guidelines were put through public consultation,[49] civil society, technology companies, and technical experts strongly opposed the traceability mandate,owing to its negative implications for encryption, privacy, and free expression.[50] However, the New Intermediary Guidelines, the revised language of which did not undergo any public

---

[47] The Information Technology (Intermediaries Guidelines [Amendment]) Rules 2018.

[48] An 'intermediary' is defined extremely broadly under s 2(w) of the IT Act and includes a wide range of services beyond messaging and social media platforms. The definition states: ''intermediary', with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-market places and cyber cafes'.

[49] 'Comments Invited on Draft of Intermediary Guidelines 2018' (*Ministry of Electronics & Information Technology*, 2018) <https://www.meity.gov.in/comments-invited-draft-intermediary-rules> accessed 8 March 2021.

[50] 'Public Comments on Draft Intermediary Guidelines Rules, 2018' (*Ministry of Electronics & Information Technology*, 2018) <https://www.meity.gov.in/writereaddata/files/public_comments_draft_intermediary_guidelines_rules_2018.pdf> accessed 8 March 2021.

consultation, continue to impose a problematic traceability mandate, albeit different from the traceability mandate in the Draft Intermediaries Guidelines.

The traceability provision in Rule 4(2) of the New Intermediary Guidelines is applicable to any 'significant social media intermediary' (SSMI) providing services primarily in the nature of messaging. An SSMI is defined as 'a social media intermediary having number of registered users in India above such threshold as notified by the Central Government.'[51] The central government has set this threshold at 50 lakh (5 million) users.[52] The New Intermediary Guidelines also empower the government to require any intermediary, which is not an SSMI, to comply with the traceability requirements and the other obligations set out in Rule 4.[53]

The traceability provision obligates SSMIs and such other intermediaries as are designated by the government to enable the identification of the 'first originator' of any information as may be required by a judicial order or an order passed under section 69 of the IT Act, if certain conditions are met. Section 69 empowers the Central and State Governments, or any of their authorized officers, to direct any government agency to monitor, intercept or decrypt information.[54] Such an order requiring identification of the first originator has to be passed for the purposes of prevention, detection, investigation, prosecution or punishment of an offence, or incitement of an offence, pertaining to the sovereignty, integrity, and security of the state, foreign relations, public order, rape, sexually explicit material or child sexual abuse material, punishable with imprisonment for at least five years. Rule 4(2) also states that where other less intrusive means are effective in identifying the originator, a traceability order shall not be passed[55] and compliance with an order would not require disclosure by the SSMI of the content of any

---

[51] New Intermediary Guidelines, rule 2(v).

[52] Ministry of Electronics and Information Technology, Notification Dated 25 February 2021 <https://www.meity.gov.in/writereaddata/files/Gazette%20Significant%20social%20media%20threshold.pdf> accessed 12 November 2020.

[53] New Intermediary Guidelines, rule 6.

[54] In terms of Rule 2(d) of the Decryption Rules, the 'competent authority' for issuing such orders is the Secretary in the Ministry of Home Affairs, in case of the Central Government; or the Secretary in charge of the Home Department, in case of a State Government.

[55] It is worth noting that this limitation applies at the stage of the order being passed by a court or an authorized government agency. These authorities, which do not possess the technical expertise to determine whether other less intrusive measures are available, would not have the benefit of receiving representations from experienced professionals or the intermediary that would have to comply with the order. An intermediary does not have an opportunity to present alternate means that are less intrusive. The practical value of this limitation is therefore limited and will likely not meaningfully restrict the number of such orders that are passed.

message. Finally, where the first originator is located outside India, the first originator within India would be deemed the first originator for the purpose of the clause.

The New Intermediary Guidelines were introduced with the purported aim of preventing the misuse of social media by criminals and 'anti-national elements'[56] and combating the spread of fake news[57] online.[58] These are undeniably important concerns impacting jurisdictions around the world. However, undermining encryption by mandating traceability is not a legitimate solution and none of the asserted goals are demonstrable or provable outcomes of such a measure. As the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression has said, governments 'have not demonstrated that criminal or terrorist use of encryption serves as an insuperable barrier to law enforcement objectives'.[59] Traceability is not a viable solution because, as WhatsApp has argued, it would not correctly identify the originator of content given how users typically use the internet.[60]

---

[56] The term 'anti-national elements' mentioned in the press release accompanying the Draft IT rules has no legal definition. 'Draft IT rules issued for public consultation' (Ministry of Electronics & Information Technology, 24 December 2018) <https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1557159> accessed 12 November 2020.

[57] 'Fake news' in itself is a dubious term that lacks an agreed upon definition. Premising the traceability requirement on the goal of fighting the ambiguous conception of 'fake news' exacerbates the provision's potential to thwart the freedom of expression and impinge upon the right to privacy. Human rights experts, including the UN Special Rapporteur on Freedom of Opinion and Expression, have warned that restrictions on the dissemination of information predicated on vague concepts such as 'fake news' should be abolished as they are incongruous with international standards on freedom of expression, *see*: UNSRFOE, OSCE & OAS, 'Joint declaration on freedom of expression and 'fake news', disinformation and propaganda' (2017).

[58] 'Government notifies Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021' (*Ministry of Information & Broadcasting*, 25 February 2021) <https://www.pib.gov.in/PressReleseDetail.aspx?PRID=1700766> accessed 8 March 2021.

[59] *See*: UNHRC 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression' (22 May 2015) A/HRC/29/32; Soumyarendra Barik, 'Encryption and Issues Related to Misinformation' (*Medianama*, 15 June 2020) <https://www.medianama.com/2020/06/223-encryption-misinformation/> accessed 12 November 2020; 'Fact Sheet: Intermediaries and Encryption' (*Internet Society*, 2 June 2020) <https://www.internetsociety.org/resources/doc/2020/fact-sheet-intermediaries-and-encryption/> accessed 12 November 2020.

[60] *See* WhatsApp's response to a proposal in *Antony Clement Rubin v Union of India* 2018 SCC OnLine Mad 13519 before the Madras High Court on enabling traceability without compromising E2EE, *see*: Aditi Agarwal, 'Exclusive: WhatsApp's Response to Dr. Kamakoti's Recommendation for Traceability in WhatsApp' (*Medianama*, 21 August 2019) <https://www.medianama.com/2019/08/223-exclusive-whatsapps-response-kamakotis-submission/> accessed 26 July 2021; *see also* 'What is Traceability and why does WhatsApp Oppose it?' (*WhatsApp*) <https://faq.whatsapp.com/general/security-and-privacy/what-is-traceability-and-why-does-whatsapp-oppose-it/?lang=en> accessed 26 July 2021.

It would facilitate the attribution of unlawful content to innocent users by bad actors, and subject innocent users to investigation and prosecution for having shared content for purely legitimate concerns.[61]

The ambiguity surrounding who might be considered the 'first originator' in practice exacerbates the potential for an adverse impact on user. Is the 'first originator' the person who first sent the information on the platform that is subject to the traceability requirement? Or is the 'first originator' the first person to send the information in a particular chain of communications carried on the platform, even if the same information was sent across multiple communications chains on the same platform, in which case there would be numerous 'first originators' of the same information? For instance, a WhatsApp or Signal user who shares a screenshot of a tweet for the first time on the platform, may not in fact be the first originator of that content. Further, content on messaging platforms often has several different branches and sources. For instance, user A was the first to share it on the platform with user B. Thereafter, at a later stage, user C, having obtained the content from elsewhere and not from users A or B, shares it with multiple other users after which the content becomes viral. In such cases, it is not clear under the New Intermediary Guidelines who the 'first originator' of the content is, who presumably would be held accountable for it. Such ambiguity may stifle expression by creating concern that a user might be regarded as a 'first originator' when in fact they might not be so.

Traceability requirements can also erode user privacy and lack effectiveness, as illustrated by the expert analysis that Dr. Prabhakaran submitted to the Madras High Court.[62] He argued that traceability is not a demonstrable deterrent as is apparent from the ubiquity of fake news on social media platforms and that it has limited utility until untraceable messaging services become prevalent. Further, he argued that phone numbers have little identification value and equally, tracing the originator of the content does not have any practical value.[63] Most importantly, the negative impact of compromis-

---

[61] *See* WhatsApp's response to a proposal in *Antony Clement Rubin v Union of India* 2018 SCC OnLine Mad 13519 before the Madras High Court on enabling traceability without compromising E2EE, *see*: Aditi Agarwal, 'Exclusive: WhatsApp's Response to Dr. Kamakoti's Recommendation for Traceability in WhatsApp' (*Medianama*, 21 August 2019) <https://www.medianama.com/2019/08/223-exclusive-whatsapps-response-kamakotis-submission/> accessed 12 November 2020.

[62] Dr. Prabhakaran, On a Proposal for Originator Tracing in WhatsApp, *Antony Clement Rubin v Union of India* 2018 SCC OnLine Mad 13519. Dr Prabhakaran submitted his expert analysis on behalf of the Internet Freedom Foundation, which was made an intervener in the case, in response to Dr Kamakoti's proposal, *see*: <https://drive.google.com/file/d/1B2ShWywwVpPX1zTz25UgPMSOokZbcJBx/view>;

[63] Dr. Prabhakaran, On a Proposal for Originator Tracing in WhatsApp, *Antony Clement Rubin v Union of India* 2018 SCC OnLine Mad 13519, *see*: <https://drive.google.com/

ing encryption on privacy and security is immense and inevitable and far outweighs any perceived benefit.

How a Traceability Requirement Undermines Encryption

Encryption evolved as a technological tool that facilitates the realization of a basic human need – to communicate without being overheard – and enabled a vast array of valuable commercial and financial services. However, law enforcement agencies and governments often view the use of encryption, particularly E2EE, as causing a 'going dark' problem whereby information is obscured in ways that the government's ability to access data is reduced.[64,65] Governments around the world have called for encryption 'backdoors' that would allow government entities and law enforcement agencies to circumvent the authentication process and intercept encrypted communications.[66,67]

---

file/d/1B2ShWywwVpPX1zTz25UgPMSOokZbcJBx/view>; Aditi Agarwal, 'Kamakoti's Proposals will Erode User Privacy, Says IIT Bombay Expert in IFF Submission' (*Medianama*, 27 August 2019) <https://www.medianama.com/2019/08/223-iff-response-kamakoti-submission-traceability-2/><https://www.medianama.com/2019/08/223-iff-response-kamakoti-submission-traceability-2/>

[64] James B. Comey, 'Going Dark: Encryption, Technology, and the Balances Between Public Safety and Privacy' (*Federal Bureau of Investigation*, 8 July 2015) <https://www.fbi.gov/news/testimony/going-dark-encryption-technology-and-the-balances-between-public-safety-and-privacy> accessed 12 November 2020; Bedavyasa Mohanty, "Going Dark' in India: The Legal and Security Dimensions of Encryption' (*Observer Research Foundation*, 13 December 2016) <https://www.orfonline.org/research/going-dark-in-india-the-legal-and-security-dimensions-of-encryption/> accessed 12 November 2020; 'Going Dark – Implications of an Encrypted World' (2019) Center for Advanced Studies on Terrorism <https://nsiteam.com/social/wp-content/uploads/2019/07/Going-Dark-Implications-of-an-Encrypted-World-Rev.-3.0-compressed.pdf> accessed 12 November 2020.

[65] It has been argued that this characterization is in fact highly inaccurate. In reality, far from engendering a 'going dark' problem, new technology has in fact enabled a 'golden age of surveillance' by adding an abundance of new vectors of information, see: 'Don't Panic: Making Progress on the 'Going Dark' Debate' (2016) The Berkman Center for Internet & Society <https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf> accessed 12 November 2020; Peter Swire, "Going Dark' Versus a 'Golden Age for Surveillance'' (Center for Democracy & Technology, 28 November 2011) <https://cdt.org/insights/%e2%80%98going-dark%e2%80%99-versus-a-%e2%80%98golden-age-for-surveillance%e2%80%99/> accessed 12 November 2020; Peter Swire & Kenesa Ahmad, 'Encryption and Globalization' (2012) 23 Columbia Sci & Tech L Rev 416, 463-473.

[66] Five Country Ministerial, 'Joint Meeting of FCM and Quintet of Attorneys-General' <https://www.justice.gov/opa/pr/international-statement-end-end-encryption-and-public-safety>; <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/822818/Joint_Meeting_of_FCM_and_Quintet_of_Attorneys_FINAL.pdf> accessed 18 November 2020.

[67] These statements acknowledge the importance of encryption for security and privacy but require companies to institute mechanisms that would create backdoors for the government. The creation of such backdoors fundamentally destroys the privacy promise of encryption as there is no such thing as a backdoor only for good actors – the same backdoors can be

Attacks on encryption by governments typically take either the form of proposed laws requiring intermediaries to build technical capabilities to decrypt data and assist the government with access[68] or laws imposing a traceability requirement such as the one under the New Intermediary Guidelines.[69]

The Indian government has so far proposed two methods for implementing the traceability mandate;[70] (a) Dr. Kamakoti's proposal[71] which entails tagging each message on the E2EE platform with the originator's information;[72] and (b) using a catalogue of alpha-numeric hashes maintained by the intermediary to compare the hash of the problematic message.[73]

a. Message Tagging Model: Dr. Kamakoti's proposal envisages two levels of encryption on an E2EE platform. The content of the message would be encrypted, as it currently is. Separately, the originator's information would also be encrypted and tagged with the message. Platforms would be required to retain the decryption key to the originator's information in an escrow. A government agency would approach such an intermediary with the necessary order, when investigating a problematic message, to decrypt the originator's information.

Dr. Kamakoti recommended that messages should be marked as either 'forwardable' or 'not-forwardable' to account for users' consent. If a user marks a message as 'forwardable' they consent to their information being tagged with the message as the originator. Whereas if a user tags a message

---

exploited by malicious actors and repressive regimes. The statements are therefore self-contradicting and based on an inaccurate understanding of how encryption works.

68 Examples: Australia, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018; United Kingdom, Investigatory Powers Act 2016; and United States of America, Proposed Lawful Access to Encrypted Data Bill (S. 4051, 116th Cong.) 2020.

69 The proposed Brazilian Internet Freedom, Responsibility and Transparency Act, known as the 'Fake News Bill', initially imposed a traceability mandate. It was removed following public criticism.

70 Aditi Agarwal, 'Traceability and end-to-end encryption cannot co-exist on digital messaging platforms: Experts' (*Forbes India*, 16 March 2021) accessed 30 July 2021.

71 Dr. V Kamakoti, Report on Originator Traceability in WhatsApp Messages, *Antony Clement Rubin v Union of India* 2018 SCC OnLine Mad 13519, <https://www.medianama.com/wp-content/uploads/Dr-Kamakoti-submission-for-WhatsApp-traceability-case-1.pdf> accessed 3 May 2021.

72 Dr. V Kamakoti, Report on Originator Traceability in WhatsApp Messages, *Antony Clement Rubin v Union of India* 2018 SCC OnLine Mad 13519, <https://www.medianama.com/wp-content/uploads/Dr-Kamakoti-submission-for-WhatsApp-traceability-case-1.pdf> accessed 3 May 2021.

73 Surabhi Agarwal, 'Govt Proposes Alpha-Numeric Hash to Track WhatsApp Chat' (*ET CIO*, 23 March 2021) <https://cio.economictimes.indiatimes.com/news/social-media/govt-proposes-alpha-numeric-hash-to-track-whatsapp-chat/81643144> accessed 3 May 2021.

as 'non-forwardable' and the recipient forwards it, the recipient who forwards the 'non-forwardable' message becomes the originator.

The practical effectiveness of this proposal is highly suspect. The originator's information would only travel with the message for the purpose of traceability when it is simply forwarded on the same platform. The function would be futile if any other form of sharing is used. For instance, if a user copies and pastes the message, or adds a caption to an image or a video before sharing it, or sharesa screenshot of the message, the originator would change. Further, the focus on forwarded messages ignores the fact that the intent and context with which the message was shared, by any user along the message's travel footprint, cannot be discerned. For example, a user could forward a message and in the next moment, send a second message to the recipients of the forwarded message that debunks it. At the very least, if implemented, this proposal will deter users from sharing information and communicating freely and in the worst-case scenario, it will result in attributing culpability to the wrong people and for the wrong reasons.

A technical measure such as this, which requires the retention of a decryption key in an escrow is fundamentally contrary to E2EE. The inability of the intermediary to access any encrypted information linked to the messages circulating on its platform is central to E2EE. The storage of such a key also makes intermediaries and users' information extremely vulnerable to attacks and undermines the practice of data minimization for privacy and security.

When the originators' identity is permanently linked to a message, users' anonymity and privacy are compromised and this causes a chilling effect on the right to freedom of expression. The traceability model will deprive users of safe spaces for communication and information-sharing on the internet. For a model whose effectiveness is purely theoretical, it carries far too great a threat to data security and users' fundamental rights and freedoms.

b. Message hashing model: The other model of implementing traceability would involve requiring platforms to maintain a library of alpha-numeric hashes of all messages sent on their platforms. It was advocated by Rakesh Maheshwari, senior director and group co-ordinator of cyberlaw and eSecurity at MeitY.[74] Hashing is a mathematical process of attaching a piece of

[74] New IT Rules: Empowering Control or Controlled Empowerment? Deciphering the Intermedia (CCAOI India, 4 March 2021) <https://www.youtube.com/watch?v=E8wkfidXaWs> accessed 3 May 2021; Surabhi Agarwal, 'Govt Proposes Alpha-Numeric Hash to Track WhatsApp Chat' (*ET CIO*, 23 March 2021) <https://cio.economictimes.indiatimes.com/news/social-media/govt-proposes-alpha-numeric-hash-to-track-whatsapp-chat/81643144> accessed 3 May 2021.

data with a fixed value.[75] This is typically used to verify the authenticity of data, including for password verification. The government wants WhatsApp and other E2EE platforms to assign an alpha-numeric hash to every single message on their platform. For instance, the hash value of a message that reads 'Good Morning' may be '4ch77da'. The government's demand is that the intermediary must maintain a library of hashes associated with each message so that the originator of problematic content can be traced when the problematic content is presented to the platform.[76]

This proposal is technically infeasible. It rests on the assumption that the hash value of a message remains constant if the content is unchanged. However, on E2EE platforms like WhatsApp and Signal, the generation of a hash value also accounts for the unique identity of the sender and the recipient.[77] Therefore, the hash value of the message 'good morning' from user A to B changes when user B forwards the same 'Good Morning' to user C. An investigation into the 'Good Morning' from user B to C would not reveal the involvement of user A at all.[78] This is because WhatsApp and Signal have a forward secrecy feature enabled by the double ratchet algorithm which essentially changes the key between two users for each message.[79] Enabling traceability in the way the government proposes would require WhatsApp and Signal to give up forward secrecy, a vital feature of E2EE. It would also mean that the intermediaries would then be able to track the entire chain of each communication on its platform which is antithetical to E2EE.

---

[75] Mehab Quresi, 'What is hashing & why does Indian govt want WhatsApp to use it?' (*The Quint*, 25 March 2021) <https://www.thequint.com/tech-and-auto/what-are-hashes-and-why-does-india-wants-whatsapp-to-implement-them#:~:text=Hashing%20is%20a%20process%20where,be%20easily%20traced%20when%20needed.&text=The%20Indian%20government%20wants%20WhatsApp%20to%20implement%20traceability%20in%20its%20services.> accessed 3 May 2021.

[76] Surabhi Agarwal, 'Govt Proposes Alpha-Numeric Hash to Track WhatsApp Chat' (*ET CIO*, 23 March 2021) <https://cio.economictimes.indiatimes.com/news/social-media/govt-proposes-alpha-numeric-hash-to-track-whatsapp-chat/81643144> accessed 3 May 2021.

[77] *See* Amit Panghal, 'WhatsApp's End to End Encryption, How does it work?' (*Medium*, 6 October 2018) <https://medium.com/@panghalamit/whatsapp-s-end-to-end-encryption-how-does-it-work-80020977caa0> accessed 26 July 2021; *see also* 'WhatsApp Encryption Overview – Technical White Paper' (*WhatsApp*, 22 October 2020) <https://scontent.whatsapp.net/v/t39.8562-34/122249142_469857720642275_2152527586907531259_n.pdf/WA_Security_WhitePaper.pdf?ccb=1-3&_nc_sid=2fbf2a&_nc_ohc=ObtXRc807aoAX-KKts4&_nc_ht=scontent.whatsapp.net&oh=554bfa3edd8370b7da89ab37be249187&oe=61026BD9> accessed 26 July 2021.

[78] Aditi Agarwal, 'Traceability and End-to-End Encryption Cannot Co-exist on Digital Messaging Platforms: Experts' (*Forbes India*, 16 March 2021) accessed 3 May 2021.

[79] Trevor Perrin and Moxie Marlinspike, 'The Double Ratchet Algorithm' (*Signal*, 20 November 2016) <https://signal.org/docs/specifications/doubleratchet/ > accessed 3 May 2021.

Further, the slightest change in the content of a message would alter its hash value. For instance, the hash of a message that reads 'Good Morning' will be different from the hash of 'Good Morning…'.Similarly, if user A sends the same message to user B twice, the double ratchet algorithm ensures that the hash value of each of those messages is different, despite the identical content.[80] This will make it practically impossible to trace a message back to the first originator with the use of alpha-numeric hashes on an E2EE system. The practical infeasibility of this proposal is also exacerbated by the sheer volume of messages that would have to be hashed, and the size of the hash library that would have to be maintained. Billions of messages are sent on WhatsApp every minute.[81] Message hashes would have to be stored for years in order to facilitate traceability for crimes associated with a message that are committed or prosecuted years later. Intermediaries that have large message volume cannot reasonably be expected to create the ability to store hashes and track each message. Even if this ability were to be developed somehow, such extensive storage would be violative of data minimization principles.

Dr. Debayan Gupta, cryptographer and assistant professor of computer science at Ashoka University, is firmly of the view that E2EE is compromised the moment anyone except the sender and recipient can tell which message was sent to whom: 'On an end-to-end encrypted platform, if I have an option of sending a message 'abc' or 'def', nobody except the recipient should be able to tell which of the two was sent.'[82] At present, the 'forward' icon on WhatsApp serves to mark the message on the receiver's phone as having been 'forwarded' and count if it has been forwarded more than five times.[83] WhatsApp itself does not know how many times a message has been forwarded.[84]

---

[80] *See* Trevor Perrin and Moxie Marlinspike 'The Double Ratchet Algorithm' (*Signal*, 20 November 2016) <https://signal.org/docs/specifications/doubleratchet/> accessed 26 July 2021.

[81] Surabhi Agarwal, 'Govt Proposes Alpha-numeric Hash to Track WhatsApp Chat' (*ET CIO*, 23 March 2021) <https://cio.economictimes.indiatimes.com/news/social-media/govt-proposes-alpha-numeric-hash-to-track-whatsapp-chat/81643144> accessed 3 May 2021.

[82] Aditi Agarwal, 'Traceability and End-to-End Encryption cannot Co-exist on Digital Messaging Platforms: Experts' (*Forbes India*, 16 March 2021) accessed 3 May 2021.

[83] 'FAQ: How to Forward Messages' (*WhatsApp*) <https://faq.whatsapp.com/web/chats/how-to-forward-messages/?lang=en> accessed 12 November 2020; 'FAQ: About Forwarding Limits' (*WhatsApp*) <https://faq.whatsapp.com/general/chats/about-forwarding-limits/?lang=en> accessed 24 February 2021. WhatsApp marks a message that is five forwards away from its original sender with a 'Forwarded many times' icon. Such messages can then only be forwarded to one chat at a time.

[84] 'FAQ: About Forwarding Limits' (*WhatsApp*) <https://faq.whatsapp.com/general/chats/about-forwarding-limits> accessed 24 February 2021; 'FAQ: Coronavirus Product

According to Dr. Debayan Gupta, E2EE breaks the moment something is attached to a message which can be tracked by the service provider – such as the originator's information in Dr. Kamakoti's proposal. Each of the proposed models for traceability is inconsistent with a communications service that is fully encrypted end-to-end. Thus, each would weaken the protections that encryption provides, and is incongruous with users' expectations about the privacy and confidentiality of their communications in an encrypted environment. E2EE platforms would have to fundamentally alter their architecture to eliminate the very features that prioritize privacy and security and inspire users' trust.[85]

The utility of techniques that providers are likely to pursue in order to implement a traceability requirement, such as tagging the originator's information with each message and maintaining a library of hashes to trace messages back to their originators is unclear.[86] This might result in intermediaries being compelled to implement an alternate model with backdoors to encryption in order to remain eligible for safe harbour protection and steer clear of liability. The New Intermediary Guidelines essentially present intermediaries with a Hobson's choice – they may either retain design components that strengthen privacy and security or expose themselves to liability. To penalize platforms for choosing to prioritize users' rights and freedoms is patently undemocratic.

Government officials are likely to point to the third proviso in the traceability provision in the New Intermediary Guidelines as they argue that the

---

Changes- About Forwarding Limits' (*WhatsApp*) <https://faq.whatsapp.com/general/coronavirus-product-changes/about-forwarding-limits> accessed 12 November 2020; Katitza Rodriguez & Seth Schoen, 'FAQ: Why Brazil's Plan to Mandate Traceability in Private Messaging Apps will Break User's Expectation of Privacy and Security' (*Electronic Frontier Foundation*, 7 August 2020) <https://www.eff.org/deeplinks/2020/08/faq-why-brazils-plan-mandate-traceability-private-messaging-apps-will-break-users> accessed 12 November 2020.

[85] WhatsApp's submission in a case before the Madras High Court that considers the issue of traceability. WhatsApp stated that a traceability mandate would force WhatsApp to fundamentally change its platform and undermine E2EE. The case has been transferred and is now pending in the Supreme Court of India, *see*: *Antony Clement Rubin & Janani Krishnamurthy v Union of India* (TP (C) 1943-46/2019); Aditi Agarwal, 'Exclusive: WhatsApp's Response to Dr Kamakoti's Recommendation for Traceability in WhatsApp' (*Medianama*, 21 August 2019) <https://www.medianama.com/2019/08/223-exclusive-whatsapps-response-kamakotis-submission/> accessed 12 November 2020; Aditi Agarwal, 'Kamakoti's Proposals will Erode user Privacy, says IIT Bombay Expert in IFF Submission' (*Medianama*, 27 August 2019) <https://www.medianama.com/2019/08/223-iff-response-kamakoti-submission-traceability-2/>.

[86] Internet Society, Traceability and Cybersecurity: Experts' Workshop Series on Encryption in India, <https://www.internetsociety.org/resources/doc/2020/traceability-and-cybersecurity-experts-workshop-series-on-encryption-in-india/#_ftnref2> accessed 23 February 2021.

New Intermediary Guidelines do not undermine encryption. It states that 'in complying for an order for identification of the first originator, no significant social media intermediary shall be required to disclose the contents of any electronic message.'[87] This proviso offers little reassurance with respect to the inviolability of the encrypted message. First, in most cases, if the government is seeking to trace the first originator of a problematic message, government officials must already have access to the content of the relevant message. Second, there is a distinction between not requiring intermediaries to 'disclose' the content of a message, and not requiring intermediaries to be able to 'access' the content at all.

The second proviso, which states that a traceability order shall not be passed where other less intrusive means are effective in identifying the originator of the information, also fails to serve as a meaningful limitation. This limitation applies at the stage of the order being passed by a court or an authorized government agency. These authorities, which do not possess the technical expertise to determine whether other less intrusive measures are available, would not have the benefit of receiving representations from experienced professionals or the intermediary that would have to comply with the order. An intermediary is not granted an opportunity to present alternate means that are less intrusive. Therefore, the practical value of this limitation is therefore limited and will likely not meaningfully restrict the number of such orders that are passed.

A more meaningful limitation would exempt SSMIs from complying with a traceability order if the only technically feasible method of doing so would require the implementation of a new mechanism that enables access to end-to-end encrypted content. Implementation of the traceability requirement by tagging originator's information or using alpha-numeric hashes or other methods involving digital attribution through signatures associated with every message[88] and increased collection and storage of metadata[89] is not fully reliable and is vulnerable to impersonation and misuse by bad actors. It can therefore result in false attributions.

---

87 New Intermediary Guidelines, rule 4(2).

88 Megha Mandavia, 'India asks WhatsApp to Fingerprint Messages to Ensure Traceability' (*The Economic Times*, 18 June 2019) <https://tech.economictimes.indiatimes.com/news/mobile/india-asks-whatsapp-to-fingerprint-messages-to-ensure-traceability/69833913> accessed 12 November 2020; Shweta Ganjoo, 'WhatsApp Maintains its Stand on Govt's Request for Message Traceability in India' (*India Today*, 18 June 2019) <https://www.indiatoday.in/technology/news/story/whatsapp-maintains-its-stand-on-govt-s-request-for-message-traceability-in-india-1551098-2019-06-18> accessed 12 November 2020.

89 Increased metadata collection to implement traceability would be contrary to data minimization and privacy by design principles and create security risks owing to longer retention of data.

Further, even in circumstances where access to the content of messages is not required by the government, the traceability mandate, as set out in the New Intermediary Guidelines, would still undermine encryption. Representatives of the Ministry of Electronics and Information Technology have stated that only the metadata relating to the first originator will be tracked, and not that relating to the entire chain of communication.[90] However, this is not practically feasible. For instance, the fourth proviso to Rule 4(2) provides that where the first originator of content is outside India, the first originator within India will be deemed the first originator for the purpose of this clause. This can arguably not be done without tracking the entire chain of communication,[91] or at least the chain until the message reaches a user located in India. Thus, re-engineering of the platform to enable capturing substantially more metadata and tracking of entire chains of communications could become necessary for compliance. The introduction of features that enable access to and storage of more information about users and their communications is synonymous with the introduction of weaknesses that will make sensitive data vulnerable to unauthorized access by third parties. The direct result, whether intended or unintended,will be an erosion of the data minimization principle as platforms are compelled to track and store more data, and an overall weakening of the privacy and security features that constitute the core tenets of E2EE platforms enabling secure communication.

Among the most popular examples of E2EE platforms in India are WhatsApp with 400 million users as of July 2019,[92] and Signal with 26.4 million downloads within two weeks in January 2021 and a projected growth of up to 200 million users in the next two years.[93] WhatsApp and Signal have a security by default design that ensures that no third party, not even WhatsApp and Signal, can access the messages, photos, videos,

---

[90] New IT Rules: Empowering Control or Controlled Empowerment? Deciphering the Intermedia (CCAOI India, 4 March 2021) https://www.youtube.com/watch?v=E8wkfidX-aWs accessed 8 March 2021.

[91] 'What is the Originator or Traceability provision in the Information Technology (Intermediary Guidelines and Digital Media Ethics Code), 2021?' (*SFLC.in*, 12 April 2021) <https://sflc.in/what-originator-or-traceability-provision-information-technology-intermediary-guidelines-and> accessed 11 May 2021.

[92] Prasid Banerjee, 'WhatsApp Announces 2 Billion Users Worldwide' (*LiveMint*, 12 February 2020) <https://www.livemint.com/technology/tech-news/whatsapp-announces-2-billion-users-worldwide-11581516342061.html> accessed 12 November 2020.

[93] Prasid Banerjee, 'Signal Logs in 26.4 Million Downloads in India in Less than Two Weeks' (*LiveMint*, 19 January 2021) <https://www.livemint.com/technology/tech-news/signal-logs-in-26-4-million-downloads-in-india-in-less-than-two-weeks-11611053954964.html> accessed 7 April 2021; 'Signal Targets 100-200 mn users in India: Brian Acton' (*National Herald*, 13 January 2021) <https://www.nationalheraldindia.com/science-and-tech/signal-targets-100-200-mn-users-in-india-brian-acton> accessed 7 April 2021.

voice messages, documents, and calls exchanged on the platform.[94] Further, Signal can only access the date and time a user registered with Signal and the last date of a user's connectivity to the Signal service.[95] This prevents the storage of hashes and the attribution of the originator's information to each message, as envisioned in the leading traceability implementation proposals. Such features that strengthen privacy and security will be severely undermined by the New Intermediary Guidelines. WhatsApp, Signal,and other E2EE platforms would have to be redesigned to either weaken encryption or introduce backdoors that would effectively destroy E2EE.[96]

Irrespective of how intermediaries' systems are re-engineered to comply with the traceability requirement, the result will be a blow to encryption that steers technology away from formats that focus on privacy and respect data-minimization principles. The traceability mandate would compel a drastic alteration of such privacy-by-design architecture and expose to service providers of E2EE platforms, and potentially other parties, information that has hitherto been private.

The Negative Impact of Traceability on Cybersecurity

Once the ability to trace the origin of a thread of communication has been created and encryption is weakened, there is no fail-safe method of ensuring that only the intended party, whether it is the service provider or the government, will be able to exploit the mechanism that facilitates traceability. The requirement of building a capability to allow government access to encrypted information online would essentially amount to mandating insecurity.[97] It is technologically impossible to create a backdoor that works only for legitimate actors or the 'good guys.'[98] E2EE platforms are valuable

---

[94] 'WhatsApp Security' (*WhatsApp*) <https://www.whatsapp.com/security/> accessed 7 April 2021; 'Is it private? Can I Trust it?' (*Signal*) <https://support.signal.org/hc/en-us/articles/360007320391-Is-it-private-Can-I-trust-it-> accessed 7 April 2021.

[95] 'Grand Jury Subpoena for Signal user Data, Eastern District of Virginia' (*Signal*) <https://signal.org/bigbrother/eastern-virginia-grand-jury/> accessed 7 April 2021.

[96] 'Building Traceability would Undermine End-to-End Encryption WhatsApp' (*The Economic Times*, 24 August 2018) <https://economictimes.indiatimes.com/tech/internet/building-traceability-would-undermine-end-to-end-encryption-whatsapp/articleshow/65515114.cms?from=mdr>accessed 7 April 2021.

[97] Hareld Abelson, Daniel Weitzner, et al, 'Keys Under Doormats: Mandating Insecurity by Requiring Government Access to all Data and Communications' (2015) Computer Science and Artificial Intelligence Laboratory Technical Report MIT-CSAIL-TR-2015-026 <https://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf?sequence=8&isAllowed=y> accessed 12 November 2020.

[98] Charles Duan, Arthur Rizer, Zach Graves & Mike Godwin, 'Policy Approaches to the Encryption Debate' (2018) R Street Policy Study 133/2018 <http://2o9ub0417chl2l-g6m43em6psi2i.wpengine.netdna-cdn.com/wp-content/uploads/2018/03/133.pdf> accessed 12 November 2020; Amie Stepanovich & Michael Karanicolas, 'Why an

precisely because they keep information exchanged between parties secure indiscriminately from *all* third parties, including the one that created and makes the platform available, and therefore provide robust protection for information online and internet users' right to privacy. Once a vulnerability has been introduced into the system, it significantly aggravates the risk of data breaches and malicious attacks.[99] Therefore weakening security on the internet with the aim of strengthening national security is counter-logical. It would also be contrary to the provision in the New Intermediary Guidelines which requires intermediaries to take all reasonable measures to secure information.[100]

Further, the blanket assumption that the government is a 'good' actor is inherently flawed. Repressive governments often use surveillance to monitor citizens' actions[101] and encryption offers a degree of freedom from such surveillance.[102] Traceability would empower repressive regimes with the ability to ascertain who interacted with a particular message that expressed dissent or encouraged protest, irrespective of the context in which they did so. Particularly in a democracy, the right to privacy is inextricably linked to the growth of a society that fosters the freedom of expression and facilitates inclusive growth.[103]

Encryption Backdoor for Just the 'Good Guys' Won't Work' (*Just Security*, 2 March 2018) <https://www.justsecurity.org/53316/criminalize-security-criminals-secure/> accessed 12 November 2020; Steve Morgan, 'Apple's CEO on Encryption: 'You can't have a Back Door that's Only for the Good Guys'' (*Forbes*, 21 November 2015) <https://www.forbes.com/sites/stevemorgan/2015/11/21/apples-ceo-on-encryption-you-cant-have-a-back-door-thats-only-for-the-good-guys/#44910af8483a> accessed 12 November 2020.

99 ibid.

100 New Intermediary Guidelines, rule (3)(1)(i).

101 Endalkachew Chala, 'Defending Against Overreaching Surveillance in Ethiopia: Surveillance Self-Defense now available in Amharic' (*Electronic Frontier Foundation*, 1 October 2015) <https://www.eff.org/deeplinks/2015/09/defending-against-overreaching-surveillance-ethiopia-surveillance-self-defense-n-0> accessed 12 November 2020; ANI, 'China Uses Tech as Tool of Repression to Monitor Citizens: US Commission' (*LiveMint*, 9 August 2020) <https://www.livemint.com/news/world/china-uses-tech-as-tool-of-repression-to-monitor-citizens-us-commission-11596931164736.html> accessed 12 November 2020; for a global overview, *see*: Adrian Shahbaz, 'The Rise of Digital Authoritarianism' (*Freedom House*, 2018) <https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism> accessed 12 November 2020.

102 ibid; R Street Paper; Andy Greenberg, 'Encryption App 'Signal' Is Fighting Censorship with a Clever Workaround' (*Wired*, 21 December 2016) <https://www.wired.com/2016/12/encryption-app-signal-fights-censorship-clever-workaround/> accessed 12 November 2020.

103 Lord Bauer, Ramon Diaz, et al, *Freedom, Democracy and Economic Welfare: Proceedings of an International Symposium* (Fraser Institute 1986) 96-100; 'Keystones to foster inclusive Knowledge Societies: Access to information and knowledge, Freedom of Expression, Privacy, and Ethics on a Global Internet' (2015) United Nations Educational, Scientific, and Cultural Organization Draft Study, 7 <https://unesdoc.unesco.org/ark:/48223/pf0000232563> accessed 12 November 2020.

Traceability's Impact on the Fundamental Right to Privacy

The traceability requirement, in permanently attributing an identity to a private communication, would jeopardise the right to privacy[104] of internet users and thwart their right to freedom of expression,[105] both of which are fundamental rights under the Constitution of India. Anonymity, privacy, and free expression are inextricably linked and instrumental to the establishment of a healthy democratic society.[106] As former UN Special Rapporteur on Freedom of Expression Frank La Rue notes, 'throughout history, people's willingness to engage in debate on controversial subjects in the public sphere has always been linked to possibilities for doing so anonymously.'[107] He further recognizes the revolutionizing and pivotal role that the internet plays in enabling anonymity: '[a]nonymity of communications is one of the most important advances enabled by the internet, and allows individuals to express themselves freely without fear of retribution or condemnation.'[108] The perception of lack of privacy has an acute and demonstrable chilling effect on the freedom of expression[109] and the imposition of traceability will

---

[104] In *K.S. Puttaswamy v Union of India* (2017) 10 SCC 1, a nine-judge bench of the Supreme Court of India unanimously held that the right to privacy is protected under the fundamental rights and freedoms set out in Part III of the Constitution of India. Several petitions challenging the New Intermediary Guidelines, partially or in their entirety, are currently pending before various Indian High Courts. The government has filed a transfer petition seeking that certain petitions be transferred to the Supreme Court to be heard together. Some of cases involving a challenge to Part II of the New Intermediary Guidelines including the traceability provision on the grounds that it violates the fundamental rights to privacy and freedom of expression, among other things, include *Live Law Media (P) Ltd. v Union of India* WP (C) 6272 of 2021 ; *Facebook Inc v Union of India* WP (C) No. 679 of 2019, decided on 24-9-2019; *WhatsApp LLC v CCI* 2021 SCC OnLine Del 2308; *Sanjay Kumar Singh v Union of India and others* WP(C) 3483 of 2021; *TM Krishna v Union of India* WP (C) No. 12515/2021; *Nikhil Wagle v Union of India* PIL/14204/2021; *Sayanti Sengupta v Union of India* WPA(C) No. 153 of 2021; *Uday Bedi v Union of India* WP(C) No. 6844 of 2021. This is not an exhaustive list of all the challenges to the New Intermediary Guidelines.

[105] Constitution of India, art 21.

[106] The importance of anonymity in a democracy was perhaps best captured by Justice John Paul Stevens in the majority opinion in *McIntyre v Ohio Elections Commission*, 1995 SCC OnLine US SC 36 : 514 US 334 (1995), wherein he stated 'anonymity is a shield from the tyranny of the majority'.

[107] UNHRC, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression' (16 May 2011) A/HRC/17/27.

[108] UNHRC, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression' (17 April 2013) A/HRC/23/40.

[109] Jon Penney, 'Chilling Effects: Online Surveillance and Wikipedia Use' (2016) 31(1) Berkeley Tech L J 117, 161-169. The article analyzes an empirical study evidencing the chilling effect of government surveillance on Wikipedia users. It uses Wikipedia data or web traffic data to explore how the traffic to privacy-sensitive articles reduced significantly after revelations of mass surveillance.

inevitably lead to this undesirable outcome. In other words, '[i]t's disingenuous when the Indian government says that they want traceability but 'not at the cost of encryption or privacy'[110] Traceability is bound to be at the cost of privacy - as well as encryption - even if it means getting meta-data.'[111]

Owing to its inescapable negative impact on the right to privacy, a traceability mandate would have to clear the four-pronged proportionality and necessity test laid down by the Supreme Court of India in the seminal case of *K.S. Puttaswamy v Union of India*.[112] In *Puttaswamy*, a nine-judge bench of the Supreme Court unanimously held that 'the right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III (fundamental rights) of the Constitution.'[113] The court observed that the right to privacy is an inalienable right that is inherent in every individual simply by virtue of being human.[114] In acknowledging the distinction between rights that are inherent and natural, and rights that the government has the power to confer and take away,[115] the court finds that the right to privacy is a natural right that is not bestowed by the State or the Constitution for the first time – it is only recognized and preserved – and can therefore not be taken away.[116] Any statute that infringes the inalienable right to privacy without any countervailing public interest would be declared void.[117]

---

[110] Nikhil Pahwa, 'Intermediary Liability: 'Many Problems Need Many Solutions', Says S Gopalakrishnan, Jt Secretary, MEITY' (*Medianama*, 19 March 2019) <https://www.medianama.com/2019/03/223-intermediary-liability-many-problems-need-many-solutions-says-s-gopalakrishnan-jt-secretary-meity/> accessed 12 November 2020.

[111] Nikhil Pahwa, 'We Need a Better Approach to WhatsApp and Traceability' (*Medianama*, 28 March 2019) <https://www.medianama.com/2019/03/223-we-need-a-better-approach-to-whatsapp-and-traceability/> accessed 12 November 2020.

[112] (2017) 10 SCC 1.

[113] (2017) 10 SCC 1 [141-142] [DY Chandrachud J]. The case recognizes nine primary types of privacy: bodily, spatial, communicational, intellectual, decisional, associational, behavioral and informational. This drew from existing literature, *see*: Bert-Jaap Koops et al., 'A Typology of Privacy' (2017) 38(2) Univ Pennsylvania J Intl L 483.

[114] (2017) 10 SCC 1 [92] [RF Nariman J].

[115] The idea of privacy being an inevitable outcome of such a juxtaposition of rights was espoused in the seminal article by Samuel D. Warren and Louis. D. Brandeis on the right to privacy as the right to be let alone, that is considered to be the birth of privacy law [*see*: Samuel D. Warren & Louis D. Brandeis, 'The Right to Privacy' (1890) 4(5) Harvard L Rev 193]. The court cites to this particular paragraph from the article: 'Once a civilization has been made the distinction between the 'outer' and the 'inner' man, between the light of the soul and the life of the body, between the spiritual and the material, between the sacred and the profane, between rights inherent and inalienable, and the rights that are in the power of the government to give and take away, between public and private, between society and solitude, it becomes impossible to avoid the idea of privacy by whatever name it may be called – the idea of a private sphere in which man may become and remain himself.'

[116] (2017) 10 SCC 1 [92] [RF Nariman J].

[117] (2017) 10 SCC 1 [180-81] [DY Chandrachud J].

The proportionality and necessity test outlined by the court requires that: '(i) the action must be sanctioned by law; (ii) the proposed action must be necessary in a democratic society for a legitimate aim; (iii) the extent of such interference must be proportionate to the need for such interference; and (iv) there must be procedural guarantees against abuse of such interference.'[118] An interference is considered 'necessary in a democratic society' in pursuit of a legitimate aim if it answers a 'pressing social need', if it is proportionate to the legitimate aim pursued and if the reasons adduced to justify the interference are 'relevant and sufficient.'[119] The aim of the test is essentially to strike a balance between public interest and the interests of an individual.[120]

The traceability mandate in the New Intermediary Guidelines arguably does not meet the requirements of the *Puttaswamy* test. It is not a necessary or proportionate measure to meet the stated objective of protecting national security, preserving law and order, or preventing the spread of fake news.[121]

---

[118] (2017) 10 SCC 1 [71] [SK Kaul J]. Chandrachud J., delivering the judgment on behalf of four judges, stated with respect to the test of proportionality that: 'A law which encroaches upon privacy will have to withstand the touchstone of permissible restrictions on fundamental rights. In the context of Article 21 an invasion of privacy must be justified on the basis of a law which stipulates a procedure which is fair, just and reasonable. The law must also be valid with reference to the encroachment on life and personal liberty under Article 21. An invasion of life or personal liberty must meet the three-fold requirement of (i) legality, which postulates the existence of law; (ii) need, defined in terms of a legitimate state aim; and (iii) proportionality which ensures a rational nexus between the objects and the means adopted to achieve them.', (2017) 10 SCC 1 [509]. In *KS Puttaswamy v Union of India*, (2019) 1 SCC 1 [*Puttaswamy (2)*], the 'fundamental precepts of proportionality' have been described as: '1. A law interfering with fundamental rights must be in pursuance of a legitimate state aim; 2. The justification for rights-infringing measures that interfere with or limit the exercise of fundamental rights and liberties must be based on the existence of a rational connection between those measures, the situation in fact and the object sought to be achieved; 3. The measures must be necessary to achieve the object and must not infringe rights to an extent greater than is necessary to fulfil the aim; 4. Restrictions must not only serve a legitimate purposes; they must also be necessary to protect them; and 5. The State must provide sufficient safeguards relating to the storing and protection of centrally stored data. In order to prevent arbitrary or abusive interference with privacy, the State must guarantee that the collection and use of personal information is based on the consent of the individual; that it is authorised by law and that sufficient safeguards exist to ensure that the data is only used for the purpose specified at the time of collection. Ownership of the data must at all times vest in the individual whose data is collected. The individual must have a right of access to the data collected and the discretion to opt out.'

[119] ibid.

[120] (2017) 10 SCC 1 [134] [DY Chandrachud J].

[121] *See*: UNHRC, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression' (22 May 2015) A/HRC/29/32. In that report, David Kaye, the former Special Rapporteur, recommended strong protection for encryption and anonymity, and that States should not restrict these privacy tools, 'even where the restriction is arguably in pursuit of a legitimate interest, many laws and policies regularly do not meet the standards of necessity and proportionality and have broad, deleterious effects on the ability of all individuals to exercise freely their rights to privacy and freedom of opinion and expression.'

The Supreme Court referred extensively to the jurisprudence of the European Court of Human Rights (ECHR) in the *Puttaswamy* decision, giving reason to believe it would turn to ECHR jurisprudence when assessing the traceability mandate. The expression 'prescribed by law' – the equivalent of 'sanctioned by law' – has been held by the ECHR to imply the following requirements:[122]

'Firstly, the law must be adequately accessible: the citizen must be able to have an indication that is adequate in the circumstances of the legal rules applicable to a given case. Secondly, a norm cannot be regarded as a 'law' unless it is formulated with sufficient precision to enable the citizen to regulate his conduct; he must be able – if need be with appropriate advice – to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail.'

The traceability provision in the New Intermediary Guidelines is devoid of any precision that would enable reasonable foreseeability. The circumstances in which the government may demand tracing of the originator, and the conditions or procedural requirements that must be followed, have not been defined with adequate clarity and limitations. Without clear demarcation of the applicability of the traceability mandate, it remains an opaque provision, devoid of reasonable predictability and necessary safeguards. In order to fulfil the 'sanctioned by law' requirement, the legal discretion granted to the government with respect to traceability ought not to be a practically unfettered power and the scope must be set out with sufficient clarity.

An important aspect of necessity is that the chosen measure must be one that is effective and least intrusive.[123] The traceability mandate fails on both counts. First, it is not clear that a traceability mandate will be effective. The originator of a message on a particular platform is not necessarily the creator of the content. In addition, sender signatures that could have to be affixed to messages to facilitate traceability can be spoofed by malicious actors,[124] creating another risk to efficacy. In any event, discerning malicious intent on the originator's part is a dubious prospect, further calling into question the efficacy of such a mandate. Additionally, tracing the chain of communication

---

[122] Judgment in the *Sunday Times v United Kingdom*, No. 6538/74, 26 April 1979, para 49. *See also Malone v United Kingdom*, No. 8691/79, 2 August 1984, paras 67-68.

[123] EDPS, 'The EDPS Quick-Guide to Necessity and Proportionality' (January 2020) <https://edps.europa.eu/sites/edp/files/publication/20-01-28_edps_quickguide_en.pdf> accessed 23 February 2021.

[124] Internet Society, Traceability and Cybersecurity: Experts' Workshop Series on Encryption in India, <https://www.internetsociety.org/resources/doc/2020/traceability-and-cybersecurity-experts-workshop-series-on-encryption-in-india/#_ftnref2> accessed 23 February 2021.

would amount to attributing culpability devoid of the context in which the content was shared – mere virality of a message would unfairly become a valid cause for suspicion. Finally, as indicated above, the traceability mandate could cause some providers to abandon the end-to-end encryption they now offer to all of their users, making users' data vulnerable to malicious actors. As a further indication of ineffectiveness, this result will pertain, even while the malicious actors simply use other methods to encrypt their communications — such as PGP (an acronym for the encryption system known as Pretty Good Privacy[125]) — or devise their own encryption algorithm with the help of a YouTube video[126] or a step-by-step guide[127] available online.[128]

Second, a traceability mandate creates new risks to communications security that makes it a very intrusive measure that is unlikely to be the least intrusive approach. As indicated above, it completely undermines anonymity, which is essential to the ability to communicate without fear of retribution. And, it could require the provider to affix the originator's information in the form of a digital fingerprint to each message, or require the creation of alpha-numeric hashes of each message, both of which are sensitive data that would otherwise not exist and that is vulnerable to exploitation by malicious actors.

Moreover, the traceability mandate is disproportionate in so far as it threatens to infringe the right to privacy of all internet users, and chills their free expression by undermining anonymity, without any demonstration as to how it would practicably lead to achieving the stated aims.[129] Lawmakers, and courts, ought to consider whether the possibility of identifying a few bad actors is worth imperilling the constitutional rights and freedoms of hundreds of millions of Indian users. In the absence of proportionality and

---

[125] Jeff Petters, 'What is PGP Encryption and How Does it Work?' (*Varonis*, 4 June 2020) <https://www.varonis.com/blog/pgp-encryption/> accessed 25 November 2020.

[126] For example, <https://www.youtube.com/watch?v=TZT7wvTeVyY>.

[127] One such guide is available from Wikihow. <https://www.wikihow.com/Create-an-Encryption-Algorithm> accessed 25 November 2020.

[128] Robert E. Endeley, 'End-to-End Encryption in Messaging Services and National Security—Case of WhatsApp Messenger' 9 (2018) J Info 95, 98; Antonis Michalas, 'How WhatsApp Encryption Works—And Why There Shouldn't be a Backdoor' (*The Conversation*, 28 March 2017) <https://theconversation.com/how-whatsapp-encryption-works-and-why-there-shou ldnt-be-a-backdoor-75266> accessed 13 November 2020.

[129] UNHRC, 'Mandate of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression' (June 2018) Research Paper 1/2018. In 2018, as states were intensifying efforts to weaken encryption and compel the installation of encryption backdoors, the former Special Rapporteur's Encryption and Anonymity issued a follow-up to his 2015 report. It correctly indicates that 'despite [their] threat to the privacy and security of *all* users, States have failed to demonstrate the necessity of backdoors, particularly given the wide range of investigative tools at their disposal'.

any demonstration as to how the interference is 'relevant and sufficient,' the traceability proposal fails to fulfil the 'necessary in a democratic society' limb of the test laid down by the Supreme Court.

Finally, safeguards against abuse are lacking. No meaningful procedural safeguards limit the conditions under which the traceability provision may be invoked. The proposed law does not provide for notice and disclosure requirements and an adequate judicial redress mechanism for individuals affected by a traceability order. In any event, the significant harms of the measure to the inalienable and fundamental right to privacy far outweigh any of the measure's hypothetical benefits.[130]

The Indian government will likely continue to press proposals to strengthen traceability and weaken encryption,[131] as is apparent from the New Intermediary Guidelines and a recent joint statement the government made with the Five Eyes nations – New Zealand, the United States, United Kingdom, Canada and Australia – and Japan demanding backdoors for law enforcement to access encrypted content.[132] Whether this approach towards encryption is incorporated in legislation is ultimately the legislature's bailiwick. A recent recommendation by an ad-hoc committee of the upper house of the parliament to break encryption and enable traceability[133] suggests

---

[130] UNHRC, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression' (22 May 2015) A/HRC/29/32. Herein, the former UN Special Rapporteur on freedom of opinion and expression, David Kaye cautioned governments against restricting privacy tools such as encryption on the grounds of fighting terrorism and maintaining public order: 'Laws, practices and policies that ban, restrict, or otherwise undermine encryption and anonymity – all in the name of public order or counter-terrorism – do significant, and I would say disproportionate, damage to the rights at the heart of my mandate'; Angela Marie Rulffes, 'Privacy vs. Security: Fear Appeals, Terrorism and the Willingness to Allow Increased Government Surveillance' (Dissertation, Syracuse University 2017) 24-28; 'Protecting Individual Privacy in the Struggle Against Terrorists' (2008) National Research Council Report, 71-75 <https://epic.org/misc/nrc_rept_100708.pdf> accessed 13 November 2020.

[131] On the other hand, the sector specific regulator, the Telecom Regulatory Authority of India (TRAI) recently released its recommendations on the Regulatory Framework for Over-The-Top (OTT) Communication Services in which it rightly acknowledges that encryption protects the end users and any requirement to obtain decrypted content would require changes to the fundamental architecture of encrypted platforms and make the parties involved in the communication vulnerable to unlawful actors. 'Recommendations on Regulatory Framework for Over-The-Top (OTT) Communication Services' (*Telecom Regulatory Authority of India*, 14th September 2020) 7 <https://www.trai.gov.in/sites/default/files/Recommendation_14092020.pdf> accessed 13 November 2020.

[132] 'International Statement: End-To-End Encryption and Public Safety' (*Department of Justice*, 11 October 2020) <https://www.justice.gov/opa/pr/international-statement-end-end-encryption-and-public-safety> accessed 13 November 2020.

[133] A 14-member ad-hoc committee of the Rajya Sabha, led by Jairam Ramesh, recommended that law enforcement agencies should be permitted to break end-to-end encryption to trace the distributor of child pornography on social media; *see*: Neha Alawadhi, 'RS Panel

that the parliament might go along with the executive. However, the future of encryption in India will to a significant extent also be informed by the jurisprudence on the interaction between encryption, traceability and the fundamental right to privacy that is evolving in the Supreme Court.[134]

Suggests Breaking Encryption To Curb Child Pornograhy Distribution' (*Business Standard*, 27 January 2020) <https://www.business-standard.com/article/technology/rs-panel-suggests-breaking-encryption-to-curb-child-pornograhy-distribution-120012600705_1.html> accessed 14 November 2020.

[134] In addition to the legal challenges to the traceability provision in the New Intermediary Guidelines, including those mentioned in footnote 104, certain cases relating to traceability, and encryption, that were earlier being heard by the High Courts in three states were transferred to the Supreme Court of India in October 2019 in view of the complex legal and technological questions involved that would impact the fundamental rights of internet users [*Facebook Inc v Union of India* 2019 SCC OnLine SC 1717]: (1) In *Antony Clement Rubin v Union of India* 2019 SCC OnLine Mad 11784, two animal rights activists approached the Madras High Court, separately but with verbatim applications, under its writ petition, praying for the issuance of a writ directing the government to declare linkage of Aadhar (a unique identity number) as mandatory for authentication while using any social media account to enable traceability.; (2) *In Sagar Rajabhau Surywanshi v Union of India* (PIL/147/2018) (not found), the petitioner prayed the Bombay High Court to issue a writ directing the government to ensure that all users of social media platforms are identifiable, with Indian nationals linked with Aadhar, and foreign nationals linked by their platform to an identity. This case was disposed by the Court since the Petitioner intended to directly intervene in the proceedings before the Supreme Court; and (3) In *Amitabha Gupta v Union of India* (WP (C) No 13076/2019), the petitioner approached the Court to direct Facebook (which owns WhatsApp) to verify new users via some statutorily authorized identity proof documents, such as Aadhaar or voter ID number. These cases have been tagged with other relevant cases in the Supreme Court and the group of matters is pending with no specific date listed for the next hearing. These are: (1) *S.G. Vombatkere v Union of India* (WP (C) No 679/2019)(pending), which involves a writ petition challenging Aadhaar Ordinance, 2019 and Aadhaar Regulations, 2019 as violative of Right to Privacy because it enables State and private actor surveillance as well as commercially exploits the personal information of citizens; (2)-(3) *Manohar Lal Sharma v Union of India* (WP(Crim) No 1/2019)(pending) and *Amit Sahni v Union of India* (WP(C) No 2 of 2019)(pending), which involve writ petitions challenging government notification authorizing 10 central agencies to intercept, monitor and decrypt any computer system; (4) *PUCL v Union of India* (WP(C) No 61 of 2019)(pending), which challenges said notification and s 5(2) of the Telegraph Act; (5) *Mahua Moitra v Union of India* (WP(C) No 916 of 2018, decided on 17-12-2019 (SC), which involves a PIL challenging the 'Social Media Communication Hub' created by the central government as invasion of citizen's social media activity, thus violative of Right to Privacy; (6) *Internet Freedom Foundation v Union of India* (WP(C) No 44 of 2019) (pending), which involves a writ Petition challenging constitutionality of s 69, IT Act, the Decryption Rules, and the aforementioned notification.

IV. The Case for Protecting and Encouraging Encryption

Surveillance Stifles Privacy and Free Expression; Encryption Preserves Both

Privacy is essential to forge interpersonal relationships and to freely communicate thoughts and ideas, especially unconventional or unpopular thoughts and ideas.[135] Even in public spaces, a degree of anonymity is necessary to preserve freedoms that are central to a democratic and open society.[136] Constant surveillance alters human behaviour for fear of disapproval or of retaliation. As the philosopher Jeffrey Reiman observed, '[t]o the extent that a person experiences himself as subject to public observation, he naturally experiences himself as subject to public review. As a consequence, he will tend to act in ways that are publicly acceptable.'[137]

The stultifying effect of surveillance could inhibit a range of individuals who know they are being watched. As the European Court of Human Rights has observed, the mere existence of law that authorizes the secret surveillance of communications amounts to an interference with the right to privacy.[138] Imagine that you are being followed by a law enforcement officer at all times. You would most likely think twice before covering your face to shield yourself from the weather or break into a sprint suddenly because you may miss the train. Also imagine if the officer could access your verbal and written communications. The average person under surveillance will hesitate to pour their hearts out to loved ones, share confidential information, seek professional assistance or search for information about healthcare

---

[135] Charles Fried, 'Privacy' (1968) 77 Yale L J 475.

[136] Christopher Slobogin, 'Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity' (2002) 72 Mississippi L J 213, 240-51.

[137] Jeffrey H. Reiman, 'Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future', (1995) 11 Santa Clara Comp & High Tech L J 27, 38. Herein, Reiman emphasizes the impact of the knowledge of surveillance on human thoughts and deeds in saying '[w]hen you know you are being observed, you naturally identify with the outside observer's viewpoint, and add that alongside your own viewpoint on your action. This double vision makes your act different, whether the act is making love or taking a drive'.; Shoshana Zuboff, *In the Age of the Smart Machine: The Future of Work and Power* (Basic Books 1988) 344-45. Zuboff explains this phenomenon among those who know they are being watched as 'anticipatory conformity'. The reason behind the skepticism that alters behavior in this manner could be anything including uncertainty surrounding how the officer's interpretation and reaction or the inherent desire to appear compliant, but the point is that in the absence of privacy, such problematic hesitation exists.

[138] *Weber and Saravia v Germany* (2006) 46 ECHR 78; Gabor Rona & Lauren Aarons, 'State Responsibility to Respect, Protect and Fulfill Human Rights Obligations in Cyberspace' (2016) 8(503) J Nat Sec L & Pol 503, 511-513.

on sensitive topics[139] or attend protests[140] or political demonstrations.[141] In the case of some individuals – such as journalists, lawyers, medical professionals, or activists[142] – exposure of their communications to any party but the intended recipient could potentially carry grave consequences. The detriments are felt particularly severely by protestors, dissidents, and persecuted minorities in repressive regimes.[143] Such impediments to simply *being* – sim-

---

[139] In the German context, a study showed that half of Germans would not correspond with psychotherapists and marriage counsellors through telephones or emails as a result of data retention. Such sensitive communication would be enabled by encryption as it would preclude access to and retention of the content of communication. *See*: Axel Arnbak, Plenary Presentation at the Taking on the Data Retention Directive Conference in Brussels: What the European Commission Owes 500 Million Europeans (Dec 3 2010) at 3, <http://www.edri.org/files/Data_Retention_Conference_031210final.pdf> accessed 25 November 2020.

[140] TUNHRC, 'Report Of The Special Rapporteur On The Rights To Freedom Of Peaceful Assembly And Of Association' (24 April 2013) A/HRC/23/39. Herein, the Special Rapporteur noted that surveillance and intelligence databases have a chilling effect on protestors; UNHRC, 'Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association: Addendum- Mission to the United Kingdom of Great Britain and Northern Ireland' (17 June 2013) A/HRC/23/39/Add.1.

[141] Roger Clarke, 'While You Were Sleeping . . . Surveillance Technologies Arrived' (2001) 73 Australian Q 10, 13. Herein, Clarke predicted, '[l]eaders of demonstrations in the future should expect both their locations and their conversations to be transparent to the police'. He states that the purpose of surveillance technologies is 'to affect the behavior of both targeted individuals, and of populations'; Stephen Owen, 'Monitoring Social Media And Protest Movements: Ensuring Political Order Through Surveillance and Surveillance Discourse' (2017) 23(6) J Study of Race, Nation & Culture 688, 690-695; Rina Chandran, 'Use of Facial Recognition In Delhi Rally Sparks Privacy Fears' (*Reuters*, 30 December 2019) <https://in.reuters.com/article/us-india-protests-facialrecognition-trfn-idUSKBN1YY0PA> accessed 13 November 2020.

[142] 'Communities At Risk: How Encroaching Surveillance is Putting A Squeeze on Activists' (*Privacy International*, 16 April 2019) <https://privacyinternational.org/news-analysis/2816/communities-risk-how-encroaching-surveillance-putting-squeeze-activists> accessed 13 November 2020; 'Unlawful Surveillance Threatens our Activism. Here's How We can Fight Back' (*Amnesty International*, 8 November 2015) <https://www.amnestyusa.org/unlawful-surveillance-threatens-our-activism-heres-how-we-can-fight-back/> accessed 13 November 2020; Eva Galperin, 'Don't Get Your Sources in Syria Killed' (*Committee to Protect Journalists*, 21 May 2012) <https://cpj.org/2012/05/dont-get-your-sources-in-syria-killed/> accessed 13 November 2020; Julie Posetti, 'Surveillance and Data Collection are Putting Journalists and Sources at Risk' (*The Wire*, 6 May 2017) <https://thewire.in/media/surveillance-data-collection-putting-journalists-sources-risk> accessed 13 November 2020.

[143] Adrian Shahbaz & Allie Funk, 'Social Media Surveillance, Freedom on the Net 2019 Key Finding: Governments Harness Big Data for Social Media Surveillance' (*Freedom House*, 2019) <https://freedomhouse.org/report/freedom-on-the-net/2019/the-crisis-of-social-media/social-media-surveillance> accessed 13 November 2020; 'Ethnic Minorities at Greater Risk of Over Surveillance After Protests' (*Privacy International*, 15 June 2020) <https://privacyinternational.org/news-analysis/3926/ethnic-minorities-greater-risk-oversurveillance-after-protests> accessed 13 November 2020; Valerie Aston, 'State Surveillance of Protest and the Rights to Privacy and Freedom of Assembly: A Comparison of Judicial and Protester Perspectives' (2017) 8(1) EJLT 1, 3-8; Elizabeth E. Joh, 'Privacy Protests: Surveillance Evasion and Fourth Amendment Suspicion' (2013) 55 Arizona L Rev 997, 1013-1022.

ply *existing in society* – translate quite literally in an online world, especially if encryption is weakened. Without the protection of encryption, individuals may hesitate to exchange sensitive communications through online intermediaries if they know they are being, or could be, watched. Human expression is then confined within the space of what may be deemed to be acceptable in the eyes behind the lens of surveillance.

Encryption permits the creation of a safe space for users' right to privacy and freedom of expression and protects them from becoming vulnerable to unfettered surveillance and malicious or repressive actors. It preserves communicational privacy reflected in the ability to restrict access to communications,[144] intellectual privacy which is the freedom to develop ideas without being monitored,[145] and informational privacy resting on the elements of secrecy, anonymity and control.[146] The importance of encryption is therefore amplified in jurisdictions such as India where the surveillance regime lacks adequate checks and balances and exacerbates the power imbalance between the state and the people.[147]

India, the world's largest democracy, is also among the biggest surveillance states. In a 2019 report on surveillance states by a UK-based research firm, India was found to display a 'systemic failure to maintain safeguards' and was ranked third in a list of forty-seven countries, behind only Russia and China.[148] The Standard Operating Procedure followed by law enforcement agencies to surveil citizens demonstrates 'centralisation of power in

---

[144] (2017) 10 SCC 1 [141-142] [DY Chandrachud J]; *see*: 'UN: Online Anonymity, Encryption Protect Rights' (*Human Rights Watch*, 17 June 2005) <https://www.hrw.org/news/2015/06/17/un-online-anonymity-encryption-protect-rights> accessed 13 November 2020; 'Decrypting the Encryption Debate: A Framework for Decision Makers' (2018) National Academies of Sciences, Engineering, and Medicine Consensus Study Report, 32-39 <https://www.nap.edu/catalog/25010/decrypting-the-encryption-debate-a-framework-for-decision-makers> accessed 13 November 2020.

[145] Neil Richards, 'Intellectual Privacy' (2008) 87 Texas L Rev 387, 389.

[146] *Spencer v R* 2014 SCC OnLine Can SC 34 : (2014) 2 SCR 212 [38-47]; *K S Puttaswamy v Union of India* (2017) 10 SCC 1 [134] [DY Chandrachud J].

[147] 'India's Surveillance State' (2014) SLFC.in Surveillance Report <https://sflc.in/sites/default/files/wp-content/uploads/2014/09/SFLC-FINAL-SURVEILLANCE-REPORT.pdf> accessed 13 November 2020. This report provides a comprehensive overview of the enabling statutes, case law and principles in respect of communications surveillance in India. It concludes that surveillance is conducted on very broadly worded grounds, surveillance systems have large scale data-mining and profiling abilities and the public is kept in the dark because communications surveillance is in the exclusive domain of the executive branch. It recommends a review of legislative provisions that sanction and regulate surveillance with a focus on the right to privacy.

[148] Paul Bischoff, 'Data Privacy Laws & Government Surveillance by Country: Which Countries Best Protect their Citizens?' (*Comparitech*, 15 October 2019) <https://www.comparitech.com/blog/vpn-privacy/surveillance-states/> accessed 13 November 2020. Each country's report, sources, and scores can be found at <https://docs.google.

the hands of an opaque and unaccountable Union Executive'[149]. Extant laws fail to ensure accountability and limit the scope of surveillance operations cloaked in secrecy.[150] The statutory preconditions based on which surveillance may be conducted are extremely broadly worded[151] and the executive branch has unfettered discretion to authorise surveillance without any independent oversight.[152]

Human Rights

As communications increasingly take a digital form, there is growing recognition globally from the perspective of human rights that encryption is an essential element for a free and open internet because it supports free expression, access to information, anonymity, and privacy.[153] In allowing for uninhibited private communication, and protecting the confidentiality,

---

com/spreadsheets/d/1uPCfyzwT2b47oX0kcYg3kn3V4H6IWUikp4jMOVUWmJA/edit#gid=0>.

[149] 'Secret Operating Procedure for Digital Snooping Revealed. Confirms Fears of Centralisation of Executive Power, Zero Judicial Scrutiny and Oversight' (*Internet Freedom Foundation*, 11 March 2019) <https://internetfreedom.in/revealed-secret-operating-procedure-followed-by-the-govt-for-digital-snooping/> accessed 13 November 2020.

[150] ibid.

[151] S 69, IT Act empowers the government to direct an agency to 'intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information generated, transmitted, received or stored in any computer resource' if it is 'in the interest of the sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence'. Telephone tapping, under s 5(2), Indian Telegraph Act 1885, may be ordered on the 'occurrence of any public emergency' or 'in the interest of the public safety'. The grounds on which surveillance may be conducted are therefore extremely elastic and devoid of any meaningful limitations. Further extending this elastic scope, in December 2018, the central government issued a notification, pursuant to s 69 of the IT Act and Rule 4 of the Decryption Rules, authorizing ten security and intelligence agencies to engage in the interception, monitoring and decryption of information generated, transmitted, received or stored in any computer resource. Six petitions challenging this notification broadly on the ground that it violates the proportionality test laid down in *Puttaswamy* are currently pending before the Supreme Court. These are: (1) *Manohar Lal Sharma v Union of India* (WP (Crim) No 1 of 2019) (pending); (2) *Amit Sahni v Union of India* (WP(C) No 2 of 2019)(pending); (3) *Mahua Moitra v Union of India* (WP(C) No 916 of 2018)(pending); (4) *Internet Freedom Foundation v Union of India* (WP(C) No 44/2019) (pending); (5) *PUCL v Union of India* (WP(C) No 61 of 2019) (pending); and (6) *Shreya Singhal v Union of India* (WP(C) No 34 of 2019) (pending). The petition filed by the Internet Freedom Foundation, also challenges the constitutional validity of s 69, IT Act and the Decryption Rules.

[152] Vrinda Bhandari & Karan Lahiri, 'The Surveillance State, Privacy and Criminal Investigation in India: Possible Futures in a Post-Puttaswamy World' (2020) 3(2) Univ Oxford Human Rights Hub J 15, 46.

[153] Wolfgang Schulz & Joris van Hoboken, *Human Rights and Encryption* (United Nations Educational, Scientific and Cultural Organization 2016) 50-59; *Travel Guide to the Digital World: Encryption Policy for Human Rights Defenders* (Global Partners Digital 2017) 40-51.

integrity, and availability of data, encryption helps fulfil an important precondition for the freedom of communication.[154] It serves as a vital tool particularly for journalists, lawyers, activists, artists, and academics to carry out their profession and exercise human rights, and for persecuted minorities and dissidents in hostile political, social, religious, and legal environments.[155] Additionally, and crucially, it fosters meaningful inclusion and protects those disproportionately affected by online violence owing to intersectional[156] forms of discrimination based on factors such as gender identity and expression, abilities, age, sexual orientation, race, ethnicity, caste, religion, class, income, and urban and rural settings.[157]

In the report of the special rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye recommended strong protection for encryption and anonymity as they enable individuals to exercise the right to freedom of expression in the digital era.[158] He emphasized that individuals' right to access information 'regardless of frontiers,' as first guaranteed by Article 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, is being impeded by 'massive blocking, throttling, and filtering of the internet.'[159] The report categorically recommends that states should not restrict encryption and anonymity, avoid measures that weaken encryption, and refrain from making identification of users a condition for access to digital communications.[160] Subsequently, in 2017, in appreciation of the importance

---

[154] ibid.

[155] UNHRC, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression' (22 May 2015) A/HRC/29/32.

[156] Kimberle Crenshaw, 'Demarginalizing the Intersection of Race and Sex: A Black Feminist Critique of Antidiscrimination Doctrine, Feminist Theory, and Antiracist Politics' (1989) 1989(1) Univ Chicago L Forum 139. Herein, the legal scholar, Kimberle Crenshaw, first introduced the term 'intersectionality' in this paper. Intersectionality focuses on how different aspects of an individual's social and political identities such as race, gender and class interact and overlap to create varying modes of privilege and discrimination.

[157] UNHRC, 'Report of the Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective' (14 June 2018) A/HRC/38/47. In this report, the Special Rapporteur affirms that, '[e]ncryption and anonymity, separately or together, create a zone of privacy to protect freedom of expression and to facilitate the freedom to seek, receive and impart information and ideas, regardless of frontiers. Anonymity online is [sic] an important role for women and others at risk of discrimination and stigma, in that it allows them to seek information, find solidarity and support and share opinions without fear of being identified.' The report recommends that 'States should protect and encourage the development of technology, including of encryption and anonymity tools that protect the rights and security of women online'.

[158] UNHRC, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression' (22 May 2015) A/HRC/29/32.

[159] UHCHR, 'Human Rights, Encryption and Anonymity in a Digital Age' (1 July 2015)

[160] UNHRC, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression' (22 May 2015) A/HRC/29/32, at p. 20.

of encryption to freedom of expression, privacy and related human rights, the UN Human Rights Council adopted a resolution encouraging 'business enterprises to work towards enabling technical solutions to secure and protect the confidentiality of digital communications, which may include measures for encryption and anonymity.'[161]

As the exercise of human rights and freedoms finds an avenue for enhanced realization in digital spheres, so does their vulnerability to attack by hostile actors. Encryption and anonymity online are no longer ancillary to the rights to freedom of expression and privacy but rather central to the evolution and realization of these rights in any democratic society. States ought to therefore encourage the use of encryption without any restrictions.[162]

National Security

Globally,[163] as in India,[164] the debate on encryption is often framed as 'privacy versus security' with the implication that strengthening one necessarily

---

[161] UNHRC Res 34/7 (23 March 2017); UNHRC, 'Mandate of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression' (June 2018) Research Paper 1/2018.

[162] Some examples of best practices involving legislations that expressly protect the right to use encryption include the Law on Electronic Commerce in Luxembourg which says that '[t]he use of cryptographic techniques is free'; the Electronic Communications and Transactions Act, 2009 in Zambia which explicitly states that individuals may use encryption 'regardless of encryption algorithm selection, encryption key length chosen, or implementation technique or medium used'; and the Brazilian Civil Rights Framework for the Internet which guarantees the 'inviolability and confidentiality of [internet users'] stored private communications'.

[163] 'International Statement: End-To-End Encryption and Public Safety' (*Department of Justice*, 11 October 2020) <https://www.justice.gov/opa/pr/international-statement-end-end-encryption-and-public-safety> accessed 13 November 2020; 'Going Dark: Encryption, Technology, and the Balances between Public Safety and Privacy' (*Federal Bureau of Investigation*, 8 July 2015) <https://www.fbi.gov/news/testimony/going-dark-encryption-technology-and-the-balances-between-public-safety-and-privacy> accessed 13 November 2020; Derek E. Bambauer, 'Privacy Versus Security' (2013) 103(3) J Crim L & Criminology 667, 667-672; Morvillo Abramowitz Grand Iason & Anello PC, 'The International Encryption Debate: Privacy Versus Big Brother' (*Lexology*, 12 June 2019) <https://www.lexology.com/library/detail.aspx?g=41bce78b-f790-4901-ba88-7b9f6ffdd488> accessed 13 November 2020; Dave Weinstein, 'Privacy vs. Security: It's a False Dilemma' (*Wall Street Journal*, 6 October 2019) <https://www.wsj.com/articles/privacy-vs-security-its-a-false-dilemma-11570389477> accessed 13 November 2020.

[164] Bedavyasa Mohanty, 'The Encryption Debate in India' (2019) Carnegie Endowment for International Peace, 2 <https://carnegieendowment.org/files/WP_The_Encryption_Debate_in_India.pdf> accessed 12 November 2020; 'The Encryption Debate' (*The Hindu*, 28 March 2016) <https://www.thehindu.com/opinion/editorial/editorial-on-the-encryption-debate/article7681977.ece> accessed 13 November 2020; Varsha Rao, 'The Encryption Debate Between WhatsApp and the Indian Government' (*TechQuila*, 26 October 2019) <https://www.techquila.co.in/the-encryption-debate-between-whatsapp-and-the-indian-government/> accessed 13 November 2020.

means weakening the other. In fact, in the encryption context, the two principles reinforce each other.[165] A cyber infrastructure made more resilient with strong encryption significantly reduces the risk of data breaches and preserves both individual privacy and national security. Encryption protects critical infrastructure, classified information, transactions, trade secrets, and personal communications and data for the government and law enforcement agencies and for the general population. The necessary corollary is that weakening encryption jeopardises security as much as it threatens privacy. The vulnerabilities in the system, whether in the form of weak encryption or 'backdoors' for exceptional access, expose individuals, businesses, and states alike to attacks by malicious actors. As such, it has been argued that a more accurate framing of the debate would be 'security versus security.'[166]

Encryption is not a threat to security but rather an integral element of both information security and national security and it is imperative that government and law enforcement officials recognize this. The Parliamentary Committee of the Council of Europe offered a strong example when it passed a resolution in 2015 endorsing 'the European Parliament's call to promote the wide use of encryption and resist any attempts to weaken encryption and other Internet safety standards, not only in the interest of privacy, but also in the interest of threats against national security posed by rogue States, terrorists, cyberterrorists and ordinary criminals.'[167] Further, the European Data Protection Board recently recommended encryption as a necessary supplementary measure to preserve data flows from Europe to the U.S.[168] This is because U.S. law, according to the Court of Justice of the European Union, provides an inadequate level of protection,[169] so encrypting data is necessary

---

[165] 'Policy Brief: Encryption' (*Internet Society*, 9 June 2016) <https://www.internetsociety.org/policybriefs/encryption/> accessed 13 November 2020; Elaine Lammert, 'Security and Privacy are Not Mutually Exclusive' (*The Cipher Brief*, 17 March 2016) <https://www.thecipherbrief.com/column_article/security-and-privacy-are-not-mutually-exclusive> accessed 13 November 2020; Encryption Working Group, 'Moving the Encryption Policy Conversation Forward' (*Carnegie Endowment for International Peace*, 10 September 2019) <https://carnegieendowment.org/2019/09/10/moving-encryption-policy-conversation-forward-pub-79573> accessed 13 November 2020.

[166] House Committee on Homeland Security, *Going Dark, Going Forward: A Primer on the Encryption Debate* (Congress 2016) 6; *Travel Guide to the Digital World: Encryption Policy for Human Rights Defenders* (Global Partners Digital 2017) 26-27.

[167] Parliamentary Assembly of the Council of Europe, *Mass Surveillance* (Resolution 2045, 2015) para 17.

[168] European Data Protection Board, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (Adopted on 10 November 2020) <https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf> accessed 25 November 2020.

[169] Judgment in Case C-311/18, *Data Protection Commissioner v Facebook Ireland and Maximillian Schrems*

to preclude access by U.S. intelligence agencies under those lax surveillance standards.

Similarly, in the U.S., amidst attempts to weaken encryption by the U.S. Government,[170] a former head of the National Security Agency explained that encryption boosts national security: 'American security is better served with unbreakable end-to-end encryption than it would be served with one or another front door, backdoor, side door, however you want to describe it.'[171] In India too, certain security officials have rightly expressed strong support for encryption to ensure security. A veteran of the Indian intelligence community who has worked extensively on counter-terrorism measures said in a recent interview: 'Encryption not only protects you, it makes you stable as a system […] 68% of our cybersecurity share is the government – it is the IT-enabled sector which is critical. Look at Aadhar, look at our banking. You have to make this system secure, you have to make this system safe. And how do you do it? You have to do it with encryption.'[172]

In the Indian context, encryption should be seen as an enabler not just of individual privacy and the economy but also of national security. Weakening privacy by threatening encryption weakens national security.[173] Cybersecurity incidents in which confidentiality of data is put at risk are increasing.[174]

---

[170] *In re Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus* IS300 at 2, No. ED 15-0451M, 2016 WL 680288, at *2 (CD Cal 2016); Eliminating Abusive and Rampant Neglect of Interactive Technologies Act 2020 ('EARN IT'); Lawful Access to Encrypted Data Act ('LAED').

[171] Paul Szoldra, 'Ex-NSA Chief Thinks the Government is Dead Wrong in Asking Apple for A Backdoor' (*Business Insider*, 26 February 2016) <https://www.businessinsider.in/enterprise/security/Ex-NSA-chief-thinks-the-government-is-dead-wrong-in-asking-Apple-for-a-backdoor/articleshow/51149769.cms> accessed 13 November 2020.

[172] News 18, 'Former IPS Officer & CIC Mr Yashovardhan Azad on #DataProtectionAuthority' (9 October 2020) <https://www.facebook.com/cnnnews18/videos/858538681550688/> accessed 13 November 2020. Yashovardhan Azad added that '[…] I think that encryption is perhaps the most important methodology today to protect our interests and for data protection… there is no doubt that encryption is very important for security, in fact that is the way to go forward. Giving backdoor rooms to security agencies can lead to a lot of problems. On the other hand breaking the entire encryption system is another problem because it makes you more vulnerable. End-to-end encryption should be there because it is for the safety of the consumer, for data protection'. He advocates for a strong data protection legislation governing access to data that prioritizes consent and establishes an independent data protection authority.

[173] Apar Gupta, 'Why there cannot be any National Security without Individual Privacy' (*Hindustan Times*, 4 November 2019) <https://www.hindustantimes.com/analysis/why-there-cannot-be-any-national-security-without-individual-privacy-analysis/story-JvDaOJLW85gXR9cILtwq7M.html> accessed 13 November 2020.

[174] The Indian Computer Emergency Response Team (CERT-In), the government agency responsible for tracking and responding to cybersecurity threats, reported that it handled over 3.94 lakh (394,000) incidents in 2019 alone, *see*: PTI, '3.94 lakh cybersecurity incidents reported to CERT-In in 2019: Dhotre' (*Business Insider*, 5 February 2020) <https://

Significant data breaches have occurred, including one which revealed that targeted users, including activists, journalists, and senior government officials, were being spied on through the compromise of encrypted messaging apps on their cell phones.[175] Thousands of important individuals were allegedly tracked through another data breach, including the President and the Prime Minister of India and several other ministers, business persons, and journalists.[176] These incidents ought to provide impetus to the recognition that encryption aids security, significantly mitigates the risk of a breach by preventing the attacker from accessing the sensitive data,[177] and must therefore be encouraged rather than restricted. As Apar Gupta, the Executive Director of the Internet Freedom Foundation puts it, '[w]e must all recognise that national security starts with securing the smartphones of every single Indian by embracing technologies such as encryption rather than deploying spyware. This is a core part of our fundamental right to privacy.'[178]

Thus, arguments for undermining encryption that represent privacy and national security as mutually exclusive goals should be recognized and rejected for the false binary on which they are based. The bottom line is that encryption protects the nation, its security, and its government officials as much as it protects the individual citizen.

---

www.businessinsider.in/business/news/3-94-lakh-cybersecurity-incidents-reported-to-cert-in-in-2019-dhotre/articleshow/73961329.cms> accessed 13 November 2020.

[175] Apar Gupta, 'Why there cannot be any National Security without Individual Privacy' (*Hindustan Times*, 4 November 2019) <https://www.hindustantimes.com/analysis/why-there-cannot-be-any-national-security-without-individual-privacy-analysis/story-JvDaOJLW85gXR9cILtwq7M.html> accessed 13 November 2020; FP Staff, 'WhatsApp claims it informed authorities about vulnerability in May 2019; govt sources say advisory full of 'Technical Jargon' (*First Post*, 2 November 2019) <https://www.firstpost.com/india/whatsapp-claims-it-informed-centre-about-vulnerability-in-may-2019-govt-sources-say-advisory-full-of-technical-jargon-7587621.html> accessed 13 November 2020. The Pegasus spyware exploited a vulnerability in the system and was able to illegally access a phone's camera and microphone, read messages and record keystrokes. The spyware could thus compromise the data at rest on the phone.

[176] Express Web Desk, 'Chinese firm Tracking Influential Indians also Harvested Data of over 50,000 Americans' (*The Indian Express*, 14 September 2020) <https://indianexpress.com/article/world/china-data-harvest-australia-india-zhenhua-data-information-technology-6595217/> accessed 13 November 2020; ET Online, 'Zhenhua Data leak: From Narendra Modi to Ratan Tata, here's the List of Prominent Indians China Spied on' (*The Economic Times*, 14 September 2020) <https://economictimes.indiatimes.com/news/defence/zhenhua-data-leak-from-narendra-modi-to-ratan-tata-heres-list-of-prominent-indians-china-spied-on/articleshow/78107743.cms?from=mdr> accessed 13 November 2020

[177] 'Encryption is a Critical Safeguard against Data Breaches' (*BSA*) <https://www.bsa.org/files/policy-filings/BSA_Encrypt_DataBreach-web.pdf> accessed 13 November 2020.

[178] Apar Gupta, 'Why there cannot be any National Security without Individual Privacy' (*Hindustan Times*, 4 November 2019) <https://www.hindustantimes.com/analysis/why-there-cannot-be-any-national-security-without-individual-privacy-analysis/story-JvDaOJLW85gXR9cILtwq7M.html> accessed 13 November 2020.

The Economic Justification

Encryption offers notable advantages to both industry and society by ensuring that transactions, communications, and industrial secrets remain safe in the virtual space. Many companies believe that the increasing demand for information security means that strict limitations on the use of encryption would result in significant financial losses as well as a steep decline in employment opportunities.[179] India is one of the largest offshoring destinations for several IT companies around the world.[180] The Indian IT industry contributed almost 8% of the country's overall GDP in 2017 and in 2019, it generated an annual revenue of approximately 180 billion USD.[181] This key sector of the Indian economy could face serious setbacks if encryption is weakened as the resulting reduction in security would diminish the willingness of IT companies to outsource work to India and hurt India's reputation as a preferred IT hub.

Laws that weaken encryption can have a substantial negative impact on a country's economy. Australian legislation[182] requiring designated telecommunication service providers to give law enforcement agencies access to decrypted communication, and requiring them to build a decryption capability if they did not already have it, had a material and detrimental impact on the market. The 'perceived compliance burden' led to multinational companies blacklisting the Australian market and moving physical, operational, and legal jurisdiction offshore.[183] Further, restrictions on encryption damage

---

[179] Charles L. Evans, 'U.S. Export Control of Encryption Software: Efforts to Protect National Security Threaten the U.S. Software Industry's Ability to Compete in Foreign Markets' (1994) 19(3) North Carolina J Intl L & Comm Reg 469, 470; Chris Duckett, 'Home Affairs Attempts to Allay Concerns about Australian Exporters for Encryption-Busting Bill' (*Zdnet*, 26 November 2018) <https://www.zdnet.com/article/home-affairs-attempts-to-allay-concerns-of-australian-exporters-about-encryption-busting-bill/> accessed 14 November 2020.

[180] Shanglio Sun, 'Contribution of Indian IT-BPM Industry in GDP of India FY 2009-2020' (*Statistica*, 17 February 2021)https://www.statista.com/statistics/320776/contribution-of-indian-it-industry-to-india-s-gdp/accessed 14 November 2020.

[181] Shanglio Sun, 'IT Industry in India – Statistics & Facts' (*Statistica,* 12 August, 2021)<https://www.statista.com/topics/2256/it-industry-in-india/>accessed 14 November 2020.

[182] The Telecommunications and other Legislation Amendment (Assistance and Access) Act 2018.

[183] Asha Barbaschow, 'Home Affairs says no Problems with Encryption Laws even though Local Companies Suffer' (*Zdnet*, 5 July 2019) <https://www.zdnet.com/article/home-affairs-says-no-problems-with-encryption-laws-even-though-local-companies-suffer/> accessed 14 November 2020; Chris Duckett, 'Encryption Laws are Creating an Exodus of Data from Australia: Vault' (*Zdnet*, 5 July 2019) <https://www.zdnet.com/article/encryption-laws-are-creating-an-exodus-of-data-from-australia-vault/> accessed 14 November 2020.

innovation and economic growth stemming from the export of encryption technologies.[184]

The Organization for Economic Cooperation and Development (OECD) recognizes that the absence of cryptography is detrimental to privacy, national security, business, and electronic commerce. It makes data and communications vulnerable to unauthorized use and negatively impacts users' trust in information and communications systems, networks, and infrastructures. Therefore, OECD's Guidelines for Cryptography Policy recommend that '[t]he fundamental rights of individuals to privacy, including secrecy of communications and protection of personal data, should be respected in national cryptography policies and in the implementation and use of cryptographic methods.'[185]

Further, encryption benefits commerce by significantly reducing the cost of data breaches. According to a 2020 report by IBM,[186] the average cost of a data breach around the world was approximately ₹28.5 crore ($3.86 million USD). In India, data breaches cost organizations ₹14 crore ($1.9 million USD) on an average between August 2019 and April 2020.[187] The IBM report found that extensive encryption is a cost mitigating factor, decreasing the average total cost of a data breach by more than ₹1.7 crore ($237,176 USD). The findings also reflect that 52% of data breaches were caused by malicious attacks – the most expensive of the root causes as compared to

---

[184] Sinita Radu, 'Restricting Encryption will Hurt Security and Economy, Won't Stop Terrorists from Using it Anyway' (*ITIF*, 14 March 2016) <https://itif.org/publications/2016/03/14/restricting-encryption-will-hurt-security-and-economy-won't-stop-terrorists> accessed 14 November 2020; Simrit Chhabra, Renjini Rajagopalan, & Vatsal Khullar, 'Framework for Regulating Encryption in India' (2019) The Quantum Hub Report, 6-9 <https://thequantumhub.com/wp-content/uploads/2020/08/Regulation-of-Encryption-TQH-Updated-08Apr19-Final.pdf> accessed 14 November 2020; Mohamad Ali, 'Backdoor Government Decryption Hurts My Business and Yours' (*Harvard Business Review*, 15 September 2016) <https://hbr.org/2016/09/backdoor-government-decryption-hurts-my-business-and-yours> accessed 14 November 2020.

[185] 'Recommendation of the Council concerning Guidelines for Cryptography Policy' (1997) Organization for Economic Cooperation and Development Legal Instrument/0289, 10 <https://dig.watch/sites/default/files/OECD%20Guidelines%20for%20Cryptography%20Policy.pdf> accessed 14 November 2020.

[186] 'Cost of a Data Breach Report' (2020) *IBM Security Report*, 5 <https://www.capita.com/sites/g/files/nginej146/files/2020-08/Ponemon-Global-Cost-of-Data-Breach-Study-2020.pdf> accessed 14 November 2020.

[187] PTI, 'Organisations in India Lost ₹14 Crore on Average to Data Breaches: IBM' (*LiveMint*, 29 July 2020) <https://www.livemint.com/companies/news/organisations-in-india-lost-rs-14-crore-on-average-to-data-breaches-ibm-11596001410186.html> accessed 14 November 2020.

system glitches and human errors[188] – the risks of which can be mitigated by encryption.

The New Intermediary Guidelines will have a debilitating impact on Indian companies, and especially start-ups. India is poised to become a global leader in the global digital economy. However, this potential rests on the ability of companies to inspire consumers' trust in their products which would be negatively impacted as companies are compelled to opt for weak encryption or not make it available at all. Such lack of trust in the global market will result in consumers outside India opting for products and services of competitors from other countries,[189] or a duality of services offered by companies with the Indian user base having access to the version that is less secure. With respect to start-ups, a study on the economic impact of safe harbours on Internet intermediary start-ups in 2015[190] revealed that an intermediary liability regime with clearly defined and low-cost compliance requirements could increase start-up success rates for intermediaries by more than 20% in India. Implementing such a regime, as opposed to the one in the New Intermediary Guidelines, would also increase the expected profit for successful start-up intermediaries by 5% in India.

Conclusion

Regulatory frameworks that would have the effect of compromising encryption, including the traceability mandate, are advanced to address grave problems such as 'fake news',[191] child sexual abuse material,[192] and offences

---

[188] 'Cost of a Data Breach Report' (2020) *IBM Security Report*, 5 <https://www.capita.com/sites/g/files/nginej146/files/2020-08/Ponemon-Global-Cost-of-Data-Breach-Study-2020.pdf> accessed 14 November 2020.

[189] Soumyarendra Barik, 'Proposed Changes to Intermediary Guidelines will Put Digital India's Future at Risk: ISOC' (*Medianama,* 9 January 2020) <https://www.medianama.com/2020/01/223-isoc-intermediary-guidelines-letter/> accessed 14 November 2020.

[190] Oxera, 'The Economic Impact of Safe Harbours on Internet Intermediary Start-Ups' (2015) <https://www.oxera.com/wp-content/uploads/2018/07/The-economic-impact-of-safe-harbours-on-Internet-intermediary-start-ups.pdf.pdf> accessed 14 November 2020.

[191] Julie Posetti, Cherilyn Ireton, et al, *Journalism, Fake News & Disinformation: Handbook for Journalism Education and Training* (UNESCO 2018) 'Fake news' is an umbrella term for misinformation and disinformation. ''Misinformation' is information that is false, but the person who is disseminating it believes that it is true.'; ''Disinformation' is information that is false, and the person who is disseminating it knows it is false. It is a deliberate, intentional lie, and points to people being actively disinformed by malicious actors.' The traceability mandate in India's New Intermediary Guidelines and in initial drafts of the pending Brazilian Internet Freedom, Responsibility and Transparency Act, colloquially referred to as the 'Fake News Bill', received impetus from aim of curbing dis/mis-information.

[192] In 2020, the U.S. Senate Judiciary Committee unanimously approved S. 3398, the EARN IT Act of 2020, which was aimed at ending the spread of online child sexual abuse material. The bill compromised the ability of social media platforms to offer end-to-end encryption

relating to national security, public order, and sexually explicit material.[193] Such purposes lend legitimacy and urgency to the proposals. However, proposals that have the effect of breaking encryption with the purported aim of achieving any such objective are richer in rhetoric than in practice. Not only does undermining encryption fail as a solution to any of these problems, but it also has the opposite effect of negatively impacting the public interest, human rights, cybersecurity, and the economy.

The online sphere is no longer an adjunct to the offline realities of society. Instead, we live our social and political lives online. It is where we exercise our rights and freedoms. Encryption makes it possible for individuals, communities, and governments to have a private space online, secure from known and unknown threats of surveillance and manipulation. Individuals can communicate and collaborate with each other, and build a democratic society that is strengthened, and not marred, by the ubiquity of the digital dimension. Preserving and strengthening encryption is in the interest of the defining ideals of a democracy - the right to privacy and the right to freedom of expression.

What Carissa Véliz of Oxford University observes in the context of privacy is equally applicable with respect to encryption and its impact on both privacy and security: '[s]ocietal choices about privacy will influence how political campaigns are run, how corporations earn their keep, the power that governments and private businesses may wield, the advancement of medicine, the pursuit of public health goals, the risks we are exposed to, how

---

to their users by threatening platforms with liability if their users conveyed CSAM. Maintaining liability protection could have effectively required platforms to be able to understand the communications content they carried, which is inconsistent with EE2E. *See*: Nandita Bose, 'US Senate Committee Approves Anti-Child Porn Bill After Addressing Google, Facebook Encryption Concerns' (*Reuters*, 2 July 2020) <https://in.reuters.com/article/us-usa-legislation-encryption/us-senate-committee-approves-anti-child-porn-bill-after-addressing-google-facebook-encryption-concerns-idINKBN2432NK> accessed 14 November 2020; a 14-member ad-hoc committee of the Rajya Sabha, led by Jairam Ramesh, recommended that law enforcement agencies should be permitted to break end-to-end encryption to trace the distributor of child pornography on social media, *see*: Neha Alawadhi, 'RS Panel Suggests Breaking Encryption to Curb Child Pornograhy Distribution' (*Business Standard*, 27 January 2020) <https://www.business-standard.com/article/technology/rs-panel-suggests-breaking-encryption-to-curb-child-pornograhy-distribution-120012600705_1.html> accessed 14 November 2020.

[193] New Intermediary Guidelines, rule 4(2); To promote national security and law enforcement interests in the U.S., Senators introduced the Lawful Access To Encrypted Data Act, S. 4051, which would have forbidden providers from offering end-to-end encryption in online services and devices unless it could be circumvented by law enforcement, *see*: Riana Pfefferkorn, 'There's now an Even Worse Anti-Encryption Bill than Earn it. That doesn't Make the Earn it Bill ok' (*The Center for Internet and Society, Stanford Law School*, 24 June 2020) <https://cyberlaw.stanford.edu/blog/2020/06/there's-now-even-worse-anti-encryption-bill-earn-it-doesn't-make-earn-it-bill-ok> accessed 14 November 2020.

we interact with each other, and not least, whether our rights are respected as we go about our daily lives.'[194] The future of the rights and freedoms that make India a thriving democracy will be informed in no small part by the government's approach to encryption. The only way forward, if the goal is to boost technology innovation and economic growth, protect individual rights and freedoms, and secure cyberspaces for the nation and the government, is to support and encourage strong encryption. The societal costs of having diluted encryption standards are, simply put, too high.

[194] Carissa Véliz, *Privacy is Power: Why and How You Should Take Back Control of Your Data* (Bantam Press 2020).

Recommender Systems and Autonomy: A Role for Regulation of Design, Rights, and Transparency

Christian Djeffal[*], *Christina Hitrova*[**] *& Eduardo Magrani*[***]

Abstract *Recommender systems are now widely deployed across multiple dimensions of the digital reality that increasingly shapes our lives. In doing so, they mould individual thoughts and actions and can affect individual and collective autonomy. In this paper we first discuss how the ubiquitous exercise of 'soft' power by recommender systems on individual users presents interference into individual autonomy and its legal dimensions, expressed through collective and individual self-determination, democratic values and institutions, as well as individual human rights and freedoms. We then argue that this exercise of power over individual and collective destinies necessitates regulatory action to establish an appropriate system of checks and balances on recommender systems and their creators. Utilising a bottom-up approach, we look at the fundamental aspects of a recommender system's design and functioning that shape the impact these algorithms have on individual autonomy. On the basis of this, we identify three key areas where regulation can be targeted in order to empower users and address current power imbalances - (1) algorithmic design, (2) data protection rights, and (3) transparency and oversight. We map the key questions and options for future regulatory action in each of these domains, highlighting the decisions and competing interests that regulators will need to consider. We conclude by discussing the policy implications of this mapping of the debate and the relevance they have for the future of recommender systems regulation.*

[*] Christian Djeffal is Assistant Professor for Law, Science and Technology at the Technical University of Munich. He researches and lectures on the relationship between law and digital technology.

[**] Christina Hitrova works on Responsible AI with PricewaterhouseCoopers (Czech Republic) and previously researched and consulted stakeholders on the links between law, ethics and technology at the Technical University of Munich and The Alan Turing Institute.

[***] Eduardo Magrani is a Doctor of Laws and an Affiliate at the Berkman Klein Center for Internet & Society at Harvard University. He is also the President of the National Institute for Data Protection in Brazil and Partner at Demarest Advogados.

We would like to acknowledge the help of our research assistants Daan Herpers and Shivangi Mishra.

I. Introduction

As the amount of information uploaded to the Internet has continued to grow, exploring content without any sort of structure or guidance has become overwhelming, possibly even impossible. Every second 6 new websites are published, 1,099 posts are shared on Instagram, 4,050 photos are uploaded to Facebook and 5,787 tweets are posted on Twitter. These numbers increase every second.[1] Mirroring this explosion, recommender systems ('RS') have quickly become ubiquitous and are currently used to personalise content choices and rankings across platforms and apps. RS are algorithms that curate — what they identify as — relevant information by tailoring it to individual users through data processing techniques. RS are used to recommend friends or content on social media, but they can just as easily

[1] Spectralplex, 'How Much Content is Uploaded to the Internet Per Second?' (*Spectralplex*) <https://spectralplex.com/how-much-content-is-uploaded-to-the-internet-per-second/> accessed 25 March 2021.

be used to suggest tailored diets or exercises in weight loss apps or present options for travel routes on the basis of traffic density information. Behind the scenes, RS are also used in targeted and behavioural advertising — the engine of dominant Internet business models. The profiling and user tracking needed for personalisation have been criticised due to the privacy intrusions that they give rise to. In this article, however, we argue that the impact of RS goes far beyond such privacy concerns. Instead, the suggestive power of 'recommendations' based on individual thoughts and actions can impact individual autonomy and, by extension, human rights as well as individual and collective self-determination.

Through their functioning, RS increasingly shape our experience in a virtual environment[2] and thanks to machine learning ('ML') and the increasing collection of personal data, these algorithms can now enable granular and persuasive micro targeting. This brings about tangible shifts in our thoughts and actions or, stated otherwise, autonomy. Individuals' choices could be affected by RS determining the content or options visible to them.[3] Individuals can also be influenced by the order in which information is presented;[4] we prioritise those items that are ranked higher on a list.[5] By doing this in the absence of conscious awareness and individual choice regarding how content is targeted at them, recommendations may disrupt an individual's capacity of self-determination. A recent, notorious example of the impact RS can have on individual autonomy, thoughts and actions, is that of Molly Russel. Molly was a fourteen-year-old schoolgirl who took her own life in November 2017, days before her fifteenth birthday. After her death, Ian Russel, her father, publicly blamed Big Tech, in particular Instagram, for his daughter's death.[6]

---

2 Silvia Milano, Mariarosaria Taddeo and Luciano Floridi, 'Recommender Systems and their Ethical Challenges' (2020) 35 AI & Society 957.

3 Christine Clavien, 'Ethics of Nudges: A General Framework with a Focus on Shared Preference Justifications' (2018) 47 Journal of Moral Education 366.

4 Andreas Hellmann, Chiing Yeow and Lurion De Mello, 'The Influence of Textual Presentation Order and Graphical Presentation on the Judgements of Non-Professional Investors' (2017) 47 Accounting and Business Research 455; Buck KW Pei, Philip MJ Reckers and Robert W Wyndelts, 'The Influence of Information Presentation Order on Professional Tax Judgment' (1990) 11 Journal of Economic Psychology 119; Michael Eisenberg and Carol Barry, 'Order Effects: A Study of the Possible Influence of Presentation Order on User Judgments of Document Relevance' (1988) Journal of the American Society for Information Science 8.

5 Mark T Keane, Maeve O'Brien and Barry Smyth, 'Are People Biased in Their Use of Search Engines?' (2008) 51 Communications of the ACM 49; Jonah Berger, 'Does Presentation Order Impact Choice After Delay?' (2016) 8 Topics in Cognitive Science 670.

6 Jacob Dirnhuber, 'Heartbroken Dad Claims Instagram 'helped to Kill His 14-Year-Old Daughter' Who took her Own Life after Viewing Suicide Posts' *The Sun* (22 January 2019) <https://www.thesun.co.uk/news/8258105/ian-russell-molly-instagram-killed-daughter/> accessed 31 March 2021.

After Molly's death, Mr. Russel found out that his daughter's Instagram newsfeed was full of suicidal posts. In his own words:[7]

> I think Molly probably found herself becoming depressed. She was always very self-sufficient and liked to find her own answers. I think she looked towards the internet to give her support and help. She may well have received support and help, but what she also found was a dark, bleak world of content that accelerated her towards more such content.

Mr. Russel alleged that Instagram's algorithms, by targeting content at Molly, ended up pushing her into that "dark rabbit hole of depressive suicidal content."[8] This case illustrates a broader phenomenon of social media influences and content curation that affect individual's physical and mental health,[9] and not just of children. Depending on their field of application, RS could also affect the rights of users, e.g., if used in news media or in healthcare. RS that prioritises some news or publications at the expense of others could be softly limiting the right of readers to access information or of writers to express their opinions and impart information. RS in health apps, by providing suggestions for exercise or diet, could directly play a role in the health of their users, thus affecting their right to health. The causal relationship between RS and particular outcomes for their users is soft but extant. Yet, assessing the power and influence RS have in a triangular relationship is trickier, e.g., situations where a RS shapes the information served to a user and it is the actions of that user that then go on to produce rights-impacting effects. For example, a RS used by a doctor could suggest a particular treatment for a patient, but it is the actions of the doctor that would ultimately determine what treatment is provided. Or, more controversially, a RS could present content against a particular protected demographic group (e.g., religious, racial, etc.) to people already demonstrating bigoted beliefs, and can, thus, encourage a view of the world that could potentially push them towards committing violence against members of those racial or religious groups. Dissecting the causal role of RS in such triangular relationships is complex and most likely does not meet the legal standard of causation in

---

[7] Press Association, 'Molly Russell Entered "Dark Rabbit Hole of Suicidal Content" Online, Says Father' *Evening Express* (17 January 2020) <https://www.eveningexpress.co.uk/news/molly-russell-entered-dark-rabbit-hole-of-suicidal-content-online-says-father-2/> accessed 31 March 2021.

[8] ibid.

[9] Faith Ridler, 'Now 30 Families Blame Social Media Firms for Their Roles in Children's Suicides' *Mail Online* (27 January 2019) <https://www.dailymail.co.uk/news/article-6636807/Now-30-families-blame-social-media-firms-roles-childrens-suicides.html> accessed 31 March 2021.

most jurisdictions. Nevertheless, it is clear that RS play a significant role in shaping the perceptions, and thus scope for autonomy of their users.

The persuasive strength of the impact of RS on autonomy may range, at its most innocent, from small nudges to premeditated and targeted manipulation of information and individuals.[10] Nudging is the design of choice architecture that pushes individuals towards a predictable and desirable behaviour without explicitly limiting freedom of choice.[11] Instead, it does so by relying on "cognitive boundaries, biases, routines, and habits."[12] Even if not directly limiting choices, a choice architecture might interfere with the ability of a person to identify and consider their options and, thus, affects their agency.[13] The use of personal information can enhance the effectiveness of recommendations, increasing the 'controlling' power of influences on the individual, threatening autonomy.[14] In the digital realm, creating architectures that affect individual choices may be unavoidable; for example, there must be a choice of layout and user interface.[15] Some have highlighted that careful considerations are needed when acting as a 'digital choice architect,' due to the great impact such decisions have on user actions.[16] In a digital setting, people are more likely to act automatically or intuitively,[17] with decreased attention span and concentration,[18] while being increasingly distracted and multitasking.[19] Moreover, the digital environment offers a wealth of tools

---

[10] Daniel Susser, Beate Roessler and Helen Nissenbaum, 'Technology, Autonomy, and Manipulation' (2019) 8 Internet Policy Review <https://policyreview.info/node/1410> accessed 5 March 2021.

[11] Richard H Thaler and Cass R Sunstein, *Nudge: Improving Decisions about Health, Wealth, and Happiness* (Rev and expanded ed, Penguin Books 2009).

[12] Pelle Guldborg Hansen, 'The Definition of Nudge and Libertarian Paternalism: Does the Hand Fit the Glove?' (2016) 7 European Journal of Risk Regulation 155.

[13] JS Blumenthal-Barby, 'Choice Architecture: A Mechanism for Improving Decisions While Preserving Liberty?' in Christian Coons and Michael Weber (eds), *Paternalism: Theory and Practice* (Cambridge University Press 2013).

[14] Susser, Roessler and Nissenbaum (n 10) 3.

[15] Daniel M Hausman and Brynn Welch, 'Debate: To Nudge or Not to Nudge*' (2010) 18 Journal of Political Philosophy 123, 124; Tobias Mirsch, Christiane Lehrer and Reinhard Jung, 'Digital Nudging: Altering User Behavior in Digital Environments', *Proceedings der 13. Internationalen Tagung Wirtschaftsinformatik (WI 2017)* (2017) <https://wi2017.ch/images/wi2017-0370.pdf> accessed 5 March 2021; Cass R Sunstein and Richard H Thaler, '"Preferences, Paternalism, and Liberty"' (2006) 59 Royal Institute of Philosophy Supplement 233, 250.

[16] Tim-Benjamin Lembcke and others, 'To Nudge or Not to Nudge: Ethical Considerations of Digital Nudging Based on Its Behavioral Economics Roots' 18, 10.

[17] Shlomo Benartzi and Jonah Lehrer, *The Smarter Screen: Surprising Ways to Influence and Improve Online Behavior* (2015).

[18] Ziming Liu, 'Reading Behavior in the Digital Environment: Changes in Reading Behavior over the Past Ten Years' (2005) 61 Journal of Documentation 700.

[19] Kep Kee Loh and Ryota Kanai, 'How Has the Internet Reshaped Human Cognition?' (2016) 22 The Neuroscientist 506.

and options at the disposal of creators and designers, along with the ability to micro-target and personalise content which may increase the effectiveness of nudges.[20] Even when users are aware of the role that algorithms play in online settings, they remain confident about their own autonomy and do not account for how they might be influenced.[21] In fact, knowing that information, e.g. advertisement, is targeted specifically to us might even change the way we view ourselves and the qualities that we associate with ourselves.[22] All of this suggests that individuals may be more vulnerable to decision-making errors in the digital realm both due to traditionally studied biases, as well as due to digital-specific and visual biases.[23]

Despite their potential far-reaching impact, until now RS have operated with little regulation to ensure checks and balances on their influence. Their name – 'recommender systems' – leaves the impression that their impact on human lives is soft and superficial. However, their influence could be described as analogous to Nye's concept of soft power in international relations – "the ability to affect others to obtain the outcomes one wants through attraction rather than coercion or payment."[24] By shaping our attention, RS attract us to one action or another. In some circumstances, the effects of this attraction can be equated with a *de facto* force, as seen in the Molly Russel case.

However, this lack of regulatory framework is changing. There have been indications that regulating RS has been on the minds of policy-makers in Europe. In November 2021, the European Commission proposed an AI Regulation ('the (draft) AI Act')[25] that seeks to establish common *ex ante* market requirements and *ex post* control measures on AI systems to ensure their safety and trustworthiness. The AI Act includes software that generates influential recommendations in its definition of AI[26] and goes on to explicitly prohibit AI systems that use "subliminal techniques beyond a person's

---

[20] Lembcke and others (n 16) 8.

[21] Leyla Dogruel, Dominique Facciorusso and Birgit Stark, '"I'm Still the Master of the Machine." Internet Users' Awareness of Algorithmic Decision-Making and Their Perception of Its Effect on Their Autonomy' (2020) Information, Communication & Society 1.

[22] Christopher A Summers, Robert W Smith and Rebecca Walker Reczek, 'An Audience of One: Behaviorally Targeted Ads as Implied Social Labels' (2016) 43 Journal of Consumer Research 156.

[23] Lembcke and others (n 16) 8.

[24] Joseph S Nye, 'Public Diplomacy and Soft Power' (2008) 616 The ANNALS of the American Academy of Political and Social Science 94, 94.

[25] Commission, "Proposal for a Regulation of the European Parliament and of the Council Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts" COM (2021) 206 final.

[26] AI Act, art 3(1).

consciousness."[27] It also prohibits systems that exploit "vulnerabilities of a specific group of persons due to their age, physical or mental disability"[28] in order to "materially distort a person's behaviour" in a way that causes or is likely to result in physical or psychological harm to that person or others. This prohibition seems to echo the dangers demonstrated by the Molly Russell case. In December 2021, the EU Digital Services Act ('DSA') was proposed.[29] The DSA also pays special attention to RS, particularly as used by very large online platforms and in advertising, and provides for multiple pathways to enhance their transparency to end users, external auditors, and the general public.[30] The DSA also recognises the systemic risk that could arise from RS and imposes risk assessment and management obligations on very large platforms. The risks of disseminating illegal content, negative effects on the exercise of fundamental rights, including freedom of expression and information, and the automated misuse and manipulation of their services with the goal of affecting democratic processes and civic discourse were specifically highlighted.[31] Even though the DSA continues to develop, the European Parliament rapporteur and the Council have expressed a desire to further reinforce transparency and user control over RS, obligations on large platforms, search engines, and online market places.[32] In the same vein, in January 2022, the Cybersecurity Administration of China also published a set of regulations intended to regulate RS, pushing for greater user control, limits on what data the systems can use, as well as more transparency of how they function.[33]

What is clear from these recent legislative developments is that there is a movement towards tackling the challenges that RS have given rise to - whether it is manipulation, behavioural change, fundamental rights impacts, or whether it is a larger scale impact on democratic processes and civic discourse, which affect collective self-determination. As these legislative

---

27 AI Act, art 5(1)(a).

28 AI Act, art 5(1)(b).

29 Commission, 'Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act)' and amending Directive 2000/31/EC, COM(2020) 825 final. (European Commission 2020) <https://eur-lex.europa.eu/legal-content/en/TXT/?qid=1608117147218&uri=COM%3A 2020%3A825%3AFIN> accessed 30 March 2021.

30 Digital Services Act (DSA), arts 29, 30.

31 DSA, arts 26, 27.

32 'Legislative Train Schedule - Proposal for a Regulation of the European Parliament and the Council on a Single Market for Digital Services (Digital Services Act) and Amending Directive 2000/31/EC / After 2020-09' (*European Parliament*, 17 December 2021) <https://www.europarl.europa.eu/legislative-train> accessed 15 January 2022.

33 Arendse Huld, 'China Passes Sweeping Recommendation Algorithm Regulations' (*China Briefing News*, 6 January 2022) <https://www.china-briefing.com/news/china-passes-sweeping-recommendation-algorithm-regulations/> accessed 15 January 2022.

processes evolve, we will observe how interests intertwined in this topic are to be balanced against each other.

With this article we would like to contribute to this debate. We focus on the perspective of individual users of RS, excluding from our analysis triangular situations where RS support decisions made by users regarding other individuals, and explore, from a European legal perspective, what role regulation does and can play in empowering individual users and safeguarding individual autonomy. We direct our analysis to future regulatory directions along the axes of shaping user-centric RS design, enabling user control through a data protection rights-based approach, and facilitating informed decision-making and accountability through comprehensive transparency. Even though the challenges posed by RS are gaining attention around the world, this article is grounded in European legal developments and, therefore, future research would be needed to shed light on whether and how they might be suited for other legal systems.

In the following Section II, we introduce autonomy and self-determination and how they are manifested, implicitly or explicitly, in law. We explain how RS operate on a technical level and how this can affect key aspects of autonomy, both legally, as well as philosophically conceptualised. Then, in the rest of the article, we discuss the current state-of-the-art of safeguarding autonomy in regulatory frameworks and then highlight key options, decisions and pathways forward. The key areas for regulation that we discuss are algorithmic design, user data protection rights, and transparency and oversight of RS as they are either directly implicated in determining the way in which individual autonomy is affected, as in the case of algorithmic design, or they constitute valuable tools to empower users or their representatives to safeguard individual autonomy, as in the case of data protection rights and transparency.

Thus, in Section III.A, we discuss regulatory options for safeguarding and promoting autonomy in the design of RS, using a law-by-design approach. In Section III.B we focus on the privacy and data protection rights upon which individuals could rely in order to control the information about them used for profiling and recommendations. Finally, in Section III.C we discuss transparency as a vital tool to ease the current asymmetrical distribution of information and power between RS creators and users and as a key infrastructure to enable accountability and meaningful human oversight over the power exerted by RS. The goal of our approach is not to limit or prohibit RS, as they may be a desirable feature of virtual environments. Instead, we seek to highlight the gaps and needs that a regulatory framework should seek

to fill in order to foster the creation and use of RS in a manner that truly ensures individual autonomy – that users are in the driver's seat, that they are aware of and can themselves shape or even exclude recommendations from their virtual worlds as they see fit, and that, vitally, there is a clear legal recognition of the impact that RS have on individuals and society that demands responsibility.

II. Autonomy and recommender systems

Autonomy is a normative concept about the rightful claim to self-determination in multiple contexts, be they collective or individual, national or international, and is also the foundation of human rights, democracy and the rule of law. The concept of autonomy in the law refers to the scope and ability of individuals or groups to make decisions for themselves or to "follow their own life plan"[34] and this right is explicitly or implicitly protected at multiple levels in the law. On a fundamental level, autonomy is demonstrated through the capacity of individuals to freely bind themselves in contracts, a manifestation of their self-determination.[35] On a higher level, autonomy is protected and enabled through legal certainty and the rule of law. Compliance with the rule of law makes governmental actions and the legal framework predictable and empowers individuals to plan their lives around them. This relation is enabled by transparency allowing individuals to judge the legality of their actions or claims. Autonomy is also a cross-cutting and transversal principle that is ingrained in every human right but comes to the fore in specific constellations, as demonstrated in human rights law practice. If a specific right is protected, this necessarily includes the autonomy of humans to use that right freely. The right to property includes the autonomy of a subject to dispose of property in any way, including destroying it. The freedom of opinion grants the right to make one's opinion known or to stay silent. Other rights are more clearly linked to individual autonomy, for example as art 8 of the European Convention on Human Rights (ECHR), the right to respect for private and family life. The European Court of Human Rights (ECtHR) interpreted this provision to find a right to personal autonomy, identity and integrity within art 8.[36] Human rights bills protecting human dignity also situate autonomy in this context. The right to self-determination, as enshrined in arts 1 of

[34] Emily Jackson, *Regulating Reproduction: Law, Technology, and Autonomy* (Hart Pub 2001) 2.

[35] Thomas Gutmann, 'Some Preliminary Remarks on a Liberal Theory of Contract' (2013) 76 Law and Contemporary Problems 39.

[36] Jill Marshall, *Personal Freedom through Human Rights Law? Autonomy, Identity and Integrity under the European Convention on Human Rights* (Martinus Nijhoff Publishers 2009) .

the International Covenant on Civil and Political Rights (ICCPR) and the International Covenant on Economic, Social and Cultural Rights (ICESCR), also shows that autonomy has a collective side. This side is expanded on especially in the area of minority rights, where a degree of autonomy could allow minority groups sufficient self-determination to benefit from the group rights that majorities typically experience.[37] The collective self-determination of peoples, communities, and nations is also linked to democratic institutions and processes. This points back to the literal historical meaning of autonomy. It means that individuals or groups should provide for the rules governing them. In contrast, the concept of heteronomy provides that the rules are made by somebody else.[38] Thus, individual and collective autonomy permeates and acts as a foundation to multiple layers of the legal order. This demonstrates that autonomy is a fundamental value and backbone of many legal systems that is safeguarded through the rule of law, fundamental rights, democratic processes and institutions, and even individual responsibility, liability, and the freedom to contract. As a cornerstone of many legal structures, there is an acknowledgement that autonomy is valuable and should be appropriately safeguarded. We will now explore whether and how RS interact with autonomy before exploring what the current and future legal landscape of regulating this relationship looks like in the next section.

In order to demonstrate how precisely RS and autonomy are interlinked, we take a conceptual approach towards understanding autonomy. Autonomy, in its practical ethical dimension, can be seen to require two essential conditions: independence from controlling influences (liberty) and capacity to intentionally act and decide (agency).[39] RS can affect both of these dimensions of autonomy on an individual and collective level. Relevant to RS, exerting control and influence or manipulation can affect the decision-making capacity of individuals,[40] thus making them subject to the will of another.[41] This could affect individual liberty directly, by limiting the scope for individual decision-making, or more perniciously, by distorting the individual capacity to make informed decisions and, thus, their agency. For

---

[37] J Wright, 'Minority Groups, Autonomy, and Self-Determination' (1999) 19 Oxford Journal of Legal Studies 605.

[38] Simon Hornblower, 'Autonomy' in Tim Whitmarsh (ed), *Oxford Classical Dictionary* (Oxford University Press 2015)..

[39] Lav R Varshney, 'Respect for Human Autonomy in Recommender Systems' [2020] arXiv:2009.02603 [cs] <http://arxiv.org/abs/2009.02603> accessed 5 March 2021; Tom L Beauchamp and James F Childress, *Principles of Biomedical Ethics* (8th edn, Oxford University Press 2019).

[40] Beauchamp and Childress (n 39).

[41] Andreas T Schmidt, 'The Power to Nudge' (2017) 111 American Political Science Review 404.

example, RS have been linked to the creation of 'filter bubbles' that limit the range and diversity of information users see[42] and can lead to political polarisation and a partial view of the world. In an extreme form, filter bubbles could reinforce messages of suicide,[43] radicalization and extremisation,[44] and mistrust of vaccines,[45] thus affecting both individuals and whole communities. Such actions can also lead to direct consequences on human rights. The Molly Russel incident spoke to children's rights, especially the physical integrity of children. Healthcare treatment or diagnosis recommendations can touch upon these and the right to health. When used in the context of social media and content curation or moderation, RS can have an impact on democracy, the freedom of speech and personality rights. This shows that RS can affect a multiplicity of human rights and freedoms and shape the space within which individuals can act with true autonomy just by directing individual attention and shaping individual thoughts and actions. From an individual level, through humans as an intermediary, RS could bring about tangible effects on human rights, freedoms, but also democratic processes and collective self-determination. Despite these effects, the current legal framework does not reflect satisfactory safeguards of such interferences.

RS are specifically created for the purpose of shaping human behaviour by exerting soft but persistent influences on individual liberty and shaping the information available for exercising agency and independent decision-making. Explicit safeguards against the influence of RS over individuals may be necessary because there is an inherent misalignment of interests between those designing and deploying RS and the final users. Creators of RS may seek to further their own commercial goals under a veneer of providing better service and more relevant content for users. Recent fieldwork with US developers of RS identified a common goal of 'hooking' people and keeping

---

[42] Tien T Nguyen and others, 'Exploring the Filter Bubble: The Effect of Using Recommender Systems on Content Diversity', *Proceedings of the 23rd International Conference on World Wide Web - WWW '14* (ACM Press 2014) <http://dl.acm.org/citation.cfm?doid=2566486.2568012> accessed 5 March 2021; Engin Bozdag, 'Bias in Algorithmic Filtering and Personalization' (2013) 15 Ethics and Information Technology 209.

[43] David D Luxton, Jennifer D June and Jonathan M Fairall, 'Social Media and Suicide: A Public Health Perspective' (2012) 102 American Journal of Public Health S195.

[44] Philip Baugut and Katharina Neumann, 'Online News Media and Propaganda Influence on Radicalized Individuals: Findings from Interviews with Islamist Prisoners and Former Islamists' (2020) 22 New Media & Society 1437; Mark Alfano and others, 'Technologically Scaffolded Atypical Cognition: The Case of YouTube's Recommender System' (2020) Synthese <http://link.springer.com/10.1007/s11229-020-02724-x> accessed 5 March 2021.

[45] Deena Abul-Fottouh, Melodie Yunju Song and Anatoliy Gruzd, 'Examining Algorithmic Biases in YouTube's Recommendations of Vaccine Videos' (2020) 140 International Journal of Medical Informatics 104, 175; Harald Holone, 'The Filter Bubble and its Effect on Online Personal Health Information' (2016) 57 Croatian Medical Journal 298.

them on a particular platform,[46] which was reflected in the way that the RS was created. RS design and operation can take a multitude of shapes; designer intent and desire can play a significant role in how RS ultimately operate. While RS can be valuable to online users, they need to balance the interests of designers and users to be a valuable solution.[47] Due to the asymmetry of power and knowledge between designers and users in shaping and understanding RS, a balance may be difficult and unlikely without some form of regulation. Here, we briefly introduce the main architectures used in RS, the data needed, as well as the role of a desired target variable for which RS optimise. All of these features can have implications for the impact the system has on individual autonomy. Furthermore, these features are also currently within the exclusive domain of determination of RS designers and developers.

In order to operate, RS require definitions of what the range of options they can recommend are, what a 'good' recommendation is and how to identify it (i.e. a target variable which the systems seek to maximise), and how their performance is evaluated,[48] which allows for future improvements of RS. There are a number of commonly used RS techniques that allow (semi-) automation of recommendations. First, *collaborative filtering* focuses on how multiple users have historically rated items, in order to predict ratings of these items by other users who have not yet rated them. RS can do that by grouping either users or items together, on the basis of similarity metrics. The RS can then suggest content on the basis of what similar users liked or on the basis of what items are similar to what a user and other similar users have liked in the past.[49] In contrast, a *content-based RS* models a user's interests by analysing attributes of items that a specific user has interacted with in the past, focusing on the user's own behaviour to predict the user's future rating of a new item.[50] Finally, the *knowledge-based approach* invites users to directly specify their interests or requirements. These interests are then combined with the system's pre-programmed domain knowledge to generate recommendations.[51] An example could be exploring real estate websites that allow refining search results through numerous user-chosen filters. In reality, RS often use hybrid architectural approaches.

---

[46] Nick Seaver, 'Captivating Algorithms: Recommender Systems as Traps' (2019) 24 Journal of Material Culture 421.

[47] Francesco Ricci, Lior Rokach and Bracha Shapira (eds), *Recommender Systems Handbook* (Springer US 2015) 6.

[48] Milano, Taddeo and Floridi (n 2) 2.

[49] Charu C Aggarwal, *Recommender Systems* (Springer International Publishing 2016) 8.

[50] ibid 14.

[51] ibid 15.

RS also need different types of data about users and content or items to operate, depending on the recommender technique used.[52] Data can be used *inter alia* to assess the user's interest in an item or to assess the similarity of different users or of different items. RS can rely on both explicit and implicit user feedback. Actions, e.g. recording users 'liking' or 'sharing' a piece of content or even visiting a page, can serve as an implicit positive rating of that content that RS then use to inform and reinforce their operation. More complex models can also include data about time and duration of interactions of users, location, social or network information, as well as external domain knowledge.[53] Demographic data classifiers can especially boost the accuracy of other RS techniques.[54] Clearly, the three RS architectural approaches, as well as the data used ascribe a different weight to a single user's actions in terms of their impact on determining the ultimate recommendations that user receives.

A third key feature of RS is their determination of what 'good' recommendations are. "Good" is an inherently subjective term, especially in the context of personalisation. What is a "good" recommendation for one would not be so for another. Moreover, to automate the computation and presentation of recommendations, 'good' needs to be defined mathematically. RS are said to present items that are of interest or relevant to a particular user.[55] but how that should be translated into the RS's design and what they should optimise for is not predetermined. In machine learning (ML), the technology behind many RS, this is the key role of a target variable – a specific and measurable variable that allows the ML model to calculate and predict whether its performance (recommendation) will be poor or good, based on data from past performance. In RS, the target variable is the measurable variable that designers have determined to be a good proxy measure of a "good" recommendation – e.g., whether a user interacts with a piece of content, whether they share it, whether they 'like' it etc. The RS then seeks to maximise this. The difficulty here lies in identifying which measurable variable(s) can be used to represent a user's positive reaction to a recommendation. The goals of service providers could be to increase the number or diversity of items sold, interacted with, increase user satisfaction and fidelity, or simply improve understanding of what the user wants.[56] The use of such a variable will not always coincide with the users' definition of what a 'good' recommendation is for them. Moreover, should a "good" recommendation

[52] Ricci, Rokach and Shapira (n 47) 9.
[53] Aggarwal (n 49) 2.
[54] ibid 19.
[55] See Ricci, Rokach and Shapira (n 47) 1.
[56] ibid 5–6.

only be assessed on the basis of how a user perceives it or is there also space for reflecting the reputability of a source or the content of the item being recommended? Imagine the case that a person positively reacts to a piece of content, advocating for racial inequality. Does that mean this was a "good" recommendation? The interests of designers and the users seem to be satisfied with this recommendation being rated positively, but is there space to discuss collective self-determination and the social interest? These are not easy questions and there is not necessarily one correct answer. But they are, nevertheless, decided every time a RS is created. For this reason, in the next section we start our mapping of the pathways to regulating RS in order to safeguard individual autonomy by first discussing the importance of regulating RS design and the role users can and should play within it.

III. Regulating autonomy in recommender systems

Given the deep sources of tension between RS and autonomy, in this paper we seek to explore the potential for regulatory interventions to safeguard autonomy by enhancing user empowerment in three ways: (i) through the design and functioning of RS, utilising a law-by-design approach; (ii) through privacy and data protection rights to control RS data inputs, with a rights-based approach; and (iii) through transparency in user interactions and co-shaping of RS, with a process-based solution. We structure our analysis along these three dimensions— algorithmic design, data inputs, and transparency — to introduce specific regulatory options. At every step, we explore how autonomy is safeguarded in law today and the current state of art and propose pathways for the future, as possible solutions to further enhance autonomy.

A. Designing Recommender Systems

New technologies of ML have fuelled the capacity of RS to increase their performance and issue more fitting recommendations. Generally, the improvements are due to the availability of training data allowing the respective algorithms to be optimized in certain regards. However, the design goals and the respective metrics towards which such an algorithm can be optimised vary. They range from engagement with the RS by spending time or buying products to more general goals like accurate user information or presentation of information the user might not have been exposed to. Every system communicates to a person in order to support and shape their decision-making. Considering that RS exert such an important influence on persons, the argument can be made that there should be some ways for users to actively influence them or, at the very least, there should be some expectation on the

part of the creators of RS to consider and account for the impact their work might have on the autonomy of the intended users. Here we will explore how regulation can influence algorithmic design and propose options to shape RS design in an autonomy-enhancing manner through law.

i. State of the art of design for autonomy

In law, there is a growing amount of legislation that directly engages in the design process. Notable and known examples relate to privacy and IT-security, as provided for in arts 25 and 32 of the General Data Protection Regulation (GDPR), which lay down privacy and security by design obligations.[57] Thereby, they transfer legal principles into the very design of technologies by mandating they be considered at every step of a technology's creation, use, and maintenance. Data protection and IT-security are to be included in design processes as design goals of their own right, although ones of many, balanced against qualifications like the cost of implementation. This begs the question regarding whether regulators could add autonomy as another design goal in the same fashion as data protection and privacy. An analysis of the law shows that there are already first signs of including such design goals.

Take for example art 29 of the draft EU DSA. This provision specifically addresses RS in the context of online platforms. The transparency obligation in this article hints at a nascent autonomy by design principle. It provides that "*[v]ery large online platforms that use recommender systems shall set out in their terms and conditions …. any options for the recipients of the service to modify or influence those main parameters that they may have made available, including at least one option which is not based on profiling…*". The obligation states that users are empowered to modify the parameters of a RS. It indicates that, at the least, users can choose to receive recommendations not based on personal profiling. This could mitigate the role of personalisation that otherwise enhances the effectiveness of recommendations in achieving their pre-determined goal. Moreover, the DSA also seeks to establish a duty on the part of large online platforms to manage systemic risks arising from their platforms. The draft act mandates that large online platforms should particularly take into account the negative effects on

[57] Peter Schaar, 'Privacy by Design' (2010) 3 Identity in the Information Society 267; Dag Wiese Schartum, 'Making Privacy by Design Operative' (2016) 24 International Journal of Law and Information Technology 151; Privacy and security by design obligations are also found in the current draft Indian data protection legislation. Saumyaa Naidu and others, 'The PDP Bill 2019 Through the Lens of Privacy by Design' (The Center for Internet & Society 2020) <https://cis-india.org/internet-governance/blog/the-pdp-bill-2019-through-the-lens-of-privacy-by-design>.

fundamental rights, including the right to privacy, freedom of expression and information, non-discrimination, and the rights of the child[58] among these risks. Platforms are explicitly tasked to consider 'how their recommender systems and systems for selecting and displaying advertisement influence any of the systemic risks'.[59] They are then tasked with taking appropriate action to mitigate identified risks, including by altering how their RS operate,[60] and their risk management activities are subject to independent audits[61] and public disclosure.[62] This provision will affect not only the process of RS design, but also its long-term maintenance and review. It is geared towards pushing platforms to reflect on and mitigate risks that arise as a result of their functioning and, especially, of the design and operation of their RS and advertisement systems. Both of these requirements in the DSA clearly indicate that legislators are looking into checking the power and influence of RS, including by demanding that user autonomy is considered and enhanced by design.

Similarly, the recent European Commission proposal for an AI Act, while it does not directly address RS, or user autonomy, demonstrates that it seeks to safeguard individual autonomy in the face of powerful artificial intelligence (AI). Art 5(1)(a) of the AI Act seeks to ban any "system that deploys subliminal techniques beyond a person's consciousness in order to materially distort a person's behavior", while art 5(1)(b) addresses systems that exploit "any of the vulnerabilities of a specific group of persons due to their age, physical or mental disability, in order to materially distort the behavior of a person pertaining to that group".[63] These prohibitions of systematic utilisation of weaknesses of individuals clearly address limitations in their capacity to exercise autonomy and highlight awareness of the persuasive powers of AI.

At the national level, an explicit example of inclusion of autonomy by design can be found in the German Digital Healthcare Act.[64] This act supports digital technologies like mobile apps by providing for funding schemes from health insurances. The Digital Healthcare Act introduces Section 20(k)(1) of the German Social Law Book V,[65] which provides for measures to

---

[58] DSA, art 26(1)(b).
[59] DSA, art 26(2).
[60] DSA, arts 27(a) and 27(b).
[61] DSA, art 28.
[62] DSA, art 33.
[63] Both alternatives are only applicable when applied "in a manner that causes or is likely to cause that person or another person physical or psychological harm" – arts 5(1)(a) and 5(1)(b).
[64] DVG 2019 (BGBI I p 2562)
[65] SGB V 1988 (BGBI I p 2477).

enhance patients' self-determination when it comes to digital applications and telemedicine. Section 139(e)(2) of the German Social Law Book V provides for requirements for health insurances to remunerate digital applications if the applications meet a set of criteria. One of these criteria are positive effects on healthcare. The respective draft secondary legislation mentions "patients' sovereignty" as one of the decisive criteria of positive effects. Thereby, patients' sovereignty is one of the evaluation criteria that designers of those apps would have to take into account even at the design stage if they want their app to be covered by health insurance.

An autonomy-by-design requirement could take different forms. It could require RS designers to mitigate and minimise the risks their systems pose to autonomy or it could require them to consider how to maximise and proactively help realise individual autonomy in the design of their technologies.[66] One example for the latter approach would be the technology clause in art 4(g) of the United Nations Convention on the Rights of Persons with Disabilities (UNCRPD) which obliges states "*[t]o undertake or promote research and development of, and to promote the availability and use of new technologies, including information and communications technologies, mobility aids, devices and assistive technologies, suitable for persons with disabilities, giving priority to technologies at an affordable cost*".[67] This clause explicitly addresses the progressive realisation of autonomy in technology and shows that in very specific cases the law can demand or incentivise autonomy in technology. There are clearly instances of both logics in existing legislation at multiple levels. Regulators should determine which approach would be best-suited for their goals, perhaps taking a diversified view depending on the application of RS.

Regardless, these examples signify the general trend in legislation to consider autonomy, sovereignty and self-determination of users in the context of algorithmic design. However, these examples are – to date – rather general. Therefore, the question arises—what regulatory possibilities are there to apply autonomy-by-design principles in real life? The regulation of RS to enhance autonomy can include a number of considerations and principles for designers to keep in mind, however, a case-by-case approach would be

---

[66] Wolfgang Hoffmann-Riem, 'Re:Claim Autonomy, Die Macht Digitaler Konzerne' in Jakob Augstein (ed), *Reclaim Autonomy: Selbstermächtigung in Der Digitalen Weltordnung* (Erste Auflage, Originalausgabe, Suhrkamp 2017) 122.

[67] Convention on the Rights of Persons with Disabilities (adopted 24 January 2007 UNGA A Res 61/106 (CPRD)), art 4(g); An example in the Indian context could be the digital accessibility provisions under the Rights of Persons with Disabilities Act 2016, for reference see, 'Digital Accessibility in the Rights of Persons with Disabilities Act 2016' (2017) Centre for Internet and Society, India.

necessary to assess how precisely such principles are to be transposed into algorithmic design. This is due to the fact that the actual risks of RS can vary considerably, depending on their context of application. What tools might exist to help fulfil this? What regulatory structures might be relevant to establish in order to facilitate this? In the remainder of this section, we look at more concrete opportunities for this.

ii. Ways to further enhance autonomy

Autonomy can be included as a regulatorily-mandated design goal for RS, as discussed. This would require a clarity of whether its goal is to minimise negative impact on autonomy or also to maximise the positive and empowering impact on individual autonomy. Beyond this, however, regulatory options can distinguish between setting autonomy as a design goal to be implemented throughout the process of technology creation, or rather focusing on the final impact of the technology on autonomy, perhaps through requiring that it meet desirable standards for access to the market. In order to have a better grasp on these choices, it is necessary to know about different concepts in the design of RS, as well as the links between algorithmic design and individual autonomy which will be explained below.

a. User capacity and shared decision-making

A fundamental starting point for autonomy-enhancing algorithmic design is a greater understanding of the factors that make up an autonomous human decision in a human-machine interaction. Interdisciplinary research is necessary to understand the conditions under which a human decision could be assumed to be independent. This is particularly important in order to delimit whether a certain system is considered a recommender system or whether human autonomy has shrunk so far that the system effectively operates as an automated decision-making system. Several criteria have been introduced as a delimitation. The competence of human recipients of recommendations is one of them.[68] Another question is the extent to which a decision could actually be influenced.[69] So far, understanding the factors affecting human

---

[68] Philip Scholz, '22' in Spiros Simitis, Gerrit Hornung and Indra Spiecker Döhmann (eds), *Datenschutzrecht: DSGVO mit BDSG* (Nomos 2019) para 27; Mario Martini, 'Art. 22' in Boris Paal and Daniel Pauly (eds), *Datenschutz Grundverordnung: DS-GVO* (2nd edn, CH Beck 2018) para 18; Article 29 Data Protection Working Party, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679' (2018) WP251rev.01 29 <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053> accessed 31 March 2021.

[69] Gerald Spindler and Anna Z Horvátg, 'Art. 22 Automatisierte Entscheidungen Im Einzelfall Einschließlich Profiling' in Gerald Spindler and Fabian Schuster (eds), *Recht Der*

capacity has been especially relevant in the context of current regulatory approaches to automated decision-making systems processing personal data, specifically as per Article 22 GDPR that lays down safeguards for such systems. Debates about when a system fulfils the definition of an automated decision-making system have pushed such discussions forward. The answer is necessarily binary: either a system is an automated decision-making system in the sense of art 22 GDPR or the provision does not apply. This is relevant because, when discussing how different design approaches could be used to enhance or mitigate impacts on individual autonomy, a greater understanding of the relationship between suggestions and recommendations and individual decision-making is necessary. For example, in the case of decision support systems, one could design a taxonomy that describes different levels of human-computer interaction ranging from simple filters to an automated decision-making system. One factor guiding the different levels of such a taxonomy could be the degree of autonomy that rests with the user when interacting with the system, which could help assess the risk of direct interaction with RS. Potential measures could be linked to the different level. Such a taxonomy could describe the different levels of human autonomy in the same way that levels of autonomy of humans are described for automated vehicles. At the very least, such understanding would be necessary to ground all subsequent regulatory and design activities around autonomy-by-design for algorithms.

b. Serendipity and randomization

A technical aspect that directly shapes how and with what aim a recommendation nudges individuals is the process of choosing a target variable and optimising RS. The optimisation process is crucial in machine learning.[70] Setting the goals of optimisation is a key component of designing algorithms and an instance in which human agency can guide the way in which AI-systems operate.[71] In supervised learning, designers also specify a concrete and measurable target variable that the algorithm is trained to seek to optimise for.[72] While some tasks are binary like image recognition of a horse (it is or it isn't a horse), RS have to carry out more complex computations to predict whether showing a particular item to a user and at a particular order

Elektronischen Medien (CH Beck 2019); Article 29 Data Protection Working Party (n 68) 21.

[70] Suvrit Sra, Sebastian Nowozin and Stephen J Wright (eds), *Optimization for Machine Learning* (MIT Press 2012).

[71] Björn Haferkamp, 'Was Ist Optimal? Nutzen Und Fallstricke Der Optimie' in Björn Bergh (ed), *Big Data und E-Health* (Erich Schmidt Verlag 2017).

[72] David Lehr and Paul Ohm, 'Playing with the Data: What Legal Scholars Should Learn About Machine Learning' (2017) 51 University of California, Davis 653.

will result in a higher or lower target variable. Above, we gave the example of optimising for selling more or diverse items, but a target variable need not perpetuate the commercial interests of the designers. A target variable could also, for example, be used to mitigate the intentionally nudging impact RS can have on user autonomy by introducing unexpected recommendations in different ways – through serendipity, diversity, or randomisation.

The concept of serendipity centres around the question of how to recommend information that fits the interests of the respective person without recommendations being known or expected.[73] Through item-based grouping, a RS could help individuals with very obvious choices. A person looking for a hammer will probably need nails. However, a more complex RS might also be able to suggest a new system to hang something without damaging the wall. A similar but distinct concept is diversity. Unlike serendipity, diverse recommendations are not aimed at finding what the user is looking for in the first place. Rather, they confront the user with content that is different from what she or he expected.[74] A system recommending job ads might include ads that go beyond the imagination of the user, but which might also fit.

Finally, in contrast to serendipity, randomisation does not relate to the actual fit of a recommendation to a user but selects alternatives outside of what is recommended by the system. Randomisation can enhance the scope of action of a system by allowing it to confront people with data outside of the usual training. If a news RS is personalised in a way that operates as a filter bubble, curating content along a specific political stream, randomization might break that up by including recommendations beyond the confines of what the system can predict will be positively received by the user. In addition to enhancing the independence of users from the 'will' of the designers of RS, randomisation can be a valuable and desired feature for risk management systems and applications of RS in public bodies exercising some form of oversight. One example is the system used by the German tax authority to identify tax applications and recommend them for further human scrutiny. Section 88 of the German Tax Code provides for the necessity of a randomized human control of this recommender system. One measure to complement the automated risk assessment is the random selection of cases for human review,[75] irrespective of their risk level. This measure fulfils two

---

[73] Aggarwal (n 49) 3–4.

[74] Natali Helberger, Kari Karppinen and Lucia D'Acunto, 'Exposure Diversity as a Design Principle for Recommender Systems' (2018) 21 Information, Communication & Society 191.

[75] Ann Cavoukian, 'The 7 Foundational Principles' (2009) <https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf> accessed 31 March 2021.

functions.[76] First, it tests overall compliance, especially of the applications with low risk levels. Second, it allows for the evaluation of the system itself, as the risk management system should select certain applications in a random fashion for further review irrespective of their risk level. An additional step in the system used by the German tax authority is the freedom of users to completely sidestep it. Another requirement of the system is that officials must have complete access to all applications and must be able to select cases themselves. Thus, there are technical features which could serve as 'breaks' along the way from designer intent to user nudging, thus limiting the intentional influence RS exert on their users.

c. User control

While the steps in the previous section demonstrate ways in which the link between designer interests and user influence through RS can be limited, user autonomy and self-determination can also be enhanced through greater participation of users in the shaping of the RS they use – user control. There is a vivid area of research that looks into whether and how users can influence RS voluntarily. Currently, individuals can and often do contribute to their information curation, e.g. by choosing whether to follow certain individuals, pages, channels or by blocking content from sources.[77] However, user control approaches go far beyond the ordinary acts of users providing profile data or giving feedback.[78] Instead, user controls entail more direct impact, e.g. settings through which users actively tweak and change the underlying algorithms[79] or can choose between different algorithms.[80] It puts users in the driver's seat and enhances their autonomy. So far, the reported results of experiments are promising. Users make active use of these possibilities, they have a positive experience[81] and such measures generally also increase their

---

[76] Nadja Braun Binder, 'Ausschließlich Automationsgestützt Erlassene Steuerbescheide Und Bekanntgabe Durch Bereitstellung Zum Datenabruf' (2016) Deutsche Steuer-Zeitung 526.

[77] Lisa Merten, 'Block, Hide or Follow—Personal News Curation Practices on Social Media' (2020) Digital Journalism 1.

[78] For examples of user control see Yucheng Jin, Bruno Cardoso and Katrien Verbert, 'How Do Different Levels of User Control Affect Cognitive Load and Acceptance of Recommendations?' 2017 <http://ceur-ws.org/Vol-1884/paper7.pdf> 8; Mechanisms of instant feedback are described in Harald Steck, Roelof van Zwol and Chris Johnson, 'Interactive Recommender Systems: Tutorial', *Proceedings of the 9th ACM Conference on Recommender Systems* (ACM 2015) <https://dl.acm.org/doi/10.1145/2792838.2792840> accessed 5 March 2021.

[79] Jin, Cardoso and Verbert (n 78) 38.

[80] Michael D Ekstrand and others, 'Letting Users Choose Recommender Algorithms: An Experimental Study', *Proceedings of the 9th ACM Conference on Recommender Systems* (ACM 2015) <https://dl.acm.org/doi/10.1145/2792838.2800195> accessed 5 March 2021.

[81] F Maxwell Harper and others, 'Putting Users in Control of Their Recommendations', *Proceedings of the 9th ACM Conference on Recommender Systems* (ACM 2015) 8

trust.[82] Therefore, user control is a design choice that can substantially add to recommender systems enhancing autonomy. As discussed above, the draft DSA also highlights user choice in shaping RS and in, at the very least, having a choice between a personalised and non-personalised system.

User control of algorithms has also attracted attention in the social media industry. Twitter announced the research project "blue sky" that aims to build an "app store for (…) algorithms".[83] The goal is decentralisation of algorithms used by social media that allows users to control the algorithms shaping the information they see. One element that goes beyond current approaches in decentralised networks like Mastodon is the idea of creating choice for content moderation algorithms. In a conversation with investors, Twitter CEO Jack Dorsey framed the idea as follows:

> *The problem of discovery around content is one that is easiest when it is centralized, and that's how we've operated for almost the past 15 years. But even that has some potential to shift. And one of the things we brought up last year in our Senate testimonies … is giving more people choice around what relevance algorithms they're using for ranking algorithms you're using. You can imagine a more market-driven and marketplace approach to algorithms. And that is something that not only we can host but we can participate in.*[84]

This is one specific example of how user control could be implemented for content moderation by creating a market for content moderation algorithms which would give users a choice between different algorithms.

d. A new freedom of association

As mentioned above, collaborative filtering RS techniques are based on grouping 'similar users' together to drive the predictive power of the models. Through profiling, RS classify and group users together. While measures of user control would influence or change the ways in which people are profiled or the way content is targeted to them, it is also possible to give users power to influence how user groups are formed or, at the very least, how

---

<https://dl.acm.org/doi/10.1145/2792838.2800179> accessed 5 March 2021.

82 Jin, Cardoso and Verbert (n 78) 40.

83 Jacob Kastenakes, 'Twitter's Jack Dorsey Wants to Build an App Store for Social Media Algorithms' (*The Verge* 9 February 2021) <https://www.theverge.com/2021/2/9/22275441/jack-dorsey-decentralized-app-store-algorithms>.

84 'Twitter, Inc.'s (TWTR) CEO Jack Dorsey on Q4 2020 Results - Earnings Call Transcript' (*SeekingAlpha*) <https://seekingalpha.com/article/4404806-twitter-inc-s-twtr-ceo-jack-dorsey-on-q4-2020-results-earnings-call-transcript> accessed 16 April 2021. This refers back to an idea of Stephen Wolfram to give users a choice in content moderation.

they themselves are grouped. This could be done, for example, through RS allowing individuals to directly associate themselves with a certain group.[85] Certain RS are already exploring this opportunity with regard to gender. A famous fashion RS explores the possibility of allowing users to be more fluid with their gender for the purposes of recommending items to them. Instead of asking whether the user is male, female or something else, they want to know whether somebody would feel male, female or something else.[86] Generalising this idea would mean that the possibility for users to choose a certain group, category, or label they could be characterised with could be a design feature of RS. This would transgress the notion of data protection and its focus on data being correct and up-to-date. It would allow users to associate themselves with groups depending on their will at particular times. This would function as a loose reminder of the freedom of association as a human right in the sense that the freedom of association also encompasses the right to be part or not to be part of a group.[87]

One might object to such a design feature with the argument that it might harm the accuracy and the fit of the respective recommendation. There might be also further burdens to the optimization of the respective system given that the person choosing the group might not share many of its attributes. Yet there are a number of potential autonomy-enhancing benefits of such an approach. Firstly, certain circumstances may warrant such a feature. This would be cases in which certain individuals have a strong and legitimate interest not to be categorised in a rigid manner, but also where there are no potential negative consequences from a recommendation based on the user's self-determined grouping. For example, in the case of gender, a fashion recommendation would pose no harm regardless of gender specified, however health recommendations may be based on research that is biologically gender-specific. Secondly, a freedom of association would also allow for the intuitive self-determination of users who might not have expertise how the system works but might gain some experience about the association with certain groups, which produces the best outcomes for them. A limitation of

---

[85] One could also think about interactive possibilities of recommending things amongst users. Bart P Knijnenburg, Saadhika Sivakumar and Daricia Wilkinson, 'Recommender Systems for Self-Actualization', *Proceedings of the 10th ACM Conference on Recommender Systems* (ACM 2016) 12 <https://dl.acm.org/doi/10.1145/2959100.2959189> accessed 29 July 2021.

[86] This information is based on an expert interview.

[87] Christian Tomuschat, 'Freedom of Association' in Ronald J St Macdonald (ed), *The European System for the Protection of Human Rights* (Nijhoff 1993); Jürgen Bröhmer, 'Kapitel 19: Versammlungs- und Vereinigungsfreiheit' in Oliver Dörr, Rainer Grote and Thilo Marauhn (eds), *EMRK/GG. 2: Kapitel 20 - 33, Register* (2. Aufl, Mohr Siebeck 2013). Of course, the freedom of association as a human right requires some stability of the respective group which would not be the case.

this approach is that it may be specific to RS that rely on a communicative relationship between a human and a computer in which the ultimate decision rests with the human being.

e. Inter-subjective autonomy

In all the above-mentioned cases, design features address autonomy at the level of an individual user. However, this misses the importance of group or collective autonomy. In the process of profiling and grouping users, an influential decision could be made about which feature similarities are relevant, and thus become a group and which do not form a group of their own. Thus, profiling constructs groups of users but leaves other potential groups unconstructed. This provokes the important design question of whether inter-subjective autonomy can also be exercised through the design of RS. Is there a possibility for groups to determine themselves? This line of thinking can draw upon different ideas such as pluralism or other conceptions focusing on the interests of developing states such as post-colonial computing.[88] Inter-subjective autonomy requires design features for groups to influence the design of RS, and at the very least to establish their existence in the 'eyes' of an algorithm. A first step would be to define certain classes that are not present if categories like gender or ethnicity are narrowly constructed. As a next step, if a group is constructed and this group can express its preferences, it might be possible to allow this group to influence the respective recommender system in the ways described above.

What is clear from the foregoing discussion is that the way RS are designed can shape the impact they have on individual and collective autonomy. Moreover, we have shown that recent legislative initiatives show indications for the requirement of designers and deployers to consider autonomy in the process of creating RS. We have also introduced a number of technical design measures that could either help minimise the intentional, human-designed impact of RS on autonomy or can help maximise autonomy and empower RS users. Nevertheless, we also highlighted that there are more decisions for regulators to make and clarify, including what a potential autonomy-by-design obligation would entail – simply accounting for and mitigating the impact RS have on autonomy or rather actively considering how to use technology in a manner that empowers individuals to pursue their life paths. Moreover, further research will be necessary to understand how to define and assess

---

[88] Lilly Irani and others, 'Postcolonial Computing: A Lens on Design and Development', *Proceedings of the 28th International Conference on Human factors in Computing Systems - CHI '10* (ACM Press 2010) <http://portal.acm.org/citation.cfm?doid=1753326.1753522> accessed 29 July 2021.

degrees of human autonomy and independence in human-computer interaction, as well as whether and how different contexts of RS application justify a differential approach to implementing autonomy-by-design in practice. Regardless, it is clear that design must be one of the regulatory pathways to truly safeguarding autonomy.

B. Input: Governance of personal data

It would be unfair to say that individuals currently have no recourse to control how they are 'seen' and profiled, including by RS. Privacy and data protection legislation have increasingly been adopted all over the world. This is relevant to autonomy because through inferences, grouping, and classification, RS can also interfere in the personal identity experience by, for instance, classifying a profile in a manner not corresponding to the features or categories with which the user self-identifies.[89] Moreover, the use of automated inferences[90] can reinforce biases, stereotypes, and stigmas, even without people's awareness. These inferences can significantly affect people's privacy, identity, and self-determination.[91] In that context, data protection regulation can be a tool to govern the development and use of RS. The question of how legal rights can empower individuals to shape the data input of RS in a manner that safeguards individual autonomy is further explored below.

i. State of the art in European data protection law

The EU has the GDPR which does not regulate RS specifically, but rather the collection and use of any personal data,[92] including for profiling and automated decision-making. The GDPR[93] plays an important role in safe-

[89] Milano, Taddeo and Floridi (n 2) 962.

[90] In Europe, there is still no consensus on the classification of inferences made by automated systems based on information about people. For the Article 29 Working Party, it would be classified as personal data and, then, protected under GDPR, but the Court of Justice of the European Union disagrees with such an approach. (Joined Cases C-141/12 & C-372/12, *YS, M and S v Minister voor Immigratie, Integratie en Asiel* [2014] OJ C 315); Sandra Wachter and Brent Mittelstadt, 'A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI' (2019) Columbia Business Law Review 494; Article 29 Data Protection Working Party (n 68) 5.

[91] Wachter and Mittelstadt (n 90) 513.

[92] Personal data means "any information relating to an identified or identifiable natural person ('data subject')". Art. 4 (1) Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1.

[93] Although this study was mostly based on the European scenario, it is worth mentioning that the GDPR was a robust data protection regulation that inspired many other countries, not only on the drafting of their data protection bills but also stimulating a higher level of enforcement and compatibility with the European guideline. In Latin America, for instance, this was the case of Brazil, which built its Data Protection Regulation mirroring

guarding individual autonomy because it strengthens individual control over personal data.[94] It is addressed at public authorities and private actors alike. It, therefore, fulfils the obligations of states to respect and protect human rights in society. The regulation embodies the principle of informational self-determination, setting specific obligations for data controllers while protecting and empowering individuals.[95] There are a number of key features of the current data protection legislation in this regard.

a. Consent

In order to ensure greater individual self-management of data,[96] consent, as an expression of free choice, self-determination and autonomy, plays an important function in data protection.[97] It is essential to the exercise of individual control over personal data.[98] The GDPR establishes explicit, free and *informed* consent as one of the lawful bases of art 6, permitting the processing of personal data and legitimizing algorithmic processing of personal data.[99] Although there are other legal bases in the regulation, the data subjects' consent plays a central role in the law regarding autonomy, since it allows genuine and informed individual control over an individual's data.[100] When consent is obtained in full compliance with the conditions imposed by the GDPR, it is an effective tool to ensure users' control whether or not personal data concerning them will be processed,[101] which enables autonomy. Consent can be an especially valuable and necessary safeguard in the context of intrusive activities such as in the case of decision-making based solely on

---

the GDPR envisioning an enhanced privacy culture internally, and the possibility of enabling lawful international transfers, and stimulating companies to uniformize its policies on an international level with a GDPR standard.

94 Tatiana Shulga-Morskaya, 'Protection of Personal Data through Implementation of the Right to Informational Self-Determination: Identifying Opportunities and Pitfalls' (2019) <https://www.giga-net.org/2019symposiumPapers/17_Shulga-Moskaya_PROTECTION-OF-PERSONAL-DATA.pdf> accessed 30 March 2021.

95 ibid.

96 Daniel J Solove, 'Privacy Self-Management and the Consent Dilemma' (2013) 126 Harvard Law Review 1880.

97 Bart W Schermer, Bart Custers and Simone van der Hof, 'The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection' (2014) Ethics and Information Technology <http://link.springer.com/10.1007/s10676-014-9343-8> accessed 5 March 2021.

98 Solove (n 96).

99 Bruno Ricardo Bioni, *Proteção de Dados Pessoais - A Função e Os Limites Do Consentimento* (2nd edn, Forense 2019).

100 Article 29 Data Protection Working Party, 'Guidelines on Consent under Regulation 2016/679' (2018) WP259 rev.01 <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051> accessed 30 March 2021.

101 European Data Protection Board, 'Guidelines 05/2020 on Consent under Regulation 2016/679, Version 1.1' (4 May 2020) 5 <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf> accessed 30 March 2021.

automated processing that, in other circumstances, would be prohibited by the law.[102] The Article 29 Working Party, a former expert body providing authoritative interpretations of European data protection law, furthermore suggested that in most of the cases of algorithmic data processing, such as in RS, which affect individual and collective autonomy, focus should be on getting the user's consent.[103] Upon closer examination, there are a number of requirements for ensuring consent actually safeguards individual autonomy, which are not always easily met in practice.

According to art 4(11) of the GDPR, valid consent must be freely given, specific, informed, and unambiguous, through a clear statement of affirmative action that indicates the data subject's wishes and agreement to the processing of their personal data.[104] It is vital that consent is informed, meaning that individuals are provided sufficient information to understand what they are asked to agree to, including what data would be processed, by whom and for what purpose.[105] This is linked to a right to receive information, necessary for the validity of consent.[106] The importance of information is further discussed also in Section III.C of this paper.

Consent must also be unambiguous and explicit in that, as clarified in recital 32 of the GDPR, silence, pre-ticked boxes or inactivity should not be accepted as consent. Despite the non-binding status of the GDPR's recitals, this provision reinforces the voluntary and non-mandatory nature of consent, as it must be actively given in order to maintain the individual's control

---

[102] ibid 18.

[103] Article 29 Data Protection Working Party (n 100) 47.

[104] ibid 5; European Data Protection Board (n 101) 7–18. To be considered valid in the terms of the regulation, consent must be simultaneously:

(i) freely given – meaning a real choice and control for data subjects. If the user feels compelled to consent or will endure negative effects by not consenting, consent will not be considered informed, thus, invalid. Also, consent is not free when there is not an option to refuse or withdraw consent without detriments – it must not be considered a condition;

(ii) specific – users' consent must be directed to one or more specific purposes, giving them a choice in relation to each of these purposes (granularity). This enables control and transparency;

(iii) informed – meaning that the controller, before obtaining consent, must provide users with enough information to ensure informed decision making. For example, informing users about what they are agreeing to and how to exercise their right to withdraw, if necessary;

(iv) unambiguous indication of the data subjects' wishes to authorize the processing of their data – it must be given through an active motion or declaration by the user, making clear and obvious that they accepted and understood the terms.

[105] GDPR, arts 13, 14.

[106] European Data Protection Board (n 101) 94.

over data.[107] The inclusion of the obligation to inform users regarding the possibility to withdraw consent confirms that it is reversible, which puts a degree of control on the side of RSs' users.[108] The e-Privacy Directive[109] also requires informed and prior consent for all except the necessary technical cookies on websites, rejecting opt-out mechanisms for all other cases, but rather requiring explicit user action to indicate consent. This is positive for the exercise of individual autonomy since the user must decide and express their active choice for use of tracking technology, in a measure of opt-in.[110] In the same vein, the European Court of Justice decided, in the case of *Planet 49*, that pre-selected checkboxes are insufficient to obtain valid consent for placing cookies on users 'systems, as it does not constitute an unambiguous indication of their wishes.[111]

Finally, consent must be free in that the data subject is offered an effective control over his data and, in the context of RS, has a genuine choice with regard to accepting or declining (without detriments) the terms of the service.[112] However, digital platforms which are the largest users of RS, fail to provide real alternatives for consent, instead presenting the users with a 'take it or leave it' choice.[113] This undermines the requirement for 'free' consent, thus affecting user autonomy and agency. In this case, the users' control is illusory, and consent could be questioned as a basis for the processing of personal data that could be perceived as unlawful.[114]

b. Responsibilities of data controllers and processors

Apart from empowering users by giving them control over their personal data through consent, the GDPR also enhances autonomy by balancing the regulatory burden across the different key actors of the data network

---

[107] Iris van Ooijen and Helena U Vrabec, 'Does the GDPR Enhance Consumers' Control over Personal Data? An Analysis from a Behavioural Perspective' (2019) 42 Journal of Consumer Policy 91, 100.

[108] ibid 7.

[109] Directive 2002/58/EC of the European Parliament and of the Council of July 12, 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] OJ L 201.

[110] Martino Trevisan and others, '4 Years of EU Cookie Law: Results and Lessons Learned' (2019) 2019 Proceedings on Privacy Enhancing Technologies 126, 138.

[111] Case C-673/17 *Verbraucherzentrale Bundesverband eV v Planet49 GmbH* [2019] ECLI:EU:C:2019:801.

[112] European Data Protection Board (n 101).

[113] Varshney (n 39); Helen Nissenbaum, 'A Contextual Approach to Privacy Online' (2011) 140 Daedalus 32; Mariarosaria Taddeo and Luciano Floridi, 'The Debate on the Moral Responsibilities of Online Service Providers' (2016) 22 Science and Engineering Ethics 1575.

[114] European Data Protection Board (n 101) 5.

processing, especially in terms of the need for compliance of the obligations related to the principles, accountability and data subject's rights protection.[115] Data controllers and processors are namely those responsible for processing personal data in compliance with a number of legal principles that seek to establish a general framework that balances the interests of individuals with the controllers' and processors'. For example, art 7 (1) and recital 42 of the GDPR place the burden of demonstrating the compliance with the requirements of valid consent on data controllers. Moreover, even with the person's consent, both data controller and processor still must comply with data protection principles of GDPR's art 5(1) and (2),[116] which are: (a) lawfulness, fairness and transparency; (b) purpose limitation; (c) data minimisation; (d) accuracy; (e) storage limitation; (f) integrity and confidentiality; (2) accountability. Also, the processing must be legitimized by one of the legal bases presented in art 6 (1), attached to specific purposes, and the personal data involved has to be accurate, updated, adequate, relevant and strictly limited to what is necessary for this purpose that was accepted by the user in the moment of consent. Thus, for instance, even in the case of personal data processing in RS based on consent, this would not legitimize the collection of excessive data in relation to a particular purpose.[117] The GDPR requires even stronger compliance when the processing involves "special categories of personal data,"[118] which demands a second layer of legal basis, which are presented in art 9(2)of the GDPR. Therefore, if the RS is based on the processing of sensitive data, it would imply a higher data processing risk which leads to the necessity of enhanced compliance and stronger safeguards. Thus, the GDPR imposes significant obligations and requirements on data controllers in order to preserve and strengthen human autonomy.

c. Data protection rights for empowering individuals

In the monitored, surveilled and data-driven society, the safeguard of individual and collective autonomy online must also rely on a data protection subject's rights, as they derive logically from the aforementioned data protection principles. These rights are intended to empower users to control what happens to their data. Following the GDPR's principle of accountability, the

[115] Alexandra Giannopoulou, 'Algorithmic Systems: The Consent Is in the Detail?' (2020) 9 Internet Policy Review <https://policyreview.info/node/1452> accessed 5 March 2021.

[116] Article 29 Data Protection Working Party (n 100) 13.

[117] Article 29 Data Protection Working Party (n 100).

[118] According to art 9(1) GDPR, special categories of personal data are related to: "Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited".

key actors of RS's data processing will need to demonstrate their compliance with the regulation in general, and specifically that they can provide data subjects' rights through effective mechanisms and internal processes.[119] In that sense, GDPR embodies important data subject's rights, actionable against the controller during all the steps of processing. This includes the moment of creating the profile and also when making the automated decision about the user, based on his profile, with the purpose to recommend items. Even where a user consents to their personal data being processed, for example, the rights of arts 15-20 of the GDPR are still applicable,[120] which enable users to, *inter alia*, supervise the processing of their data and, when necessary, make updates, ask for additional information or even object to the processing of their data.[121]

Among the key rights is the right to be informed. As a consequence of the principle of transparency (art 5(1)(a) and recital 60 GDPR), RS's controllers must proactively inform data subjects about their rights, the existence of data processing and all information related to it, including its purposes, besides a clear, meaningful and understandable explanation of how profile and RS techniques work,[122] which is provided in arts 13 and 14 of GDPR. These provisions encompass the right of the data subjects to receive information from the controller, who has the legal obligation to inform them, even without request. According to art 12, the controller must freely provide information to the data subject, in a concise, transparent, accessible, and easy way, and also facilitate the exercise of their rights under arts 15 to 22, which are: right to access, to rectification, to erasure, to processing restriction, to data portability, to object to processing, and not to be subject to a decision based solely on automated processing.[123]

---

[119] Álvaro Tejeda-Lorente and others, 'Adapting Recommender Systems to the New Data Privacy Regulations' in Hamido Fujita and Enrique Herrera-Viedma (eds), *Volume 303: New Trends in Intelligent Software Methodologies, Tools and Techniques* (IOS Press eBooks 2018).

[120] Article 29 Data Protection Working Party (n 100) 30.

[121] The right to object (GDPR, art 21) does not apply when consent is the legal basis for the processing. However, a similar outcome is possible, since people can withdraw consent at any time, as easy as giving it and without detriments; ibid 21, 22, 30.

[122] Tejeda-Lorente and others (n 119) 16–17.

[123] Shulga-Morskaya (n 94) 8. In the Indian context, most of the above listed rights can be found under the data protection Bill, for a detailed study of this, see Pallavi Bedi, 'Comparison of the Personal Data Protection Bill with the General Data Protection Regulation and the California Consumer Protection Act' (The Centre for Internet & Society 2020) <https://cis-india.org/internet-governance/blog/comparison-of-the-personal-data-protection-bill-with-the-general-data-protection-regulation-and-the-california-consumer-protection-act-2>.

The right to access, under art 15 and recital 63, reinforces the right to information of the previous articles, as it allows individuals to actively request information from the controller. In this sense, people may require confirmation of the existence of personal data processing concerning them and also the presence of automated decision-making for recommendation, which can be used for profiling. Where that is the case, the subject must be able to access his personal data, all information related to its processing and also meaningful information about the logic involved in the automated profiling techniques. This access may also enable the exercise of other important rights (depending on the situation and legal basis), such as rectification to update or amend inaccuracies (art 16 GDPR), erasure (art 17 GDPR), restriction of processing (art 18 GDPR) and object (art 21 GDPR).

In terms of individual self-determination, as an expression of autonomy, the right to information and access to personal data is a powerful instrument, since it provides users with the fundamental basis to understand the processing of their data, the RS's techniques and, thus, to make informed decisions accordingly.[124] In some circumstances, these rights may give people greater knowledge about the logic involved in the recommendations they receive, which allows them to exercise other rights, for example rights of rectification, erasure and portability.[125] According to the European Data Protection Supervisor, the right to data portability would allow people to use data for their own purposes and exercise their option to change information service providers.[126] Thus, it is understood as an expression of individual autonomy and empowerment, as it enables individuals to access and then transfer their personal data from one platform to another, without detriments.[127] This also serves to enhance competition between service providers and could make it an important competitive feature, insofar as how individuals assess and perceive the digital services they can choose from and the adequacy of the treatment of their data. This is confirmed by GDPR's recital 68 that sustains the idea of data portability rights as a form of strengthening users' control over their own data, where the processing happens by automated means. By setting these principles and rights, the GDPR effectively safeguards the power of individuals to exercise their autonomy by managing their data in

[124] van Ooijen and Vrabec (n 107) 94.
[125] ibid 102.
[126] European Data Protection Supervisor, 'EDPS Recommendations on the EU's Options for Data Protection Reform' (European Data Protection Supervisor 2015) 2015/C 301/01 7 <https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:52015XX0912(01)> accessed 30 March 2021; van Ooijen and Vrabec (n 107) 102.
[127] van Ooijen and Vrabec (n 107) 102.

line with their preferences.[128] Moreover, compliance with the GDPR also ensures companies and governments respect and fulfil the individual's rights and freedoms.

ii. Ways to further enhance autonomy

a. Truly informed exercise of rights

Despite the guarantees and protections afforded by the GDPR to individuals to empower them in the control of their personal data, some of its provisions are still difficult or inconvenient for controllers to abide by. One such example is the issue of truly informed consent. In practice, the consent often incorporated in the privacy policies of large platforms can be perceived as ineffective. Instead of empowering users, it operates as a way to legitimize business models of the information economy to "adapt" to the GDPR rules.[129] This scenario may deprive individuals' agency since the consent given by the user is rarely informed in an adequate way, but rather a condition to access the service.[130] Given the impossibility of negotiating the terms of service, people tend to focus on the immediate benefit (access to a product or service online), to the detriment of the possible long-term harm to their privacy, which can reinforce the loss of control over their data.[131] This is especially the case when these platforms embody algorithm-based profiling, nudging and even manipulation, as is the case in RS.

Another reason behind the difficulty of attaining truly informed consent is the challenges for individuals to actually understand how their personal data is processed, and to what end, by AI techniques. These techniques may be technically opaque and unpredictable, considered "black boxes" or may be protected by trade secrecy. Both these types of protections are further discussed in Section III.C and may hinder the right to information and measures of explanation and transparency that are essential to the effective exercise of autonomy through consent and the data subject's rights, mainly those rights associated with information and access. Sophisticated AI algorithms used in RS are not easily explainable to data subjects and sometimes

---

[128] Paul Bernal, *Internet Privacy Rights: Rights to Protect Autonomy* (Cambridge University Press 2014) 14.

[129] Izabella Alves Jorge Bittencourt and Évelyn Vieira Gomes, 'O Consentimento Nas Leis de Proteção de Dados Pessoais: Análise Do Regulamento Geral Sobre Proteção de Dados Europeu e Da Lei Brasileira 13.709/2018' in Fabrício Polido, Lucas Anjos and Luíza Brandão (eds), *Políticas, Internet e Sociedad* (Instituto de Referência em Internet e Sociedade 2019).

[130] Varshney (n 39).

[131] Bioni (n 99).

even for controllers, as the technology may operate in unpredictable ways.[132] Therefore, individuals are placed in a situation of informational, technical and economic asymmetry, where the lack of foresight makes it difficult to ensure informed consent and, consequently, autonomy.[133] Moreover, individuals may also be confronted with the controllers' interests related to intellectual property and industrial secrecy[134] which further obfuscates the information necessary for them to exercise their rights in an informed way.

A possible new e-Privacy Regulation, still in the draft and discussion phase, may help address some challenges around making consent actionable without overwhelming users.[135] On January 5, 2021, despite some criticism,[136] the Portuguese presidency of the Council of the European Union published the 14th draft of the regulation, which is simpler and aligned with the GDPR[137] and would replace the current e-Privacy Directive. In line with the idea of giving greater control to users and thus guaranteeing their autonomy, the draft focuses on consent for the treatment of electronic communication data, a wider category of data than personal data. Consent is required whether for the processing of the content of electronic communication data, metadata or information from the terminal equipment of the user. Although

---

[132] van Ooijen and Vrabec (n 107) 96.

[133] Lilian Edwards and Michael Veale, 'Enslaving the Algorithm: From a "Right to an Explanation" to a "Right to Better Decisions"?' (2018) 16 IEEE Security & Privacy 46.

[134] Wachter and Mittelstadt (n 90) 498–499.

[135] An interesting development in the Indian context is the role of consent managers as proposed under the Personal Data Protection Bill 2019. Consent Managers as envisaged under the Bill act as data fiduciaries that enable data principals to delegate the exercise of their agency. For a detailed study see Samraat Basu and Siddharth Sonkar, 'Regulating Consent Managers in India: Towards Transparency and Trust in the Digital Economy' (Oxford Law Faculty, 1 April 2020) <https://www.law.ox.ac.uk/business-law-blog/blog/2020/04/regulating-consent-managers-india-towards-transparency-and-trust> accessed 15 January 2022.

[136] The German Federal Commissioner for Data Protection and Freedom of Information (BfDI), Professor Ulrich Kelber, criticised the last draft of the e-Privacy Regulation, as he considered it a risk to data protection and privacy. According to the Commissioner's interpretation of the document, the draft would allow the use of cookie walls, which is considered a hindrance in individuals' protection on the internet. Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI), 'BfDI Kritisiert Position Des Rats Zur EPrivacy-Verordnung' (10 February 2021) <https://www.bfdi.bund.de/DE/Infothek/Pressemitteilungen/2021/03_Ratsposition-ePrivacy-VO.html> accessed 30 March 2021.

[137] Dan Cooper and Anna Oberschelp de Meneses, 'Council of the EU Released a (New) Draft of the ePrivacy Regulation' (Inside Privacy, 6 January 2021) <https://www.insideprivacy.com/eu-data-protection/council-of-the-eu-released-a-new-draft-of-the-eprivacy-regulation/> accessed 30 March 2021; Presidency, 'Proposal for a Regulation of the European Parliament and of the Council Concerning the Respect for Private Life and the Protection of Personal Data in Electronic Communications and Repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)' (Council of the European Union, 2021) 5008/21 <https://data.consilium.europa.eu/doc/document/ST-5008-2021-INIT/en/pdf> accessed 30 March 2021.

the draft refers to the GDPR's definition of consent, the document attempts to address some of the problems associated with that consent, such as overloading requests or mandatory consent to access certain services. Among the possible solutions raised in the draft is the possibility of implementing technical means in electronic communications software to allow specific and informed consent through transparent and easy settings for users. Thus, it would allow end users, in a transparent and friendly manner, to manage consent for the storage and access to data stored on their terminal equipment, easily configuring, changing, and withdrawing consent at any time.[138]

b. Greater control over inferred data

Greater transparency and information may be especially important in the case of inferred data where individuals do not directly provide information about themselves, but instead assumptions about them are made on the basis of other data and their behaviour. More control of individuals over the way they are viewed and the assumptions made about them may be desirable. RS may use data to create inferences about a person on the basis of which they make recommendations that may interfere in their behaviour, thus giving rise to a risk to individual reputation, privacy, self-determination and autonomy. Even though the current GDPR framework provides for detailed governance of personal data that could be input into RS, it still lacks protection against how data is subsequently evaluated.[139] Thus, we still face accountability gaps in the GDPR; for instance, for data processing related to inferences that may be inaccurate, biased, and even sensitive.[140] This could especially be a problem in situations where inferences relate to data that would otherwise be considered sensitive, e.g. gender, sexual orientation or religious beliefs. Such inferences could, moreover, be based on anonymous or non-personal data – another type of data not covered by the GDPR but that could nevertheless pose risks to data subjects.[141] To cover these gaps, the GDPR should include not only personal data, but also the accuracy of decision-making processes and the assessment of the reasonableness of inferential analysis carried out by algorithms.[142]

The draft e-Privacy Regulation also demonstrates that safeguards are necessary for data beyond personal data. In its current version, this regulation would be broader than the GDPR, since it is not limited to the processing of

---

[138] Presidency (n 137) 38.
[139] Wachter and Mittelstadt (n 90) 620.
[140] ibid 613.
[141] ibid 615–618.
[142] ibid 615.

personal data; rather, it is applicable to electronic communications data.[143] This incorporates both the content and the metadata of these communications, which may include sensitive information, even if not classified as personal data, such as website visited, geographical location, time, date and duration of some website's use.[144] This information may be used in RS's data processing and monitoring techniques in order to create users, profiles and would now be protected.

Some have suggested the existence of a new right to reasonable inferences, which would also provide for the associated right to challenge unreasonable high-risk assumptions.[145] This possibility would enable individuals to object to certain inferences or the irrelevance, lack of confidence or inaccuracy of data used to create those inferences, going beyond the current right of individuals to rectify their personal data by correcting inaccurate data. As a result, these practices would empower individuals to exercise control over their data, reinforcing the right to access and rectification, while also complementing the right to challenge solely automated decisions, including profiling.[146] This could also help implement in practice the above-mentioned freedom of association that could allow individuals to freely choose which groups or labels they are or are not associated with.

c. Impact assessments going beyond data protection

Another way of enhancing individual autonomy through data protection is by providing actionable tools for those handling personal data to appropriately and lawfully handle data. One option is for providers of RS to implement data protection risk and impact assessments, in accordance with art 35 of the GDPR and as a best practice. The draft e-Privacy Regulation also establishes obligations or advice for the implementation of impact assessments, referring to the already existing art 35 of the GDPR. Even though the legal provisions of the GDPR mainly deal with issues related to privacy, the risks that RS give effect to make it recommendable to go further. RS designers or implementers could implement algorithm audits and algorithmic impact assessments to map the RS risks related to legal compliance and ethical guidelines, human rights, especially autonomy, but also fairness (bias audits), non-discrimination, due process and ensuring the public oversight.[147] Audits can help secure compliance with existing legal and ethical

[143] Cooper and Oberschelp de Meneses (n 137); Presidency (n 137).
[144] Presidency (n 137) 11.
[145] Wachter and Mittelstadt (n 90) 619.
[146] ibid 619–620.
[147] Ada Lovelace Institute and Data Kind UK, 'Examining the Black Box: Tools for Assessing Algorithmic Systems' (Ada Lovelace Institute 2020) 3 <https://www.adalovelaceinstitute.

standards, while algorithmic impact assessment, including algorithmic risk assessment and impact evaluation, may help assess possible societal impacts on the autonomy of RS before and during its implementation in real life.[148] By acting to alleviate any shortcomings identified, risk assessments and audits, particularly through agile design decisions, could serve as valuable governance tools to help RS creators strengthen autonomy and self-determination of their users in practice.

d. Recent legislative initiatives

The recent legislative initiatives of, i.e. the aforementioned DSA and the AI Act, also have a role to play in further developing data governance frameworks and data rights of individuals. As said before, the DSA devoted considerable attention to RS, especially in art 29 and recital 62. This provision addresses "very large platforms" that use RS, requiring them to set their terms and conditions in a clear, accessible, and comprehensible manner to inform users of the RS and, where possible, inform them of options to influence the recommendations. This draft's obligation would empower users through information, being a step beyond the focus of the GDPR on users' ability to exercise control over their data.[149] Although it is noteworthy that the DSA is a first initiative to specifically address RS, the proposal is only applicable to large online platforms and is still vague. It does not explain the possible options that users should have, in terms of influencing recommendations sent to them nor a way to align this with other fundamental rights. For the regulation to effectively give users control over their data in RS, the draft could, for example, require the implementation of democratic and fairer recommender algorithms or enable users to effectively choose between different recommendation algorithms, including from third parties.[150]

In addition, the European Commission has expressed awareness of the need to address the specific challenges that AI systems may create.[151] Thus, the recently proposed AI Act aims to foster the development of an ecosystem

---

org/report/examining-the-black-box-tools-for-assessing-algorithmic-systems/> accessed 6 March 2021.

148 ibid.

149 Natali Helberger and others, 'Regulation of News Recommenders in the Digital Services Act: Empowering David against the Very Large Online Goliath' (Internet Policy Review, 26 February 2021) <https://policyreview.info/articles/news/regulation-news-recommenders-digital-services-act-empowering-david-against-very-large> accessed 30 March 2021.

150 ibid.

151 European Commission, 'Regulatory Framework on AI | Shaping Europe's Digital Future' (*European Commission*, 1 July 2021) <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai> accessed 29 July 2021.

of trust in AI in Europe.[152] RS would fall within the definition of AI within the draft Act[153] and depending on the scope of the RS, it could be classified in one of the four levels of risk created by the AI Act. The proposal follows a risk-based approach, defining the possible uses of AI according to whether they create an unacceptable, high, limited or minimal risk to people's security and fundamental rights. According to recital 14, depending on the intensity and the scope of the risks of AI systems, some systems may be prohibited. Indeed, as was mentioned in the introduction, AI systems developed with a "*significant potential to manipulate persons through subliminal techniques (…) or exploit vulnerabilities (…) in order to materially distort their behaviour in a manner that is likely to cause them or another person psychological or physical harm*" would be prohibited by the AI Act, as they are considered a threat to safety, livelihoods and rights of people. Where manipulative or exploitative practices, facilitated by AI, are not prohibited, the draft proposal points to other potential legal safeguards to ensure individuals are sufficiently informed and can freely choose whether or not to be subjected to profiling that could affect their behaviour - data protection law, consumer protection, or digital services legislation.[154] The latter legislative body, particularly, may soon be modernised in the EU through the DSA. Nevertheless, as we have seen so far, there are gaps in some of these mentioned legal frameworks in terms of the protection they offer against manipulation or influence through RS.

Where the requirements for prohibition are not met, high-risk AI applications are subject to strict requirements of risk management and reporting on data governance, transparency, human oversight, accuracy, robustness, and cybersecurity.[155] Depending on the purposes, the modalities of use and the function performed by the RS, it could be classified as high-risk, as it may create threats to peoples' health, safety or fundamental rights. The list of high-risk AI systems is focused on specific use cases in the fields of biometric identification, management of critical infrastructure, education, employment, access to public services or essential private services, law enforcement,

---

[152] Commission, "Proposal for a Regulation of the European Parliament and of the Council Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts" (n 25).

[153] Recital 6 of the AI Act proposal. Further, the definition is on art 3 (1) of the AI Act: "artificial intelligence system' (AI system) means software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with".

[154] Commission, "Proposal for a Regulation of the European Parliament and of the Council Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts" (n 25) 13.

[155] AI Act, ch 2.

border control, or the administration of justice.[156] The list specifically focuses on systems used to make decisions, and as such, it is an open question whether RS would fall within that scope, given their 'advisory' role in shaping human decision-making. Nevertheless, it is conceivable to imagine RS used to provide rankings that could then be used to prioritise needs and direct resources or workflow, for example, in the context of education or employment.

Where the requirements for meeting the high-risk threshold are also not met, AI systems are subject to significantly fewer obligations; yet, they are important for safeguarding individual autonomy. In such cases, a RS would need to comply with certain transparency obligations, such as the delivery of information to users that they are interacting with an AI, in order to allow their informed decision.[157] The multiple new requirements arising from the AI Act would overall have an impact on the way RS are designed, created, and maintained, and create an incentive to RS's providers to promote compliance by design in the case of RS.[158]

To sum up, the GDPR and other digital technology-related regulations like the draft DSA, the draft AI Act, and the draft e-Privacy Regulation, try to develop a stronger culture of informational self-determination associated with data protection in the context of RS and are important to ensure enhanced control, through the effective exercise of data subjects' rights and lawful consent. For example, after the GDPR adoption and the last amendments in the current e-Privacy Directive, European consumers encountered significantly less unconditional usage of persistent cookies when using the Internet and its services.[159] Already in the early days of the GDPR, in 2018, transparency measures increased 4.9%; more websites had privacy policies and informed their users about cookies practices, data subjects' rights and the legal basis for processing of personal data.[160] Nevertheless, current privacy-related regulations alone might not be considered sufficient to guarantee

---

[156] AI Act, annex III.

[157] AI Act, art 52.

[158] Friederike Reinhold and Angela Müller, 'AlgorithmWatch's Response to the European Commission's Proposed Regulation on Artificial Intelligence – A Major Step with Major Gaps' (AlgorithmWatch, 22 April 2021) <https://algorithmwatch.org/en/response-to-eu-ai-regulation-proposal-2021> accessed 29 July 2021.

[159] Adrian Dabrowski and others, 'Measuring Cookies and Web Privacy in a Post-GDPR World' in David Choffnes and Marinho Barcellos (eds), *Passive and Active Measurement*, vol 11419 (Springer International Publishing 2019).

[160] Martin Degeling and others, 'We Value Your Privacy ... Now Take Some Cookies: Measuring the GDPR's Impact on Web Privacy' (2019) Proceedings 2019 Network and Distributed System Security Symposium <http://arxiv.org/abs/1808.05096> accessed 30 March 2021.

an adequate level of autonomy on matters specific to autonomy and RS. the strengthening of users' protection is necessary and examples exist, such as the changes brought by the new draft of the e-Privacy Regulation, the implementation of limits, obligations and requirements for AI systems in the AI Act (that would be enforced and supervised by the European Artificial Intelligence Board and national authorities within the Member States), and the creation of new rights, such as the right to reasonable inferences. All of these are important steps towards safeguarding autonomy. In parallel, solutions to embed autonomy in the design of RS through the prism of data governance, as well as solutions coming proactively from the private sector,[161] society and technology (for example, the law-by-design approach and its implementation through audits and risk assessments) should be considered and fostered simultaneously.

C. Output: Communication and Transparency

A final aspect where regulation can play a key role in enhancing individual autonomy is through transparency. It is a widely supported principle in AI ethics frameworks[162] and is one of the five OECD AI Principles,[163] endorsed by the G20 countries,[164] as well as a requirement in the EU's Trustworthy AI guidelines.[165] Transparency has also been a key feature of the recently proposed EU AI Act and DSA. Importantly, transparency can play a key role in ensuring and safeguarding individual autonomy in the context of RS. Firstly, there is a positive obligation inherent in the principle of respect for autonomy

---

[161] For example, Google announced the intention to remove support for third-party cookies in their browser Chrome and that the company is working on the development of a Privacy Sandbox to build innovations that would protect anonymity while still delivering results for advertisers and publishers. Google made explicit that it will not replace third-party cookies with alternative identifiers to track individuals as they browse across the web nor use them in their products. The company aims to power their products with privacy-preserving APIs, such as Federated Learning of Cohorts (FLoC) which prevent individual tracking while still delivering results for advertisers and publishers; David Temkin, 'Charting a Course towards a More Privacy-First Web' (*Google*, 3 March 2021) <https://blog.google/products/ads-commerce/a-more-privacy-first-web/> accessed 30 March 2021.

[162] Jessica Fjeld and others, 'Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-Based Approaches to Principles for AI' (*Berkman Klein Center for Internet & Society* 2020) 41 <http://nrs.harvard.edu/urn-3:HUL.InstRepos:42160420> accessed 6 April 2021.

[163] OECD, 'Recommendation of the Council on Artificial Intelligence' (25 May 2019) <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449> accessed 5 March 2021.

[164] G20, 'G20 Ministerial Statement on Trade and Digital Economy' (8 June 2019) 20 <https://trade.ec.europa.eu/doclib/docs/2019/june/tradoc_157920.pdf> accessed 5 March 2021.

[165] High-Level Expert Group on Artificial Intelligence, 'Ethics Guidelines for Trustworthy AI' (2019) <https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines> accessed 27 April 2020.

to disclose information necessary to foster autonomous decision-making.[166] Agency is necessary for autonomy and it requires that individuals have sufficient understanding of the environment within which they decide and act, as well as of the meaning and consequences of their decisions.[167] This is reflected, for example, in the notion of informed consent in the GDPR and elaborated in the previous section.[168] Secondly, transparency can safeguard individual freedom by ensuring individuals can control or hold accountable those who may exert control or influence over them, thus further safeguarding self-determination and autonomy. Transparency can also serve to enhance the quality and impact of RS. Explaining to users how an individual recommendation has been made may enhance trust and acceptance by users.[169] Moreover, understanding the model's operation can empower users to adjust their interaction with the RS to produce more desirable recommendations,[170] ultimately improving the service.

Transparency is, however, not a simple matter to regulate. First, what transparency means and what it covers is not a straightforward question. Moreover, transparency may conflict with protecting commercially sensitive or valuable information, as well as private information regarding other users. How to present information so that it is understandable to its target recipients and who they are is a further challenge. Therefore, a nuanced consideration is necessary in order to ensure transparency of RS appropriately safeguards individual autonomy. We define transparency as the availability of information about an actor's workings or performance that allows monitoring or control from others[171] in order to focus on its role as a tool of accountability. In the rest of this section, we explore the current state of transparency regulation and explore how it interacts with the domains of intellectual property law, data protection law, as well as how it is represented in the recently proposed draft Digital Services Act and AI Act. We then present the questions that regulators will methodically and purposefully need to tackle, in order to shape transparency to effectively yet proportionately safeguard individual autonomy.

---

166 Beauchamp and Childress (n 39) 104.

167 ibid 102.

168 GDPR, art 6(1)(a).

169 Henriette Cramer and others, 'The Effects of Transparency on Trust in and Acceptance of a Content-Based Art Recommender' (2008) 18 User Modeling and User-Adapted Interaction 455.

170 Donghee Shin, 'User Perceptions of Algorithmic Decisions in the Personalized AI System: Perceptual Evaluation of Fairness, Accountability, Transparency, and Explainability' (2020) 64 Journal of Broadcasting & Electronic Media 541, 549.

171 Albert Meijer, 'Transparency' in Mark Bovens, Robert E Goodin and Thomas Schillemans (eds), *The Oxford Handbook of Public Accountability* (Oxford University Press 2014).

i. State of the art concerning transparency obligations

a. Intellectual property law

Transparency of RS can both be facilitated and hindered by intellectual property (IP) law. Patents grant privileged rights to innovators in exchange for transparency that fosters scientific progress by sharing valuable and breakthrough insights. Mechanisms used in recommender and ranking systems may be patented[172] which could be a building block of their transparency. However, there are barriers to relying on patents for transparency. Firstly, the patentability of AI and ML is a matter of ongoing debate. The European Patent Convention excludes 'programs for computers' from being patentable inventions[173] and artificial intelligence and machine learning may be considered too abstract in nature to be patentable.[174] However, specific models that deliver a technical effect, such as targeting content to individuals in a particular manner, may be patentable if sufficiently innovative.[175] Secondly, even if patentable, the transparency provided by patents is targeted at experts, not average users. Disclosure need only be 'sufficiently clear and complete for it to be carried out by a person skilled in the art'.[176] This suggests extending software patentability may be part of the solution, but the transparency it provides, while valuable in advancing science, does not, as it stands, facilitate transparency to non-experts and lay persons. Finally, even where patents could deliver some form of transparency, the exclusive rights conferred on innovators are likely to hinder competition and, thus, limit consumer choice and, by extension, the ability of individuals to exercise autonomy when choosing a recommender system.

Where RS are not patentable, innovators may look to other forms of protection. Copyrighting of the AI code can offer limited protection, since it does not extend to the principles and mechanics underlying the software, but

---

[172] Examples of patented recommendation and ranking algorithms include Google's PageRank, Facebook's newsfeed, and Amazon's multiple recommender system. Lawrence Page, 'Method for Node Ranking in a Linked Database'; Mark Zuckerberg and others, 'Communicating a Newsfeed of Media Content Based on a Member's Interactions in a Social Network Environment'; Jennifer A Jacobi, Eric A Benson and Gregory D Linden, 'Personalized Recommendations of Items Represented within a Database.'

[173] Convention on the Grant of European Patents of October 5, 1973 as revised by the Act revising Article 63 EPC of 17 December 1991 and the Act revising the EPC of November 29, 2000 (European Patent Convention) (adopted 5 October 1973) OJ EPO 2001, Special edition No. 4, 55, art 52(2)(c).

[174] European Patent Office, 'Guidelines for Examination in the European Patent Office' (March 2021) <https://www.epo.org/law-practice/legal-texts/html/guidelines/e/index.htm> accessed 31 March 2021 Part G, Chapter II, Point 3.3.1.

[175] ibid Part G, Chapter II, Point 3.3.

[176] European Patent Convention, art 83.

rather just to the code as such.[177] Similar to how copyright protects written works of art, the words of Shakespeare's Romeo and Juliet as they are written are protected from being copied, however the story of two tragic lovers from rival families can be retold with different words and small changes to the story. In this same manner, copyright law cannot sufficiently protect the 'ideas' of how particular AI technologies operate, but rather simply protect their code, word-for-word. Handling AI models as trade secrets is often the choice of innovators. Trade secrets protect any information that is commercially valuable, including a method of production or an algorithm formula,[178] for as long as reasonable steps to keep it secret are maintained.[179] Perhaps the most notorious example of the conflict between transparency and trade secrets came with the US case of *Loomis v Wisconsin*, where a criminal defendant was denied access to a risk scoring algorithm used to inform the judge's decision in the case.[180] That case illustrates the tension between human rights and trade secrets. Such lack of transparency could place algorithms beyond the reach of legal assessments.[181] IP law, thus, can present a challenging field of law to navigate when discussing RS transparency to support individual autonomy. It either does not facilitate transparency for end users and non-experts or it hinders transparency overall.

b. Data protection law

Transparency is also a key principle of personal data processing according to art 5(1)(a) of the GDPR - the principle of lawfulness, fairness, and transparency and, in that capacity, could help individuals understand more about what personal data of theirs is processed, how, and what rights they have in that regard. Recital 60 of the GDPR clarifies the obligation of data controllers to provide individuals with information that would be 'necessary to ensure fair and transparent processing.' This is further detailed in the regulation with a number of proactive transparency and disclosure requirements, as well as with rights on individuals to demand information (the right to access). All information regarding 'risks, rules, safeguards and rights' related

---

[177] Recital 11, Art 1(2) Directive 2009/24/EC on the legal protection of computer programs (Software Directive) [2009] OJ L 111, 16.

[178] Brian T Yeh, 'Protection of Trade Secrets: Overview of Current Law and Legislation' (*Congressional Research Service* 2016) <https://fas.org/sgp/crs/secrecy/R43714.pdf> accessed 6 March 2021.

[179] Art 2(1)(c) Directive (EU) 2016/943 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure [2016] OJ L157, 1.

[180] *Loomis v Wisconsin,* 881 NW2d 749 (Wis. 2016), cert. denied, 137 S Ct 2290 (2017)

[181] Woodrow Barfield and Ugo Pagallo, *Advanced Introduction to Law and Artificial Intelligence* (Edward Elgar Publishing 2020) 171 et seq.

to personal data processing and how to exercise rights should be clearly communicated with individuals.[182] Individuals should also be made aware of the existence and consequences of profiling,[183] particularly relevant to the manner of operation of RS. This information could, in theory, enhance individual awareness of external influences, however users often do not read the privacy policy documents where this information is recorded[184] and when they do, they might be confronted with vague or complicated text.

The GDPR could also provide individuals with glimpses into the process behind the creation and operation of the RS. The GDPR allows individuals to know how and by whom their personal data is handled and managed,[185] and also the purpose of the processing,[186] and they could receive copies of the personal data controllers hold about them.[187] This might help answer who, and for what reason, is processing personal data or profiling individuals, thus seeking to influence them. But there are limitations. Firstly, the specified purpose of processing might not reveal the specific goal of RS used. If personal data is collected to help improve a service, it is not clear what a RS would optimise for in order to improve such a service. Secondly, these rights would not allow individuals to know which of all of their personal data that is held by a controller are actually used or influential for the performance of RS. This limits the insight into the RS's logic that users could gain through data protection rights.

Finally, the GDPR could also limit what information about RS could be provided to individuals. It protects personal data from unauthorised disclosures.[188] Training data is of vital importance to the performance of ML algorithms, often used in RS. For that reason, it is important to consider whether, and to what extent, training data should form part of relevant transparency obligations, with due regard to the data protection rights of individuals whose data may form part of such training data. Thus, the European data protection law, as it currently stands, also leaves potential gaps in terms of the use of transparency to support individual autonomy in a RS context.

---

[182] GDPR, arts 13(2), 14(2); Recital 39.
[183] GDPR, recital 60.
[184] Jonathan A Obar and Anne Oeldorf-Hirsch, 'The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services' (2020) 23 Information, Communication & Society 128; Nili Steinfeld, '"I Agree to the Terms and Conditions": (How) Do Users Read Privacy Policies Online? An Eye-Tracking Experiment' (2016) 55 Computers in Human Behavior 992.
[185] GDPR, arts 13(1)(a), 14(1)(a); Recital 39.
[186] GDPR, arts 13(1)(c), 14(1)(c); Recital 39.
[187] GDPR, art 15(3).
[188] GDPR, art 5(f).

c. Digital Services Act

The draft DSA also promotes transparency, particularly in RS. It requires *very large* online platforms to disclose in a clear and accessible manner 'the main parameters used in their recommender systems.'[189] Transparency and usability, where there are options for users to modify or adjust the parameters of the RS, are also highlighted.[190] Here, transparency is used to empower users not only to understand the logic of the RS, but also to ensure that they can shape it. The DSA also makes strides with regard to targeted advertising transparency. Online advertisements are required to be clearly marked as such, notably including information on the identity of the natural or legal persons behind them, as well as 'meaningful information about the main parameters used to determine the recipient' of the advertisement.[191] While consumer protection law already mandates advertisements to be clearly marked,[192] this obligation would allow insights into the purpose and manner in which advertising seeks to target and influence individuals. Very large platforms would also have to publish aggregate data about advertising, including who ordered the advertisement, the intended recipients, as well as the number of recipients.[193] This might facilitate public accountability and research regarding advertising practices.

The draft DSA also proposes transparency obligations that shed light on the manner in which online platforms operate. A general obligation to be transparent about content moderation and handling of illegal content is discussed.[194] In addition, reporting duties for very large platforms are proposed, covering *inter alia* their assessments of systemic risks arising out of their RS and targeted advertising systems[195] and proportionate and effective risk mitigation steps they have taken, including adapting their RS.[196] The performance of this and other obligations is subject to independent auditing[197]

---

[189] DSA, art 29(1).
[190] See s III.A. above and DSA, art 29.
[191] DSA, art 24.
[192] Arts 2(b), 3 Directive 2006/114/EC of the European Parliament and of the Council of 12 December 2006 concerning misleading and comparative advertising (codified version) 2006 [32006L0114] 21. ''Native Advertising: A Guide for Businesses | Federal Trade Commission' (*Federal Trade Commission*, December 2015) <https://www.ftc.gov/tips-advice/business-center/guidance/native-advertising-guide-businesses> accessed 6 March 2021; 'How to Comply with EU Rules Applicable to Online Native Advertising' (*IAB Europe,* 2016) <https://iabeurope.eu/wp-content/uploads/2019/08/IAB-Europe-Online-Native-Advertising-Guidance.pdf> accessed 6 March 2021.
[193] DSA, art 30.
[194] DSA, art 13.
[195] DSA, arts 26, 33.
[196] DSA, arts 26, 27(1)(a), 33.
[197] DSA, arts 28(3), 33.

and reporting, also subject to disclosure.[198] The information that has been revealed to the public may be redacted to protect commercially confidential information or the privacy of other users, but would still be accessible to EU authorities.[199] Such disclosures could allow some transparency to users about the RS used and the way in which they operate, although it might be redacted or technical. However, public oversight through EU authorities would be ensured. This is a clear move towards embedding transparency into the operation of very large platforms with a prominent role for transparency of RS. However, even here, the types of transparency presented and their intended audiences are not all intended to safeguard the autonomy of individual users. Rather, the transparency obligations are framed as a way to ensure public oversight over the operation of highly impactful platforms.

d. The AI Act

The recently proposed EU AI Act also lays down a number of requirements and obligations regarding the transparency and oversight of AI systems. Most of these obligations, however, only apply to systems which are classified as 'high risk.'[200] If RS meet this standard, then a range of transparency requirements would apply to them, including a documented and maintained risk management system,[201] design that is "sufficiently transparent to enable users to interpret the system's output and use it appropriately"[202] and that allows for human oversight[203] and technical documentation demonstrating compliance with high-risk AI requirements.[204] These requirements include information about the overall process of the system's creation, maintenance and oversight, relevant metrics, risks, and the system's design specifications, general logic, and "the key design choices including the rationale and assumptions made."[205] Thus, in the AI Act there are transparency obligations that cover both– the process of the system's creation, as well as its internal logic, architecture, performance and even extend to aspects of human-computer interaction (HCI). A publicly accessible EU database of high-risk AI systems is also envisioned, albeit containing less detailed information.[206] The draft AI Act also provides for some transparency obligations for AI systems that are not considered to be high-risk, however, these are more modest. For

[198] DSA, arts 28(4), 33.
[199] DSA, art 33(3).
[200] AI Act, annex III.
[201] AI Act, art 9.
[202] AI Act, art 13(1).
[203] AI Act, art 14.
[204] AI Act, art 9.
[205] AI Act, annexes IV.2.b and IV.
[206] AI Act, art 60.

example, where natural persons interact with AI systems, they are informed of their AI nature.[207] This makes some, but not fully sufficient, progress towards ensuring individuals have enough information about RS to be aware of and fully understand the way RS influence them. Even if RS are considered "high-risk," not all of the information maintained about them is intended to be accessible to end-users or the public. Some of it is reserved for enabling oversight by public authorities, subject to appropriate confidentiality safeguards.[208] Nevertheless, a strong link to individual autonomy is the requirement to design "high-risk" AI systems in a manner that ensures humans can understand and use their outputs, thus putting users in an empowered position. There is, however, scope to further consider and develop transparency requirements for safeguarding autonomy of RS users.

ii. Towards more meaningful transparency

Transparency obligations as well as limitations to transparency exist in a piecemeal manner across multiple legal frameworks. However, a coherent and purposeful approach would be necessary, using individual autonomy as the guiding "North Star" and goal of transparency. At the same time, regulating transparency also has to take into account competing interests, e.g. IP law, that may justify limited disclosure of information. This will require defining transparency and its relevant dimensions – scope of disclosure, obligations and rights, proactive or demand-driven disclosure, and intended recipients – in a purposeful manner that allows users to autonomously make their own informed decisions and also enables them to hold those that seek to influence them accountable. This could be done by (1) mediating the type and *content* of transparency obligations – both in terms of what is disclosed, as well as how it is disclosed, or (2) by moderating the *recipients* of information. These two aspects are interlinked, as information disclosed to a particular recipient should be understandable and usable by its intended recipient. Below, we highlight some of the challenges future regulation should account for.

a. Defining the scope of transparency purposefully

A first step for regulators would be to define what transparency should cover, with a view towards achieving specific objectives or goals. The content of disclosures may depend on the individual case – on its context and impact of the disclosure, as well as on the intended recipients of the information

[207] AI Act, art 52(1).
[208] AI Act, arts 64(6), 70.

and their goals.[209] Having a clear view of what functionalities transparency should fulfil will help ensure that it is balanced and proportionate *vis-a-vis* competing interests. Regulators can then choose from a range of transparency options. A fundamental question is whether the goal of transparency is to inform end users and, thus, facilitate informed decision-making, or is it to facilitate human oversight of RS with the goal of indirectly protecting individual autonomy? Ideally, a complementary approach should be taken, taking advantage of the strengths of both approaches. For example, transparency can be achieved by providing information that does not infringe on trade secrets. Users can receive explanations about the RS's operation or a specific recommendation that allow them to understand the context and consequences of their actions, but that are not technical to the extent of breaching trade secrets.[210] Alternatively, if technical disclosures are necessary for an assessment of the RS, this may be done by limiting disclosure to authorised and independent organisations, similar to what is already practiced where public authorities examine commercially sensitive data, such as in IP litigation. There are mechanisms to allow the disclosure of sensitive information sufficiently to enable human control and oversight. Ideally, transparency regulation will seek to combine the strengths and complementarity of both approaches.

Once there is a clear goal for transparency to fulfil, regulators would need to narrow down the precise definition and scope of transparency that would allow them to achieve it. When it comes to a particular RS, we can differentiate between disclosing information about (1) the process of the creation of the RS - *process transparency* and (2) the results of the process - the system, its data and logic, performance, and results - *outcome transparency*.[211] Then, regulators need to consider what is *knowable* about algorithmic systems to identify the scope of desirable disclosure. What we can know about an algorithm includes information about (1) human involvement and decisions made in the creation and implementation of a system, assumptions, goals, intents; (2) about the type, features, qualities, provenance and legal terms for the use of the data, as well as its management; and (3) about the model itself – its type, performance metrics, metadata (date, version), thresholds, assumptions, rules it includes, along with influential variables and weighting if

[209] Alan FT Winfield and Marina Jirotka, 'Ethical Governance Is Essential to Building Trust in Robotics and Artificial Intelligence Systems' (2018) 376 Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences 20180085.

[210] Céline Castets-Renard, 'The Intersection Between AI and IP: Conflict or Complementarity?' (2020) 51 IIC - International Review of Intellectual Property and Competition Law 141.

[211] David Leslie, 'Understanding Artificial Intelligence Ethics and Safety: A Guide for the Responsible Design and Implementation of AI Systems in the Public Sector' (*Zenodo* 2019) <https://zenodo.org/record/3240529> accessed 27 April 2020.

known.[212] Regulators need to consider which of this information they would like disclosed to whom and in what shape in order to safeguard autonomy. As we saw above, the current and proposed legal framework provides for a tapestry of transparency and disclosure obligations.

Aspects of both outcome and process transparency are necessary to safeguard autonomy. Outcome transparency is key to support individual agency by highlighting how individual autonomy may be impacted. It could incorporate information about the model and how and why it operates. The Consultative Committee on the Council of Europe's Convention Hundred and Eight suggests that in order to enable public scrutiny, a reasonable solution could be disclosures of the logics of an AI algorithm in general, covering its overall operation, the type of expected input and output data, the variables and weights used by the algorithm, as well as details about its architecture.[213] Moreover, previous work on transparency in the context of nudging highlights the need for being transparent that a particular technique of nudging is used to achieve a particular goal,[214] as well as highlighting specific instances of nudging, making them identifiable to nudgees.[215] This is in line with the requirement in the EU's Guidelines for Trustworthy AI that AI systems be clearly identified as such to end-users along with information on the system's capabilities, limitations, and purpose[216] and can be encompassed within outcome transparency.

Instead, process transparency is vital to ensure accountability of those designing and creating RS and justifiability of the design choices made, for example what a RS is optimising for and which user data it considers influential. It could cover information about the human involvement in the RS's creation, as well as the data used and decisions made to tailor and optimise

---

[212] Nicholas Diakopoulos, 'Transparency' in Markus D Dubber, Frank Pasquale and Sunit Das (eds), *The Oxford Handbook of Ethics of AI* (Oxford University Press 2020) 201 et seq .

[213] Alessandro Mantelero, 'Artificial Intelligence and Data Protection: Challenges and Possibilities' (Consultative Committee of the Convention for the protection of individuals with regard to automating processing of personal data (Convention 108)) T-PD(2018)09Rev <https://rm.coe.int/artificial-intelligence-and-data-protection-challenges-and-possible-re/168091f8a6> accessed 6 March 2021.

[214] Cass R Sunstein, 'The Ethics of Nudging' (2015) 32 Yale Journal on Regulation 413; Luc Bovens, 'The Ethics of Nudge' in Till Grüne-Yanoff and Sven Ove Hansson (eds), *Preference Change: Approaches from Philosophy, Economics and Psychology* (Springer Netherlands 2009).

[215] Lembcke and others (n 16) 11.

[216] High-Level Expert Group on Artificial Intelligence (n 165) 18; High-Level Expert Group on Artificial Intelligence, 'Assessment List for Trustworthy Artificial Intelligence (ALTAI) for Self-Assessment' (2020) Text 14 <https://ec.europa.eu/digital-single-market/en/news/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment> accessed 6 March 2021.

the model. Transparency of the data used is highlighted in a number of policies. In the EU's Guidelines for Trustworthy AI transparency should cover data traceability and provenance.[217] The Council of Europe, in its Report on AI, similarly highlights that transparency of data used to train and operate an algorithm.[218] Where information about the logic of operation of a RS may be unknowable due to its complexity (see point 2.c. below), process transparency could offer an important replacement mechanism of checks and balances. As the EU's Guidelines on Trustworthy AI suggest, where explanations of the way systems operate are not possible, other types of transparency should be prioritised.[219]

b. Understandable disclosure formats

The goal of regulating for transparency should be to provide higher quality information rather than simply "more" information.[220] Information should be provided to its intended recipients in a useful manner and, following the example of the GDPR, should be easily accessible, understandable, concise, using "clear and plain language."[221] Regulation could standardise procedures and formats for disclosure,[222] including by considering mechanisms like standardised icons, certification schemes or seals.[223] Research from human-computer interaction (HCI) could help shed light on how information can be intuitively presented[224] or to help identify what explanations users and experts think are necessary, as well as how they can be provided.[225] In fact, there are already some existing tools that could help communicate

---

[217] High-Level Expert Group on Artificial Intelligence (n 165) 18.
[218] Mantelero (n 213) 11–12.
[219] High-Level Expert Group on Artificial Intelligence (n 216) 14–15.
[220] Rolf H Weber, 'Socio-Ethical Values and Legal Rules on Automated Platforms: The Quest for a Symbiotic Relationship' (2020) 36 Computer Law & Security Review 36:105380, 7.
[221] GDPR, art 12(1), Recitals 39, 58.
[222] Diakopoulos (n 212) 211.
[223] GDPR, art 12(7), Recital 100.
[224] Jaron Harambam and others, 'Designing for the Better by Taking Users into Account: A Qualitative Evaluation of User Control Mechanisms in (News) Recommender Systems', *Proceedings of the 13th ACM Conference on Recommender Systems* (*ACM* 2019) <https://dl.acm.org/doi/10.1145/3298689.3347014> accessed 6 March 2021; Chen He, Denis Parra and Katrien Verbert, 'Interactive Recommender Systems: A Survey of the State of the Art and Future Research Challenges and Opportunities' (2016) 56 Expert Systems with Applications 9; Dietmar Jannach, Sidra Naveed and Michael Jugovac, 'User Control in Recommender Systems: Overview and Interaction Challenges' in Derek Bridge and Heiner Stuckenschmidt (eds), *E-Commerce and Web Technologies: 17th International Conference, EC-Web 2016, Porto, Portugal, September 5-8, 2016, Revised Selected Papers*, vol 278 (Springer International Publishing 2017).
[225] Malin Eiband and others, 'Bringing Transparency Design into Practice', *23rd International Conference on Intelligent User Interfaces* (*ACM* 2018) <https://dl.acm.org/doi/10.1145/3172944.3172961> accessed 6 March 2021.

outcome and process transparency. For outcome transparency, information about models can be provided through model cards, with an overview of model performance, its intended uses, limitations, and key architectural features.[226] Data transparency can be achieved by sharing 'definitions and meanings of variables in the data, as well as how they are measured'.[227] Documents like Datasheets or Dataset Nutrition Labels can play a role to record qualities of the data, as well as rationale for human manipulations.[228] Moreover, transparency of specific instances of recommendations could be achieved by highlighting them through the use of borders around elements or textual notifications. More research will be necessary to determine when digital elements on a page constitute a 'nudge' and how to best (visually) represent this to make individuals aware of it.[229] This may, however, be necessary especially for the DSA-proposed transparency and highlighting of targeted advertising. On the other hand, process transparency that provides insights into the creation of RS is also desirable. Information on human involvement can be collected progressively throughout the process of RS creation through end-to-end documentation intended to support accountability and auditability.[230] Relevant aspects for communication to individuals or authorities can then be extracted. This may require changes to internal work processes; however, this is nothing new. Legal acts, including the GDPR, often require both technical and organisational measures for compliance with their obligations.[231] It is important, however, that transparency regulation considers how to ensure disclosed information is useful and fit for purposes of safeguarding autonomy.

c. Explainability and oversight

A final challenge that transparency regulation must tackle is the potential use of complex ML systems in ML. Where sophisticated ML algorithms are used, it may be impossible to know how and why systems operate the

---

[226] Margaret Mitchell and others, 'Model Cards for Model Reporting' (2019) Proceedings of the Conference on Fairness, Accountability, and Transparency 220.

[227] Diakopoulos (n 212) 203.

[228] Timnit Gebru and others, 'Datasheets for Datasets' [2020] arXiv:1803.09010 [cs] <http://arxiv.org/abs/1803.09010> accessed 6 March 2021; Sarah Holland and others, 'The Dataset Nutrition Label: A Framework to Drive Higher Data Quality Standards' [2018] arXiv:1805.03677 [cs] <http://arxiv.org/abs/1805.03677> accessed 6 March 2021.

[229] Lembcke and others (n 16) 11.

[230] Inioluwa Deborah Raji and others, 'Closing the AI Accountability Gap: Defining an End-to-End Framework for Internal Algorithmic Auditing', *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency* (*ACM* 2020) <https://dl.acm.org/doi/10.1145/3351095.3372873> accessed 6 March 2021.

[231] GDPR, Recital 78.

way they do[232] or how and why an individual has been classified a certain way and, therefore, receives a certain algorithmic output.[233] This problem, labelled 'black box' AI, addresses the necessity of explainable AI for trust and legal accountability.[234] Where AI is unexplainable, some types of transparency may be difficult to realise. However, there are two possible solutions. First, regulators may consider whether there is a need to limit the use of unexplainable and uninterpretable AI models.[235] Depending on the context, interpretability and transparency of AI models may be prioritised to ensure the legal compliance[236] of RS models used. For example, in the draft AI Act, high risk AI systems and their outputs have to be sufficiently interpretable to be used appropriately.[237] Some argue that interpretable models may perform just as well as 'black box' models,[238] with some initial supportive research in the area.[239] Second, where RS are uninterpretable, other information about the RS is still knowable. *Process transparency* is always possible. We might also disclose an algorithm's purpose or optimisation goal, design and basic functionalities,[240] such as the model's architecture and performance and could even cover the data processed on an individual basis. This information could be provided for oversight by sufficiently resourced public authorities. For example, "professional means, such as external auditors assessing the

[232] Lembcke and others (n 16) 10.

[233] Jenna Burrell, 'How the Machine "Thinks": Understanding Opacity in Machine Learning Algorithms' [2016] 3 Big Data & Society 205395171562251.

[234] Giulia Vilone and Luca Longo, 'Explainable Artificial Intelligence: A Systematic Review' [2020] arXiv:2006.00093 [cs] <http://arxiv.org/abs/2006.00093> accessed 6 March 2021; Finale Doshi-Velez and others, 'Accountability of AI Under the Law: The Role of Explanation' [2019] arXiv:1711.01134 [cs, stat] <http://arxiv.org/abs/1711.01134> accessed 6 March 2021; Finale Doshi-Velez and Been Kim, 'Towards A Rigorous Science of Interpretable Machine Learning' [2017] arXiv:1702.08608 [cs, stat] <http://arxiv.org/abs/1702.08608> accessed 6 March 2021.

[235] Lembcke and others (n 16); Burrell (n 233); Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (1st edn, Harvard University Press 2015).

[236] German AI Strategy specifically mentions the need for transparency in the way AI operates and produces outputs – the "criteria, objectives, logic" to assess compliance with legal requirements, including that of non-discrimination. German Federal Government, 'Artificial Intelligence Strategy' (2018) 16, 38 <https://www.ki-strategie-deutschland.de/home.html>.

[237] AI Act, art 13(1).

[238] Cynthia Rudin, 'Stop Explaining Black Box Machine Learning Models for High Stakes Decisions and Use Interpretable Models Instead' (2019) 1 Nature Machine Intelligence 206; Cynthia Rudin and Joanna Radin, 'Why are we Using Black Box Models in AI When we don't need To? A Lesson From an Explainable AI Competition' (2019) 1 Harvard Data Science Review <https://hdsr.mitpress.mit.edu/pub/f9kuryi8> accessed 6 March 2021.

[239] Elaine Angelino and others, 'Learning Certifiably Optimal Rule Lists for Categorical Data' [2018] arXiv:1704.01701 [cs, stat] <http://arxiv.org/abs/1704.01701> accessed 8 April 2021.

[240] Cary Coglianese and David Lehr, 'Transparency and Algorithmic Governance' (2019) 2123 Faculty Scholarship at Penn Law 1.

code (…) or (…) interdisciplinary partnerships" can be ways to ensure the ethical justifiability of uninterpretable algorithms used to shape individual choices.[241] The key is to provide information that enables meaningful human control that could then itself consider the impact of the system on autonomy.

In conclusion, transparency is a potentially powerful tool to safeguard autonomy; and has multiple dimensions that can be moulded by a regulator to achieve a desired purpose of enhancing autonomy. Technology-specific challenges of RS, such as uninterpretability, do not pose a barrier to all relevant transparency, nor do legal challenges, such as IP law or data protection law. By shaping the scope of transparency, its intended percipients, and usability, regulators could create a coherent framework to utilise the potential of algorithmic transparency for autonomy.

IV. Conclusion

Recommender systems, by their very nature and intended use, affect individual autonomy and, boosted by profiling and micro targeting, are able to shape human thought and action. Ultimately, this affects individual and collective autonomy and self-determination, as well as human rights. The current regulatory framework, as it exists, leaves gaps in terms of ensuring accountability and oversight of the creation, use, operation, and impacts of RS. Exercising such power, however, cannot be permissible without appropriate checks and balances. In this paper, we mapped the current and recent European legislative trends with relevance to RS and their impact on autonomy to highlight how, through different angles and with different justifications, there is a clear indication that this is an issue very much on the policy agenda. We proposed a set of considerations and possibilities for the future development of a regulatory framework that can appropriately control the exercise of such power over user autonomy. We structured our analysis to address RS's design (Section III.A), the data they use (Section III.B), and the information about them which is presented to end users or qualified third parties (Section III.C). Key steps that can serve to safeguard or promote individual autonomy are possible at each of these junctions in the creation and operation of RS.

A possible autonomy-by-design approach could empower the self-determined and directed use of RS by individuals, aligning RS with the general preferences of users. This can be enabled *inter alia* by architectures of user control, user shaping algorithms or choosing between algorithms. This idea

[241] Lembcke and others (n 16) 10; Pasquale (n 235); Burrell (n 233).

is already foreshadowed in current legislative proposals and in projects in the IT-industry. Moreover, technical additions or modifications of RS may also diminish the manipulative impact that RS have on individual experiences, e.g., by including serendipity or randomisation techniques. A rights-based approach could also empower users to control the way their data is processed and their digital reflections and the GDPR can help mitigate some of the risks created by RS[242] through the data subjects' rights and principles and obligations for controllers it establishes. However, as seen throughout this article, there are still blind spots, for instance, in terms of effective application in practice or control of individuals over inferences made about them, meaning that individuals cannot fully control the processing of their data by RS, nor the impact RS have on them. Additional consideration of impact assessments, audits, greater transparency, freedom of choice, and even new rights may be necessary to effectively close this gap. Finally, transparency, through its role in empowering user choice, understanding, and accountability of RS creators and deployers, also has a vital role to play. Yet, it has to be regulated in a complex landscape of overlapping and conflicting interests and obligations that include IP law, data protection law, and features of complex AI technologies. Nevertheless, a push towards transparency is visible in the recent legislative initiatives in the EU. To help regulators think through this complex field going forward, we emphasise the need for purpose-driven regulation and build a taxonomy of the diversity of information, recipients, and forms of disclosure that regulators can consider when shaping their policy.

The regulatory options we have highlighted should not prejudice other complementary and vital efforts. One such effort is investing in digital literacy and education to enhance people's awareness and knowledge about artificial intelligence,[243] especially regarding the harms, benefits and effects of the most common applications that track, target and categorize individuals (RS, for instance). It is vital to reduce information asymmetries, empower users and make them more prepared to deal with these technologies, ensuring their rights and informational self-determination. Another example is interdisciplinary training of data scientists that could improve the value-driven design of technology in practice. Currently, discrepancies between formal legal requirements and the real practice can reduce the GDPR to

[242] Access Now, 'Human Rights in the Age of Artificial Intelligence' (2018) 30 <https://www.accessnow.org/cms/assets/uploads/2018/11/AI-and-Human-Rights.pdf> accessed 31 March 2021.

[243] Commission, 'Digital Education Action Plan 2021-2027: Resetting Education and Training for the Digital Age' (European Commission 2020) COM(2020) 624 final 4 <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0624&from=EN>.

a formality.[244] It requires a more granular application of its rules,[245] in a "user-centric design".[246] Careful in-depth consideration throughout the process of technology design and implementation is necessary in order to ensure desirable social outcomes are achieved and relevant legal standards or goals are met. In order to safeguard individual autonomy from the continuous shaping and moulding exerted by RS online, regulators and policy-makers need to think holistically about the different dimensions of regulation, as well as the entirety of the RS— from their creation and design, through their deployment, until their final use and interaction with human beings.

Whether it is a law-by-design approach that seeks to shape RS design, a rights-based approach to empower users to control how they are perceived and profiled by RS, or a focus on processes and procedures to correct asymmetries in information and power between creators and users of RS through transparency measures, there are a range of tools available to policy makers. Like any regulation, turning these ideas into a regulatory framework would require balancing competing interests. Despite the potential challenges, there needs to be a clear stance about the priority of individual autonomy as a value that is worth pursuing and protecting. Autonomy and self-determination, both individual and collective, underpin fundamental values in our social and legal orders, including the rule of law, democracy, and human rights. As the digital increasingly shapes large parts of our lives, the protection of autonomy needs to be expanded and cover operation of innovations exerting 'soft power' over us like RS. Using the goal of individual autonomy as a North Star to aim for, policy-makers could shape a purposeful regulatory space that ensures truly human-centred technology. This is a young and dynamic field of research, however, and more is undoubtedly to come. New policy developments, such as the drafts of the Digital Services Act, the AI Act, and the e-Privacy Regulation, clearly highlight that there is political will to act and shape technology instead of simply allowing it to shape us. To make these attempts meaningful, it is important to focus on autonomy through different means.

---

[244] Giannopoulou (n 115) 4–6.

[245] ibid 6; Solon Barocas and Helen Nissenbaum, 'Big Data's End Run around Anonymity and Consent' in Julia Lane and others (eds), *Privacy, Big Data, and the Public Good: Frameworks for Engagement* (Cambridge University Press 2014) <http://ebooks.cambridge.org/ref/id/CBO9781107590205> accessed 6 March 2021.

[246] Giannopoulou (n 115) 9.

Amazon's Competition Investigation in India: A Case for Expansion of Investigation and Grant of Interim Relief

*Madhavi Singh**

Abstract *In the last few years, associations of domestic retailers have become vociferous opponents of Amazon's practices in India. In response to complaints of anti-competitive conduct, the Competition Commission of India has initiated an investigation into Amazon's anti-competitive vertical agreements in online smartphone retail. Against this backdrop, Reuters published a series of investigative reports which indicate that Amazon used internal data of third-party sellers and engaged in preferential treatment of private labels and preferred sellers. The Reuters reports join a series of other reports and studies which reveal that such conduct is pervasive across product categories. In light of this information, this paper makes two broad arguments. First, the paper argues that the scope of the competition investigation in India should be broadened beyond smartphones. The investigation should be reoriented to focus on the relationship between Amazon and its preferred sellers or retailers more broadly, rather than bifurcating the investigation along the lines of separate product categories. Second, the paper argues that the publicly-available information is sufficient to satisfy the legal test for passing an interim order. Such an interim order should prohibit Amazon from acting in the dual capacity of marketplace and seller. The necessity of the interim order has been highlighted through reference to the potentially irreparable and unquantifiable harm done to competition and consumers and the protracted nature of competition proceedings which might render the final order redundant.*

* *Felix Scholar, Bachelor of Civil Law (University of Oxford); BA LLB (National Law School of India University). The author is a Research Associate at the Centre for Asian Legal Studies at National University of Singapore and a Visiting Faculty at National Law School of India University. Views are personal. Email: madhavisingh@nls.ac.in.*

I. Introduction

Even as the world wraps its head around the Wall Street Journal exposé of Facebook[1] and attempts to understand the implications of the Facebook papers,[2] there have been yet other journalistic investigations of a Big Tech company's internal documents and practices which once again reveal legally and ethically dubious conduct. In 2021 Reuters published two special reports based on thousands of pages of Amazon's internal documents which show that, at least in India, Amazon has been copying retailers' products and favoring private labels on its e-commerce platform as part of its formal strategy and that even high-level executives of the company were aware of these actions.[3] Although this exposé of Amazon's practices has attracted only a fraction of the public attention in comparison to the Facebook Papers, the investigation and evidence unearthed against Amazon are legally significant in multiple ways, especially in India, as most of these documents apparently pertain to the company's practices in India.

---

1 'The Facebook Files: A Wall Street Journal Investigation' *The Wall Street Journal* <https://www.wsj.com/articles/the-facebook-files-11631713039> accessed 6 December 2021.

2 Andrew Marantz, 'The Meta Narrative: What we've Learned from the Facebook Papers' *the New Yorker* (5 November 2021) <https://www.newyorker.com/news/daily-comment/the-meta-narrative-what-weve-learned-from-the-facebook-papers> accessed 6 December 2021; Bill Chappell, 'The Facebook Papers: What you need to Know about the Trove of Insider Documents' *NPR* (25 October 2021) <https://www.npr.org/2021/10/25/1049015366/the-facebook-papers-what-you-need-to-know> accessed 6 December 2021.

3 Aditya Kalra, Test the Boundaries: Amazon Documents Reveal Company's Secret Strategy to Dodge Indian Regulators, *Reuters* (17 February 2021) <https://www.reuters.com/investigates/special-report/amazon-india-operation/> accessed 6 December 2021; Aditya Kalra & Steve Stecklow, 'The Imitation Game: Amazon Copied Products and Rigged Search Results to Promote its Own Brands, Documents Show' *Reuters* (13 October 2021) <https://www.reuters.com/investigates/special-report/amazon-india-rigging/> accessed 6 December 2021.

For a long time now, retailers in India have cried foul over Amazon's conduct claiming that it engages in several anti-competitive practices which disadvantage third-party sellers on its platform resulting in an uneven playing field and eventual elimination of retailers from the market. Associations of retailers and Small and Medium enterprises have raised these concerns before the Ministry of Commerce and Industry,[4] the Reserve Bank of India,[5] the Enforcement Directorate[6] and the Competition Commission of India.[7] Additionally, retailers have also resorted to other means of expressing their grievances including organizing a protest during Jeff Bezos' visit to India,[8] launching a call for a boycott of Amazon during the festival sale season,[9] requesting Indian tech moguls to discontinue their ties with Amazon and stop acting as a front for its private labels,[10] and attempting to characterize Amazon as the modern 'English East India Company.'[11] In the shape of the collective of Indian retailers, Amazon might have found its match, because even though these entities may not be comparable to the global tech behemoth in terms of size and access to funds, they certainly have the political clout and sway to influence the government and lobby regulators

---

4 'Complaints against E-commerce Players being Looked into: Govt' *Financial Express* (31 July 2021) <https://www.financialexpress.com/industry/complaints-against-e-commerce-players-being-looked-into-govt/2301262/> accessed 6 December 2021.

5 'Centre Directs ED, RBI to Act against Amazon, Flipkart for FDI, FEMA Violations' *The Times of India* (31 December 2020) <https://timesofindia.indiatimes.com/business/india-business/centre-directs-ed-rbi-to-act-against-amazon-flipkart-for-fdi-fema-violations/articleshow/80043646.cms> accessed 6 December 2021.

6 'ED Initiates Probe against Amazon Over 'Violation' of Foreign Exchange Law' *The Print* (28 January 2021) <https://theprint.in/india/ed-initiates-probe-against-amazon-over-violation-of-foreign-exchange-law/594109/> accessed 6 December 2021.

7 *Delhi Vyapar Mahasangh v Flipkart Internet (P) Ltd* 2020 SCC OnLine CCI 3 (India); *Lifestyle Equities CV v Amazon Seller Services (P) Ltd* 2020 SCC OnLine CCI 33 (India); 'Prepare, Present Complaints against Big Online Retailers before CCI: Goyal' *Business Standard* (9 August 2020) <https://www.business-standard.com/article/economy-policy/prepare-present-complaints-against-big-online-retailers-before-cci-goyal-121080901885_1.html> accessed 6 December 2021.

8 Soutik Biswas, 'Why India is Greeting Amazon's Jeff Bezos with Protests' *British Broadcasting Corporation* (15 January 2020) <https://www.bbc.com/news/world-asia-india-51117315> accessed 6 December 2021.

9 'Traders, Online Sellers Protest against E-commerce Brands' *The Economic Times* (2 November 2021) <https://retail.economictimes.indiatimes.com/news/industry/traders-online-sellers-protest-against-e-commerce-brands/87477436> accessed 6 December 2021.

10 'Indian Sellers Collective asks Narayana Murthy to end ties with Amazon' *Business Standard* (19 July 2021) <https://www.business-standard.com/article/companies/indian-sellers-collective-asks-narayana-murthy-to-end-ties-with-amazon-121071900531_1.html> accessed 6 December 2021.

11 PTI, 'RSS – Linked Weekly Terms Amazon as 'East India Company 2.0' *The Indian Express* (26 September 2021) <https://indianexpress.com/article/india/rss-linked-weekly-amazon-as-east-india-company-7536066/> accessed 6 December 2021.

into taking action and getting their voices heard.[12] Unsurprisingly, therefore Indian retailers have managed to convince several government agencies, including the Enforcement Directorate and the Competition Commission of India, to investigate Amazon's practices in India. Given the high stakes involved, namely, greater control of one of the biggest digital retail markets in the world,[13] the altercation between independent retailers and Amazon is expected to be intense and long-drawn.

In this backdrop this article looks at some of the journalistic reports and studies, especially the Reuters reports on Amazon's conduct in India, to argue that in light of all the information that is publicly available, the Competition Commission of India ("Commission" or "CCI") should: (i) expand and reorient the scope of its competition investigation into Amazon; and (ii) pass an interim order prohibiting Amazon from operating in the dual capacity of a marketplace and a seller.

II. Competition Cases Against Amazon in India

One of the primary regulators which is currently assessing the legality of Amazon's conduct is the CCI. The allegations against Amazon before the CCI have taken the form of two cases that have culminated in very different outcomes.

In *Delhi Vyapar Mahasangh v Flipkart Internet (P) Ltd & Amazon*[14] an association of Small and Medium Enterprises brought a complaint against the two biggest e-commerce platforms in India, Amazon and Flipkart, alleging that both platforms entered into several vertical agreements with their preferred sellers, that is, sellers who are directly or indirectly affiliated or controlled by these e-commerce platforms. It was alleged that both e-commerce platforms engaged in deep discounting, preferential listing and

---

[12] Anuj Srivas, 'Amazon's Jeff Bezos is in India, But he is not Exactly Getting a Welcome Wagon' *The Wire* (15 January 2020) <https://thewire.in/business/amazon-jeff-bezos-india-welcome-wagon> accessed 6 December 2021.

[13] 'Value e-commerce in India to grow to $40 Billion by 2030: Kearney' *Livemint* (17 August 2021) <https://www.livemint.com/economy/value-e-commerce-in-india-to-grow-to-40-billion-by-2030-kearney-11629176945549.html> accessed 6 December 2021; 'Indian E-retail Market Expected to Grow to $140 Bn by FY26: Bain & Company' *Business Standard* (17 August 2021) <https://www.business-standard.com/article/companies/indian-e-retail-market-expected-to-grow-to-140-bn-by-fy26-bain-company-121081700144_1.html> accessed 6 December 2021; 'India's Consumer Digital Economy to Grow 10X to $800 Bn by 2030: Redseer' *Business Standard* (1 July 2021) <https://www.business-standard.com/article/current-affairs/india-s-consumer-digital-economy-to-grow-10x-to-800-bn-by-2030-redseer-121063001783_1.html> accessed 6 December 2021.

[14] *Delhi Vyapar Mahasangh v Flipkart Internet (P) Ltd* 2020 SCC OnLine CCI 3 (India) ("*Delhi Vyapar Mahasangh*").

exclusive tie-ups for both preferred sellers as well as their own private labels which amounted to an abuse of dominance as well as an anti-competitive agreement under the Competition Act, 2002. Importantly, in *Delhi Vyapar Mahasangh* the allegations were limited only to the sale of smartphones on these platforms and did not cover other product categories. In this case, the CCI *prima facie* found merit in the allegations and initiated a detailed investigation. This investigation is still ongoing. It should be noted that Amazon is being investigated for entering into anti-competitive vertical agreements (with preferred sellers) in violation of section 3(4) of the Competition Act.[15] There is currently no investigation against Amazon for abuse of dominance under section 4 of the Competition Act.[16][17]

In contrast to *Delhi Vyapar Mahasangh*, the CCI in *Lifestyle Equities v Amazon* refused to initiate an investigation when similar allegations were levelled against Amazon in the category of online fashion retail.[18] The different outcomes were sought to be justified on the basis of the different market

---

[15] The Competition Act 2002, s 3(4):

> Any agreement amongst enterprises or persons at different stages or levels of the production chain in different markets, in respect of production, supply, distribution, storage, sale or price of, or trade in goods or provision of services, including-
>
> (a) tie-in arrangement;
> (b) exclusive supply agreement;
> (c) exclusive distribution agreement;
> (d) refusal to deal;
> (e) resale price maintenance,
> (f) shall be an agreement in contravention of sub-section (1) if such agreement causes or is likely to cause an appreciable adverse effect on competition in India.

[16] The Competition Act 2002, s 4(2):

> There shall be an abuse of dominant position [under sub-section (1), if an enterprise or a group]-
>
> (a) directly or indirectly, imposes unfair or discriminatory-
> (i) condition in purchase or sale of goods or service; or
> (ii) price in purchase or sale (including predatory price) of goods or service.
> (b) limits or restricts—
> (i) production of goods or provision of services or market therefor; or
> (ii) technical or scientific development relating to goods or services to the prejudice of consumers; or
> (c) indulges in practice or practices resulting in denial of market access in any manner; or
> (d) makes conclusion of contracts subject to acceptance by other parties of supplementary obligations which, by their nature or according to commercial usage, have no connection with the subject of such contracts; or
> (e) uses its dominant position in one relevant market to enter into, or protect, other relevant market.

[17] *Delhi Vyapar Mahasangh* (n 14) [15] (the Commission noted that the Informant had levelled allegations of joint or collective abuse of dominance which is not envisaged under the Competition Act).

[18] *Lifestyle Equities CV v Amazon Seller Services (P) Ltd* 2020 SCC OnLine CCI 33 ("Lifestyle Equities"); The order has been appealed before the National Company Law Appellate Tribunal - Competition Appeal (AT)-20/2020.

structures and competitive dynamics in the two markets. Online fashion retail was considered much more competitive than online smartphone sales and additionally, there was no evidence of exclusive tie-ups in the former.[19] Further, the primary allegation in *Lifestyle Equities* pertained to counterfeiting and unauthorized selling of products – wrongs which were considered to be outside the scope of competition law.[20] The decision of the CCI to close the case in *Lifestyle Equities* has been appealed before the National Company Law Appellate Tribunal, whose decision is awaited.[21]

With these cases, India joins a slew of jurisdictions including the USA,[22] European Union,[23] Germany,[24] France,[25] and Australia,[26] which are attempting to use the antitrust framework to regulate Amazon's practices. However, the investigation against Amazon in India unlike most other jurisdictions is not based on abuse of dominance.[27] The fact that Amazon's conduct is being investigated using the framework of vertical agreements and not abuse

---

[19] ibid [30].

[20] ibid [28].

[21] National Company Law Appellate Tribunal, Competition Appeal (AT)-20/2020.

[22] Laurine Feiner & Annie Palmer, 'DC Attorney General Sues Amazon on Antitrust Grounds, Alleges it Illegally Raises Prices' *CNBC* (25 May 2021) <https://www.cnbc.com/2021/05/25/dc-attorney-general-sues-amazon-on-antitrust-grounds-alleges-it-illegally-raises-prices.html> accessed 6 December 2022; Annie Palmer & Laurine Feiner, 'DC Attorney General goes After Amazon's First-party Business in Amended Antitrust Complaint' *CNBC* (13 September 2021) <https://www.cnbc.com/2021/09/13/dc-attorney-general-targets-amazons-first-party-business-in-amended-antitrust-complaint.html> accessed 6 December 2021.

[23] 'Antitrust: Commission Opens Investigation into Possible Anti-competitive Conduct of Amazon' (*European Commission,* 17 July 2019) <https://ec.europa.eu/commission/presscorner/detail/en/ip_19_4291> accessed 6 December 2021; 'Antitrust: Commission sends Statement of Objections to Amazon for the use of non-public Independent Seller Data and Opens Second Investigation into its E-commerce Business Practices' (*European Commission,* 10 November 2020) <https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2077> accessed 6 December 2021.

[24] Siladitya Ray, 'Amazon is being Investigated by Germany's Antitrust Watchdog for Allegedly Influencing Third-party Seller Prices During Pandemic' *Forbes* (17 August 2020) <https://www.forbes.com/sites/siladityaray/2020/08/17/amazon-is-being-investigated-by-germanys-antitrust-watchdog-for-allegedly-influencing-third-party-seller-prices-during-pandemic/?sh=7104930a4ad6> accessed 6 December 2021; 'German Watchdog Launches New Investigation into Amazon' *Reuters* (28 October 2020) <https://www.reuters.com/article/amazon-com-germany-competition-idUSKBN27D2OQ> accessed 6 December 2021; 'German Antitrust Watchdog Launches New Proceedings against Amazon' *Reuters* (18 May 2021) <https://www.reuters.com/business/retail-consumer/german-antitrust-watchdog-launches-new-proceedings-against-amazon-2021-05-18/> accessed 6 December 2021.

[25] 'France Files Complaint against Amazon for Abuse of Dominant Position' *Reuters* (18 December 2017) <https://www.reuters.com/article/us-amazon-com-france-idUKKBN1EC0QN> accessed 6 December 2021.

[26] 'Australian Regulator to Probe Amazon, eBay and Other Online Markets' *CNBC* (21 July 2021) <https://www.cnbc.com/2021/07/22/australian-regulator-to-probe-amazon-ebay-and-other-online-markets.html> accessed 6 December 2021.

[27] *See* (n 23-26).

of dominance is noteworthy since it changes the elements of the violation which have to be proved and has other potential implications. For instance, it means that the relevant market for Amazon need not be delineated and therefore, the competition assessment need not be narrowly focused on certain product categories which form the relevant market. Instead examining potential violation of 'vertical agreement' allows the investigation to be focused broadly on the nature of the relationship between Amazon and its sellers, not constrained by product categories. This and other peculiarities of using vertical agreements instead of abuse of dominance framework have been discussed in greater detail later in this paper.

III. New Information and Evidence About Amazon's Practices

Amazon has consistently denied many of the allegations levelled against it as being factually incorrect. Before regulators in India as well as those in other jurisdictions, Amazon insists that it has access to the same data as all other sellers on its platform and it does not use internal non-public data of third-party sellers.[28] Similarly, Amazon claims that its search results are based on relevance, reviews and other objective metrics and it does not unfairly favour private labels or preferred sellers in the search ranking.[29] In the backdrop of these ongoing competition cases and Amazon's outright denial of the allegations as being factually incorrect, the Reuters' investigative reports come at a crucial time. According to Reuters, the internal documents in its possession reveal, amongst other things, that Amazon, at least in India:

(i) Gave preferential treatment to a few Special Merchants[30] or selected sellers by giving them discounted fees, access to Amazon's global retail tools and helping them cut exclusive deals with other big tech manufacturers.

(ii) Secretly exploited non-public internal seller data (including proprietary data, data relating to business strategies and transactions

[28] Lauren Feiner, 'Amazon Exec Tells Lawmakers the Company doesn't Favor Own Brands Over Products Sold by Third-party Merchants' *CNBC* (16 July 2019) <https://www.cnbc.com/2019/07/16/amazon-tells-house-it-doesnt-favor-own-brands-in-antitrust-hearing.html> accessed 6 December 2021.

[29] ibid.

[30] Kalra, 'Test the Boundaries' (n 3). (Cloudtail and Appario were two of Amazon's special merchants).

– number of units purchased, returned, etc.) to copy successful products,[31] sell them at steep discounts and boost the sales of its private labels.

(iii) Manipulated search results on the platform to favour the company's own products.[32]

Apart from calling into question the credibility of Amazon's representations, the reports also indicate how extensive these practices are. Such conduct was observed across several product categories including textile/fashion retail, smartphones, home furnishings, health and household products. The Reuters reports come alongside other recent reports and studies in the Wall Street Journal,[33] the New York Times,[34] the Markup,[35] and the Capitol Forum,[36] which make similar claims that Amazon uses internal data of sell-

---

[31] Whether unauthorized copying and counterfeiting falls within the subject matter domain of competition law is not a question that this paper seeks to answer. In order to avoid this question, the competition law concerns against Amazon which this paper seeks to address are not those of counterfeiting or copying but of use of internal seller data and preferential treatment.

[32] Kalra, 'Test the Boundaries' (n 3); Kalra & Stecklow, 'The Imitation Game' (n 3).

[33] Dana Mattioli, 'Amazon Scooped up Data from its Own Sellers to Launch Competing Products' *The Wall Street Journal* (23 April 2020) <https://www.wsj.com/articles/amazon-scooped-up-data-from-its-own-sellers-to-launch-competing-products-11587650015> accessed 6 December 2021; Shane Shifflett and others, 'Amazon's Choice isn't the Endorsement it Appears' *The Wall Street Journal* (22 December 2019) <https://www.wsj.com/articles/amazons-choice-isnt-the-endorsement-it-appears-11577035151#refreshed?-mod=article_inline> accessed 6 December 2021; Dana Mattioli, 'Amazon Changed Search Algorithm in ways that Boost its Own Products' *The Wall Street Journal* (16 September 2019) <https://www.wsj.com/articles/amazon-changed-search-algorithm-in-ways-that-boost-its-own-products-11568645345> accessed 6 December 2021; cf Dana Mattioli, 'How Amazon Wins: By Steamrolling Rivals and Partners' *The Wall Street Journal* (22 December 2020) <https://www.wsj.com/articles/amazon-competition-shopify-wayfair-allbirds-antitrust-11608235127> accessed 6 December 2021.

[34] Julie Creswell, 'How Amazon Steers Shoppers to its Own Products' *The New York Times* (23 June 2018) <https://www.nytimes.com/2018/06/23/business/amazon-the-brand-buster.html> accessed 6 December 2021

[35] Adrianne Jeffries & Leon Yin, 'Amazon Puts its Own "Brands" First Above Better-rated Products' (*The Markup*, 14 October 2021) <https://themarkup.org/amazons-advantage/2021/10/14/amazon-puts-its-own-brands-first-above-better-rated-products> accessed 6 December 2021; Leon Yin & Adrianne Jeffries, 'How we Analysed Amazon's Treatment of its "Brands" in Search Results' (*The Markup*, 14 October 2021) <https://themarkup.org/amazons-advantage/2021/10/14/how-we-analyzed-amazons-treatment-of-its-brands-in-search-results> accessed 6 December 2021.

[36] 'Amazon: EC Investigation to Focus on whether Amazon uses Data to Develop and Favor Private Label Products; Former Employees Say Data key to Private Label Strategy' (*The Capitol Forum*, 5 November 2018) <https://thecapitolforum.com/wp-content/uploads/2018/11/Amazon-2018.11.05.pdf> accessed 6 December 2021; 'Amazon: By Prioritising its Own Fashion Label Brands in Product Placement on its Increasingly Dominant Platform, Amazon Risks Antitrust Enforcement by a Trump Administration' (*The Capitol Forum,* 13 December 2016) <https://thecapitolforum.com/wp-content/uploads/2016/07/Amazon-2016.12.13.pdf> accessed 6 December 2021.

ers and prioritizes its own private labels. These claims are based on numerous employee testimonials, detailed experiments, studies and extensive internal documents. For its part, Amazon has simply responded that these reports are inaccurate and unsubstantiated.[37] Further, Amazon has stated that it has a company policy which prohibits the use of internal seller data to develop private labels and investigates any allegations of violation of this policy.[38]

The Reuters reports have already caught the eye of relevant authorities both in India and abroad. The reports had a series of consequences. The Enforcement Directorate in India initiated an investigation into Amazon for potential violations of the foreign direct investment rules.[39] The High Court of Karnataka[40] and the Supreme Court of India dismissed Amazon's writ petition to halt the competition regulator's investigation.[41] US lawmakers called for the breaking up of Amazon.[42] Five members of the US House Judiciary Committee wrote to Amazon accusing the company's top executives of lying or misleading the Congress and threatening criminal action.[43] A global trade union urged the European Commission to widen its antitrust investigation of Amazon,[44] and the association of Indian digital companies

[37] 'Amazon India Boss Claims Report on Malpractices is Factually Incorrect' *The Economic Times* (18 February 2021) <https://economictimes.indiatimes.com/tech/tech-bytes/amazon-india-boss-claims-reuters-report-is-factually-incorrect/articleshow/81094015.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst> accessed 6 December 2021.

[38] Steve Stecklow and others, 'Five U.S. Lawmakers Accuse Amazon of Possibly Lying to Congress Following Reuters Report' *Reuters* (19 October 2021) <https://www.reuters.com/technology/five-us-lawmakers-accuse-amazon-possibly-lying-congress-following-reuters-report-2021-10-18/> accessed 6 December 2021

[39] Aditya Kalra, 'India's Enforcement Directorate to Examine Findings in Reuters Report on Amazon: Agency Source' *Reuters* (18 February 2021) <https://www.reuters.com/article/us-amazon-india-operations-enforcement-idUSKBN2AI1TC> accessed 6 December 2021.

[40] Aditya Kalra, 'India Antitrust Body says Reuters Story Corroborates Evidence in Probe of Amazon' *Reuters* (19 March 2021) <https://www.reuters.com/article/us-amazon-com-india-idUSKBN2BB1UF> accessed 6 December 2021; Tarush Bhalla, 'HC Refuses to Halt CCI Probe against Amazon, Flipkart' *Livemint* (23 July 2021) <https://www.livemint.com/companies/news/karnataka-hc-quashes-amazon-flipkart-s-plea-against-cci-investigation-11627049204076.html> accessed 6 December 2021.

[41] 'Supreme Court Refuses to Halt CCI Probe against Flipkart and Amazon' *The Indian Express* (10 August 2021) <https://indianexpress.com/article/business/companies/supreme-court-refuses-halt-antitrust-probe-flipkart-amazon-cci-7445413/#:~:text=The%20probe%20ordered%20by%20the,refused%20to%20stay%20the%20investigation> accessed 6 December 2021.

[42] Aditya Kalra & Steve Stecklow, 'Indian Retailers Want Probe After Report Accuses Amazon of Rigging' *The Wire* (15 October 2021) <https://thewire.in/business/indian-retailers-want-probe-after-report-accuses-amazon-of-rigging> accessed 6 December 2021.

[43] Steve Stecklow and others (n 38).

[44] Aditya Kalra, 'Labour Union Urges European Authorities to Widen Amazon Antitrust Probe After Reuters Story' *Reuters* (22 October 2021) <https://www.reuters.com/technology/labour-union-urges-european-authorities-widen-amazon-antitrust-probe-after-2021-10-22/> accessed 6 December 2021.

demanded that the government initiate a probe into the company.[45] Quite apart from these developments, this paper argues that the Reuters and other recent reports on Amazon's conduct have important implications for the ongoing competition investigation and cases against Amazon in India.

IV. Need to Broaden the Scope of Competition Investigation

As outlined earlier the scope of the competition investigation against Amazon in India is rather narrow. At present, the investigation is limited only to the product category of smartphones as directed in *Delhi Vyapar Mahasangh*. Even after accounting for *Lifestyle Equities* in which investigation has not been directed but which is currently under appeal, only two product categories, namely, smartphone and fashion retail, are covered by the present cases. The remaining product categories currently do not seem to be on the radar of the Indian competition regulator. However, as the Reuters' and other reports reveal the alleged anti-competitive conduct is observed across multiple product categories (including textile/fashion retail, smartphones, home furnishings, health and household products) and this list seems to be ever-increasing as Amazon keeps expanding its private labels in new categories.[46] Given the ubiquity of the conduct, it is far from adequate that the competition investigation remains limited to only a few product categories.

Perhaps, one reason why the competition regulator might want to look at online retail in each product category separately is that the competitive dynamics and market structure of each category could be distinct. This was also one of the grounds adopted by the CCI while distinguishing *Delhi Vyapar Mahasangh* from *Lifestyle Equities* and refusing to direct investigation in the latter even though it had been directed in the former. For instance, in the online retail of smartphones or electronics, Amazon might be one of

---

[45] 'Statement: ADIF Condemns Amazon's Predatory Playbook of Copying, Rigging and Killing Indian Brands, Urges Government for Timely Intervention' (Alliance of Digital India Foundation, 14 October 2021) <https://blog.adif.in/p/adif-amazon-reuters-ecommerce-fair-markets> accessed 6 December 2021.

[46] Anirban Sen, 'Amazon Trebles Choice of Offerings under Private Labels' *Livemint* (10 October 2018) <https://www.livemint.com/Companies/O8Wc537U13T2iREYW1jYfM/Amazon-trebles-choice-of-offerings-under-private-labels.html> accessed 6 December 2021; Digbijay Mishra, 'Amazon Scales up Accelerator for Private Labels' *The Economic Times* (13 November 2019) <https://economictimes.indiatimes.com/tech/internet/amazon-scales-up-accelerator-for-pvt-labels/articleshow/72031746.cms> accessed 6 December 2021; Alnoor Peermohamed, 'Only Private Labels Listings Back to Pre-Covid Days on Amazon' *The Economic Times* (28 May 2020) <https://economictimes.indiatimes.com/small-biz/startups/newsbuzz/only-private-labels-listings-back-to-pre-covid-days-on-amazon/articleshow/76055431.cms?from=mdr> accessed 6 December 2021

the biggest players as opposed to online fashion retail[47] or grocery shopping[48] where it might face fierce competition from other market players. However, the crucial question is whether this difference in competitive dynamics of the various product categories in which Amazon operates is 'legally relevant.'

As noted earlier, Amazon is being investigated for entering into an anti-competitive vertical agreement in violation of section 3(4) and is not being investigated for abuse of dominance under section 4 of the Competition Act. Establishing a vertical agreement does not require delineation of the relevant market or proving dominance unlike abuse of dominant position under section 4. The Supreme Court's decision in the *Coordination Committee* case created some confusion about whether relevant market delineation was a necessary step in a Section 3 analysis.[49] This confusion however has now been put to rest by the Supreme Court through an order pronounced in a Miscellaneous Application referred by the CCI requesting clarification of the ambiguous *Coordination Committee* holding. The Supreme Court has now clarified that "*the determination of 'relevant market' is not a mandatory pre-condition for making assessment of the alleged violation under Section 3 of the Act.*"[50]

It is now clear that section 3(4) does not require delineation of relevant market and the constituent elements of a vertical agreement under section 3(4) are limited to the following:

(i) the existence of an agreement;

(ii) amongst enterprises at different levels or stages of the production chain;

(iii) which causes or is likely to cause an appreciable adverse effect on competition in India.

Thus, for the assessment of vertical agreement the focal point or at least the starting point is the nature of the agreement between enterprises and

---

[47] *Lifestyle Equities* (n 19) [30].

[48] Debojyoti Ghosh & Prerna Lidhoo, 'What's Cooking in India's E-grocery Market?' (*Fortune India,* 15 July 2021) <https://www.fortuneindia.com/enterprise/whats-cooking-in-indias-e-grocery-market/105623> accessed 6 December 2021; 'Amazon, Flipkart, Others May have More Fierce Competitors Ahead After Reliance in E-commerce, Grocery' *Financial Express* (23 August 2020) <https://www.financialexpress.com/industry/amazon-flipkart-walmart-and-ril-market-wars-indian-e-commerce-pond-big-enough-for-plenty-of-fish/2062742/> accessed 6 December 2021.

[49] *CCI v Coordination Committee of Artists and Technicians of W.B. Film and Television* (2017) 5 SCC 17 (India).

[50] *CCI v Coordination Committee of Artists and Technicians of W.B. Film and Television* (2017) 5 SCC 17 (India).

not the relevant market (if at all the relevant market were to form part of the assessment). Had the competition investigation against Amazon been for abuse of dominance under section 4, then the starting point for analysis would necessarily have to look at the market structure and competitive dynamics as part of the relevant market delineation exercise. By choosing to investigate Amazon for vertical agreement under section 3(4) rather than for abuse of dominance under section 4, the CCI has successfully averted the compulsion to look at competitive dynamics or market structure as the first step of its analysis. Instead, the first step in the competition analysis of Amazon's conduct would look at the vertical relationship or agreement between Amazon and preferred sellers or retailers through which Amazon sells its private labels. More specifically, the first two elements of section 3(4) would look at the terms of Amazon's agreements with its preferred sellers (for instance, exclusivity, special benefits etc.) and the stages of the production chain at which they operate (role of Amazon as producer, distributor, inventory-manager etc.) Hence, any variance in competition dynamics or market structure of different product categories is irrelevant for the assessment of the first two elements of section 3(4) and does not justify limiting or defining the scope of the competition investigation along the lines of product categories.

The variance in competitive dynamics and market structures of different product categories on Amazon could be relevant for the assessment of the third element of section 3(4), that is, for ascertaining whether the vertical agreement(s) caused 'appreciable adverse effect on competition'. For instance, if Amazon's market share in the product category of smartphones is high then a vertical agreement in that category could have an 'appreciable adverse effect on competition'. Whereas in product categories such as fashion retail or grocery where Amazon's market share might be comparatively lesser and competition might be fierce, the effect of Amazon's vertical agreement on competition might not be appreciable. Although Amazon's market share in each product category might admittedly be different, an assessment of the third element of 'appreciable adverse effect on competition' examines not just the market share but several other factors including entry barriers, foreclosure effects etc.[51] Hence, merely because Amazon's market share in a

[51] The Competition Act 2002, s 19(3):

The Commission shall, while determining whether an agreement has an appreciable adverse effect on competition under section 3, have due regard to all or any of the following factors, namely:

a. creation of barriers to new entrants in the market;
b. driving existing competitors out of the market;
c. foreclosure of competition by hindering entry into the market;
d. accrual of benefits to consumers;

particular product category is low does not necessarily mean that its vertical agreement in that category is incapable of causing an 'appreciable adverse effect on competition'. For instance, even if Amazon's market share in online grocery retail is low, an 'appreciable adverse effect on competition' assessment should holistically look at other factors such as the company's potential to leverage its market power in other product categories and adjacent markets or its established distribution channels etc. The variance in competitive dynamics across different product categories of Amazon only becomes relevant (if at all)[52] while assessing the final element of section 3(4), namely, 'appreciable adverse effect on competition'. If such differentiated analysis of 'appreciable adverse effect on competition' for each product category is needed, then the same can be carried out during the detailed competition investigation undertaken by the Director General. It does not explain why the investigation overall needs to be limited to or defined along the lines of one or two product categories.

Another potential reason why the Indian competition regulator might be comfortable with limiting the competition investigation to one or two product categories could be because they expect that any directions given by them regarding one product category would have a domino effect[53] and would result in Amazon changing its practices across the board. Even legally it could be used as a precedent to initiate cases against Amazon in other product categories and demand it to change its behaviour. However, such a process would not only be time-consuming but also uncertain and potentially ineffectual. Without a doubt, Amazon would argue (as it did in *Lifestyle Equities*) that the precedent would not directly and squarely apply across all product categories due to differences in competitive dynamics and market structure of each category. Therefore, it is unlikely that a direction given in one product category would have a domino effect and influence Amazon to change its behaviour voluntarily across all categories. As evidence, the CCI's

e. improvements in production or distribution of goods or provision of services; or
f. promotion of technical, scientific and economic development by means of production or distribution of goods or provision of services.

[52] It might not be relevant if for instance, the CCI decides to look at 'appreciable adverse effect on competition' at the aggregate level, that is, aggregated across all product categories.

[53] For instance, the European Commission's decision in the Google comparison shopping case was considered to form a precedent which would provide the framework to consider the legality of Google's conduct vis-à-vis its other verticals. cf 'Antitrust: Commission Fines Google €2.42 Billion for Abusing Dominance as Search Engine by Giving Illegal Advantage to Own Comparison Shopping Service' (*European Commission*, 27 June 2017) <https://ec.europa.eu/commission/presscorner/detail/en/IP_17_1784> accessed 6 December 2021; Natasha Lomas, 'Google Fined $2.7bn for EU Antitrust Violations over Shopping Searches' (*TechCrunch*, 27 June 2017) <https://techcrunch.com/2017/06/27/google-fined-e2-42bn-for-eu-antitrust-violations-over-shopping-searches/> accessed 6 December 2021.

Market Study on E-Commerce already prescribes that e-commerce platforms observe platform neutrality,[54] but as revealed by subsequent reports and studies (discussed above) this prescription might not have had the desired prohibitory and self-regulatory effect. It is unclear why an order of the CCI pertaining to one specific product category would have the desired domino effect when the CCI's Market Study could not achieve the same especially if Amazon feels that it has a chance to be able to distinguish the cases on the basis of different market structures and competitive dynamics.

In line with the spirit of section 3(4), the competition investigation against Amazon should focus on the vertical agreement or relationship between Amazon and its preferred sellers or sellers through which it sells private labels more generally rather than being limited by narrow product categories. Further, the boundaries of these product categories are hardly clear or fixed. Each category could arguably be broken down into further sub-categories and the competitive dynamics in each of them might be different. For instance, household appliances could be broken down into sub-groups of electrical appliances, kitchen appliances, bathroom supplies etc.[55] and conceivably, the competitive dynamics in each of these sub-groups might be different. Thus, by attempting to look at the competition in each product category separately the competition regulator might be setting themselves up for not just an arduous but maybe even an impossible task. In any event, since section 3(4) is based on the agreement between enterprises rather than the products in question, basing the competition investigation on product categories seems redundant and inessential as per statutory requirements. Thus, the scope of the competition investigation against Amazon should be broadened.

This would also be in consonance with the investigations being carried out in other jurisdictions such as the European Union and the USA, which are looking at Amazon's practices on its e-commerce platform more broadly, not constrained by specific product categories. The European Commission has opened two antitrust investigations against Amazon. The first looks specifically at Amazon's use of non-public data from independent retailers who sell on its marketplace and whether such data is being used to favour Amazon's private labels.[56] The second investigation looks into the possible

---

[54] Market Study on E-Commerce in India (*Competition Commission of India*, 8 January 2020) <https://www.cci.gov.in/sites/default/files/whats_newdocument/Market-study-on-e-Commerce-in-India.pdf> accessed 6 December 2021.

[55] Based on Amazon's own categories and sub-categories of products at amazon.in.

[56] 'Antitrust: Commission Opens Investigation into Possible Anti-competitive Conduct of Amazon' (*European Commission*, 17 July 2019) <https://ec.europa.eu/commission/presscorner/detail/pl/ip_19_4291> accessed 6 December 2021.

preferential treatment of Amazon's private labels and those of marketplace sellers that use Amazon's logistics and delivery services.[57] The two European Commission investigations broadly pertain to Amazon's dual role as a marketplace and a retailer on its own marketplace and any potential unfairness which could arise as a consequence of this dual role. Similarly, in the USA, the first antitrust suit brought against Amazon by the D.C. Attorney General is not constrained by any specific product category.[58] Hence, leading antitrust investigations into Amazon around the world have dealt with the practices of the platform more broadly rather than restricting it to or bifurcating it along narrow product categories.

Based on the Reuters' reports which reveal the prevalence of the allegedly anti-competitive conduct across numerous product categories and in light of the spirit and elements of section 3(4) as discussed above, the scope of the competition investigation against Amazon should be expanded. It should be based on the interactions and agreements between Amazon and preferred sellers/ third-party sellers more broadly and should not be limited in scope to only certain product categories. The variance in competitive dynamics and market structures across product categories could be dealt with during the detailed competition investigation. Procedurally too, the Director General has the power to expand the scope of the investigation beyond what has been raised in the information or the reference.[59] Even if the DG is unable to exercise her discretion liberally to expand the scope of the existing investigations, the CCI could anyway initiate a broader inquiry into Amazon on its own motion – a power which has been expressly conferred on it by the Competition Act,[60] and which has been exercised by the Commission on numerous occasions in the past.[61] Any subsequent broader inquiry initiated by the CCI could also be joined with all other similar matters.[62] Thus, there

---

[57] 'Antitrust: Commission Sends Statement of Objections to Amazon for the use of Non-public Independent Seller Data and Opens Second Investigation into its E-commerce Business Practices' (*European Commission*, 10 November 2020) <https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2077> accessed 6 December 2021.

[58] Laurine Feiner & Annie Palmer (n 23).

[59] The Director General got this power pursuant to an amendment to the Competition Commission of India (General) Regulations 2019; *See* Competition Commission of India, The Competition Commission of India (General) Amendment Regulations 2020, S. No. 49 (Notified on February 6, 2020) <https://www.cci.gov.in/sites/default/files/regulation_pdf/216024.pdf>; See also *Excel Crop Care Ltd v CCI* (2017) 8 SCC 47 (India), [44]-[45].

[60] The Competition Act 2002, s 19(1) (Gives the Commission the power to inquire into any alleged contravention on its own motion).

[61] Most recently the CCI used this power to *suo moto* begin an inquiry against Facebook and WhatsApp (*In re: Updated Terms of Service and Privacy Policy for WhatsApp Users,* 2021 SCC OnLine CCI 19).

[62] The Competition Commission of India (General) Regulations 2009, Regulation 27 (Power of Commission to join multiple information).

exist neither substantive legal nor procedural hurdles to expanding and reorienting the scope of the competition investigation and such expansion of scope has been made necessary by the emergence of new information and evidence.

V. Satisfaction of the Legal Test to Grant Interim Relief

In addition to expanding and reorienting the scope of the competition investigation, the information and evidence made available by journalistic reports and studies conducted create a convincing case for the grant of interim relief against Amazon. The CCI has the power to issue interim orders even without giving notice to the parties under section 33 of the Competition Act. However, the Supreme Court has cautioned that interim orders should be issued only sparingly and under compelling and exceptional circumstances.[63] In accord with this direction, the CCI has rarely granted interim relief.[64] The Supreme Court in *CCI v SAIL* has held that in order to pass an interim order under section 33, the CCI should record its satisfaction that:

(i) A contravention has been committed and continues to be committed or is about to be committed. Such satisfaction should be of a higher degree than the formation of a *prima facie* view under section 26(1) of the Competition Act.

(ii) It is necessary to issue an order of restraint.

(iii) There is every likelihood of irreparable and irretrievable damage or there is definite apprehension that it would have an adverse effect on competition in the market.[65]

In the light of employee testimonials and the unearthing of internal documents through journalistic reports,[66] this paper attempts to show that the *Steel Authority of India Ltd.* test for granting interim relief stands satisfied. Reuters claims that it has thousands of internal documents in its possession which include drafts of meeting notes, PowerPoint slides, business reports

---

[63] *CCI v SAIL* (2010) 10 SCC 744, [119] ("*Steel Authority of India*").

[64] *Nuziveedu Seeds Ltd v Mahyco Monsanto Biotech (India) Ltd* 2016 SCC OnLine CCI 48 (India)*; Indian National Shipowners' Assn v ONGC Ltd* 2018 SCC OnLine CCI 48 (India); *Confederation of Real Estate Developers Assn of India v Department of Town and Country Planning, Government of Haryana*, 2018 SCC OnLine CCI 6 (India); *Federation of Hotel & Restaurant Associations of India v MakeMyTrip India (P) Ltd* 2021 SCC OnLine CCI 12 (India).

[65] *Steel Authority of India Ltd* (n 63) [31], [119].

[66] See (n 32- 36).

and emails. The contents of these as extracted in the Reuters reports seem to pertain directly to Amazon's alleged anti-competitive conduct in India. The Commission has the same powers as are vested in a civil court under the Code of Civil Procedure, 1908 including summoning and examining any person, requiring the discovery and production of documents, receiving evidence on affidavit etc.[67] Thus, the Commission should utilize these powers to inspect these documents and examine the reports and studies which are already publicly available to ascertain whether interim relief needs to be granted.

Proposed Interim Relief

At the outset, it is crucial to understand the kind of interim restraint being proposed to curb Amazon's anti-competitive conduct before delving into its necessity and satisfaction of the legal test under section 33 of the Competition Act. The simplest and most straightforward relief which might come to mind is that Amazon provides an undertaking that it would not engage in preferential treatment of its private labels or preferred sellers, nor use internal seller data. However, such a simple prohibitory dictum to not engage in anti-competitive conduct would be redundant. This is because Amazon already claims that it does not preferentially treat certain products nor use internal seller data.[68] Hence, such an interim order would simply prohibit Amazon from doing something which according to its own representations it already doesn't do. Further, such a simple prohibition in fact already exists. The CCI's Market Study on E-Commerce already recognizes 'Platform Neutrality' as an area requiring self-regulation from e-commerce platforms. The CCI Market Study report advices e-commerce platforms to maintain platform neutrality and not engage in preferential treatment of either private labels or preferred sellers.[69] Yet neither the CCI's directions in the Market Study report nor Amazon's own representations to this effect seem to have prevented the company from engaging in such conduct as revealed through several journalistic reports.

Additionally, at the interim stage, it is very difficult for the regulator to monitor and ensure that Amazon does not mete out preferential treatment nor use internal seller data especially since the internal workings of Amazon and its search and ranking algorithms are closely guarded secrets. Moreover, the meaning of 'preferential treatment' and which practices might fall within

[67] The Competition Act 2002, s 36(2); The Competition Commission of India (General) Regulations, regs 44-45.
[68] Lauren Feiner (n 28).
[69] Market Study on E-Commerce in India (n 52) [86]-[89].

its ambit continues to be disputed. For instance, Amazon claims that several of its practices such as 'search seeding' and 'search sparkles' are legitimate practices to promote new products which do not yet have enough sales or reviews to be effectively ranked by the search algorithm.[70] A simple prohibitory interim relief of not engaging in 'preferential treatment' would give rise to interpretative uncertainty, and potential redundancy and would also be equivalent to treating the symptoms of the problem without targeting the incentives which influence the company's conduct.

Amazon's dual role as the marketplace as well as the seller on the same marketplace is the root cause of the conflict of interest which manifests itself in the form of these anti-competitive practices. Amazon's stake in the products sold on its e-commerce platform either through special merchants/preferred sellers or in the form of its private labels incentivizes the company to engage in preferential treatment. The sale of private labels and products of preferred sellers usually come with higher profit margins. The company's push for greater penetration of private labels in all categories encourages a company-wide culture of pervasive use of internal seller data and preferential treatment,[71] which will be impossible to deter unless this incentive is removed. Most of the alleged anti-competitive practices including use of non-public seller data, unfairly favouring its own products, brokering exclusive deals between preferred sellers and manufacturers etc. are traceable to the conflict of interest which arises when Amazon plays the dual role of marketplace and seller. Thus, the solution to the continuing anti-competitive conduct should target this root cause of the problem by prohibiting Amazon from operating as both the marketplace and the seller. This would entail that neither Amazon nor its associate companies[72] nor its subsidiary companies[73] directly or indirectly operate as manufacturers or sellers on its platform.

---

[70] Kalra & Stecklow, 'The Imitation Game' (n 3).

[71] See (n 94)

[72] The Companies Act 2013, s 2(6):

"associate company", in relation to another company, means a company in which that other company has a significant influence, but which is not a subsidiary company of the company having such influence and includes a joint venture company.

Explanation - For the purposes of this clause, "significant influence" means control of at least twenty per cent. of total share capital, or of business decisions under an agreement.

[73] The Companies Act 2013, s 2(87):

"subsidiary company" or "subsidiary", in relation to any other company (that is to say the holding company), means a company in which the holding company –

(i) controls the composition of the Board of Directors; or

(ii) exercises or controls more than one-half of the total share capital either at its own or together with one or more of its subsidiary companies:

Provided that such class or classes of holding companies as may be prescribed shall not have layers of subsidiaries beyond such numbers as may be prescribed.

This absolute restriction prohibiting Amazon from operating in the dual capacity of both seller and marketplace might appear harsh at first sight especially since it seems that traditional brick-and-mortar stores,[74] as well as other e-commerce platforms[75] in India, also operate their own private labels. However, traditional business models cannot be accurately compared to an e-commerce platform since the latter has characteristics (such as network effects and data-driven precision targeting) which are unique to or at least exaggerated in comparison to the former.[76] Network effects, use of big data, collection of vast troves of granular data facilitating precise behavioural discrimination and targeting, ability to engage in targeted advertising and pop-up notifications (even outside Amazon's platform) and search bias are features which are unique to or are much more exaggerated in the e-commerce model than in traditional retail stores selling private brands. For instance, Amazon has unprecedented amounts of data to know rather accurately consumers' preferences, price sensitivity points etc. Such data is used by Amazon to design its private labels, unfairly advantage them in search ranking and follow the customer incessantly with advertisements and pop-up notifications not just on Amazon's own platform but perhaps even on other websites. These characteristics are either unique to or at the very least much more exaggerated in the e-commerce model than in traditional brick-and-mortar stores. Additionally, the proposed interim relief doesn't seek to single out or disadvantage Amazon in comparison to other e-commerce platforms

---

74 Abhirup Roy & Aditya Kalra, 'In India, Reliance Retail's Private Labels Revolution Spooks Global Consumer Goods Makers' *Reuters* (22 March 2021) <https://www.reuters.com/article/india-retail-reliance-privatelabels-idUSKBN2BE0B9> accessed 6 December 2021; Malavika Velayanikal, 'Happy Days for Customers as Retailers go the Private Label Way' *Livemint* (10 November 2019) <https://www.livemint.com/companies/start-ups/happy-days-for-customers-as-retailers-go-the-private-label-way-1573392752234.html> accessed 6 December 2021.

75 Sunder Tandon, 'Private Labels to Help Drive Profitable Growth for E-commerce Marketplaces: Report' *Livemint* (26 February 2020) <https://www.livemint.com/industry/retail/private-labels-to-help-drive-profitable-growth-for-e-commerce-marketplaces-report-11582728645180.html> accessed 6 December 2021.

76 Julie Creswell (n 34).

Explanation.—For the purposes of this clause—
(a) a company shall be deemed to be a holding company of another company even if its control is exercised by another subsidiary company of the holding company;
(b) the composition of a company's Board of Directors shall be deemed to be controlled by another company if that other company by exercise of some power exercisable by it at its discretion can appoint or remove all or a majority of the directors;
(c) the expression "company" includes any body corporate;
(d) "layer" in relation to a holding company means its subsidiary or subsidiaries;

in India such as Walmart-owned Flipkart[77] or Ajio,[78] etc. which also operate their own private labels. This article argues for the grant of interim relief against Amazon based on the evidence of preferential treatment that has emerged against Amazon[79] and if evidence of preferential treatment were to emerge against some traditional brick-and-mortar stores or even other e-commerce platforms then similar investigations or reliefs could also be demanded against them based on the facts of those cases.

Thus, as explained above, prohibiting Amazon from operating as a seller on its own marketplace is the only viable non-redundant interim relief that could be granted that addresses the competition concerns at issue. Such a restriction would manage to address almost all of the competition concerns ranging from the use of non-public seller data, search bias, preferential treatment, exclusive agreements etc. by removing the incentive which leads Amazon to engage in such conduct. The subsequent sections of this paper discuss the manner in which this proposed relief satisfies the elements of the *Steel Authority of India Ltd*. test and therefore can be granted by the CCI under section 33 of the Competition Act.

A. Element 1: Contravention Has Been Committed and Continues to Be Committed - Satisfaction of A 'Higher Than *Prima Facie*' Standard of Proof.

The standard for passing an interim order under section 33 is higher than the standard for initiating an investigation under section 26(1).[80] According to the Supreme Court, for initiating an investigation the Commission needs to reach a "*tentative view at that stage*" whereas for granting interim relief there should be "*a definite expression of the satisfaction recorded by the Commission upon due application of mind*".[81] Since the CCI in *Delhi Vyapar Mahasangh* has already formed a *prima facie* opinion that there exists a contravention, the subsequent emergence of additional internal documents and

---

[77] Flipkart also a range of private brands. See Vishnu Sreekumar, 'Quality First: How Flipkart's Private Labels Bring Trust and Affordability to the Indian Market' (*Flipkart Stories*, 25 April 2019) <https://stories.flipkart.com/flipkart-private-brands-trust-affordability/> accessed 6 December 2021.

[78] Ajio sells private labels such as 'Ajio Own'. See <https://www.ajio.com/help/whoweare> accessed 6 December 2021; Rasul Bailay, 'Reliance Retail's Private Labels Outpace Top Fashion Brands Like Puma, Nike on Ajio' *The Economic Times* (18 September 2021) <https://economictimes.indiatimes.com/industry/services/retail/ajios-private-labels-outpace-top-fashion-brands/articleshow/86304404.cms?from=mdr> accessed 6 December 2021.

[79] See (n 32-36).

[80] *Steel Authority of India Ltd*. (n 63) [31], [119].

[81] ibid [117].

evidence should concretize proof of contravention and meet the 'higher than *prima facie*' standard required under section 33. Specifically, in the context of smartphones, Reuters reported that Amazon gave preferential treatment to its Special Merchant, Cloudtail, and helped it enter into deals with tech companies such as Apple, Microsoft and OnePlus including exclusive deals to sell their smartphones.[82] This information is directly relevant for *Delhi Vyapar Mahasangh* which pertains to the exclusive sale of smartphones and proof of Amazon brokering such exclusive tie-ups for its special merchants would meet the higher standard stipulated for grant of interim relief. For other product categories too, especially textiles and categories in which Amazon's private labels compete, the reports' claim to be based on substantial evidence (including internal memos and reports) of unfair preferential treatment, manipulation of search results and use of third-party internal data which warrant closer scrutiny and could potentially satisfy the higher than *prima facie* threshold required under section 33.

In any event, as argued in the earlier section of this paper,[83] the competition investigation against Amazon should be designed to look at the agreements of Amazon with third-party sellers/ preferred sellers more generally rather than examining a few distinct product categories. Consequently, the CCI need not look for 'higher than *prima facie*' evidence for vertical agreement in each product category separately. Instead, the CCI should examine whether there exists evidence of vertical agreement between Amazon and its preferred sellers more generally. The constituent elements of a vertical agreement under section 3(4), as discussed earlier, are: (i) the existence of an agreement; (ii) amongst enterprises at different levels or stages of the production chain; (iii) which causes or is likely to cause an 'appreciable adverse effect on competition'. For Amazon, each of these elements can be proved to a 'higher than *prima facie*' standard. For the first two elements, the existence of at least some of these agreements and relationships between Amazon and a few sellers is a matter of public record and is not contested even by Amazon. For instance, Amazon's joint venture with Catamaran and Patni Group which resulted in the creation of special merchants such as Cloudtail[84]

---

82 Kalra, 'Test the Boundaries' (n 3).

83 See text in Part IV titled 'Need to Broaden the Scope of Competition Investigation'.

84 Nisha Poddar, 'Narayana Murthy to Partner with Amazon for E-commerce Business in India' *The Economic Times* (27 June 2014) <https://economictimes.indiatimes.com/tech/ites/narayana-murthy-to-partner-with-amazon-for-e-commerce-business-in-india/articleshow/37267628.cms?from=mdr> accessed 6 December 2021; Mihir Dalal & Shrutika Verma, 'Amazon's JV Cloudtail is its Biggest Seller in India' *Livemint* (29 October 2015) <https://www.livemint.com/Companies/RjEDJkA3QyBSTsMDdaXbCN/Amazons-JV-Cloudtail-is-its-biggest-seller-in-India.html> accessed 6 December 2021; 'Amazon, Catamaran to End Cloudtail Joint Venture Next Year' *The Times of India* (9 August 2021)

and Appario[85] are all matters of public record. Any doubt regarding the existence of such agreements also stands clarified in light of subsequent evidence highlighted by Reuters' reports.[86]

What could be contested by Amazon is the satisfaction of the third element of section 3(4) - whether these agreements cause or are likely to cause 'appreciable adverse effect on competition'. Once again,the reports of Reuters,[87]the Wall Street Journal,[88] the New York Times,[89] the Markup,[90] the Capitol Forum[91] etc. provide substantial evidence of preferential treatment and 'appreciable adverse effect on competition' attributable to Amazon's engagement with preferred sellers and its foray in private labels. Although the Reuters reports are primarily the ones that concern the company's conduct in India, even the other reports and studies conducted in the context of other jurisdictions could provide useful insights and learnings into Amazon's core infrastructure, search algorithm or common practices.[92] These reports reveal that Amazon has access to non-public seller data (including search data, price sensitivity data and information about previous transactions of each customer) which allows it to target its private label products with almost perfect precision.[93] Some of this additional data that Amazon has access to is extremely useful. For instance, some reports suggest that Amazon's private

---

<https://timesofindia.indiatimes.com/business/india-business/amazon-catamaran-to-end-cloudtail-joint-venture-next-year/articleshow/85181383.cms> accessed 6 December 2021 (Although both companies have announced that the joint venture will be discontinued from 2022).

85 Digbijay Mishra, 'Amazon Forms JV with Patni' *The Times of India* (25 September 2017) <https://timesofindia.indiatimes.com/business/india-business/amazon-forms-jv-with-patni/articleshow/60820854.cms> accessed 6 December 2021; 'Amazon may not Renew Venture with Patni Group' *The Hindu Business Line* (11 November 2021) <https://www.thehindubusinessline.com/companies/amazon-may-not-renew-venture-with-patni-group/article37424077.ece> accessed 6 December 2021 (Although there are news that the JV with Patni Group may also be dissolved).

86 Kalra, 'Test the Boundaries' (n 3); Aditya Kalra, 'Amazon Deployed Secret Strategy to Dodge India's Regulators, Documents Show' *Reuters* (17 February 2021) <https://www.reuters.com/article/amazon-india-operation-ecommerce-idUSKBN2AH1HY> accessed 6 December 2021.

87 Kalra, 'Test the Boundaries' (n 3); Kalra & Stecklow, 'The Imitation Game' (n 3).

88 See (n 33).

89 See (n 34).

90 See (n 35).

91 See (n 36).

92 As a corollary, the Reuters report although based on Amazon's conduct in India has been relied upon to demand that the investigation against Amazon be expanded in the EU and the U.S. Congress has also relied upon it to demand an explanation from the company. See (n 43-44) and accompanying text.

93 'Amazon: EC Investigation to Focus on Whether Amazon uses Data to Develop and Favour Private Label Products; Former Employees say Data Key to Private Label Strategy' (*The Capitol Forum,* 5 November 2018) <https://thecapitolforum.com/wp-content/uploads/2018/11/Amazon-2018.11.05.pdf> accessed 6 December 2021.

label team has access to its database of search terms that customers frequently use and these terms are added to descriptions of Amazon's private label products which boosts the ranking of the products on the search results page.[94] Similarly, it has been suggested that Amazon has access to data about consumers' price sensitivity points, their buying patterns and the items they have viewed in the past- all of which are used by the company to push its private label products on consumers. Using data which is not available to other sellers and more egregiously using the non-public internal data of sellers, Amazon increases the conversion rates for its private labels and since the search algorithm looks at the conversion rates of products, it succeeds in artificially increasing the ranking of its private labels.[95]Although Amazon claims that it has a company policy prohibiting employees from using internal seller data, employee testimonials reveal that in fact employees have unfettered access to this data and its use in decision-making is pervasive to the extent that such data was even openly discussed in company meetings.[96]

Other studies reveal that Amazon accords prominent placement to its private labels in comparison to competing products[97] - even when these competing products have higher customer ratings and more sales.[98] This was frequently achieved through 'search seeding' and the use of 'search sparkles'.[99]Additionally, it seems that Amazon has recently optimized its search algorithm so that instead of showing customers primarily the most relevant and best-selling listings the site also gives a boost to items that are more profitable for the company – a move which has been claimed to favour

---

[94] Dana Mattioli, 'How Amazon Wins: By Steamrolling Rivals and Partners' *The Wall Street Journal* (22 December 2020) <https://www.wsj.com/articles/amazon-competition-shopify-wayfair-allbirds-antitrust-11608235127> accessed 6 December 2021.

[95] *The Capitol Forum* (n 91).

[96] ibid; Dana Mattioli, 'Amazon Scooped up Data from its Own Sellers to Launch Competing Products' *The Wall Street Journal* (23 April 2020) <https://www.wsj.com/articles/amazon-scooped-up-data-from-its-own-sellers-to-launch-competing-products-11587650015> accessed 6 December 2021 (Based on revelations made in these reports Amazon has stated that it has launched an internal investigation. However, nothing is known yet about the progress or outcomes of these supposed internal investigations).

[97] 'Amazon: By Prioritising its Own Fashion Label Brands in Product Placement on its Increasingly Dominant Platform, Amazon Risks Antitrust Enforcement by a Trump Administration' (*The Capitol Forum*, 13 December 2016) <https://thecapitolforum.com/wp-content/uploads/2016/07/Amazon-2016.12.13.pdf> accessed 6 December 2021.

[98] Adrianne Jeffries & Leon Yin, 'Amazon Puts its Own "Brands" First above Better-rated Products' (*The Markup*, 14 October 2021) <https://themarkup.org/amazons-advantage/2021/10/14/amazon-puts-its-own-brands-first-above-better-rated-products> accessed 6 December 2021 (the Markup study has even claimed that- "*When we analyzed star ratings and number of reviews, neither could predict much better than a coin toss which product Amazon placed first in search results*").

[99] Kalra & Stecklow, 'The Imitation Game' (n 3).

Amazon's private labels.[100] Frequently private labels or products sold by its preferred sellers are labelled as "best seller" or "Amazon's choice" – titles which could potentially drive up sales.[101]Amazon also allegedly puts several restrictions on the advertisements that rival device manufacturers could buy on its website.[102]

In the light of all the evidence and information already in the possession of the CCI regarding Amazon's anti-competitive conduct and subsequent material, studies and evidence reported by various sources, the standard of proof required for the grant of interim relief has been met. The elements of section 3(4), namely, the existence of a vertical agreement which causes or is likely to cause an 'appreciable adverse effect on competition' have been proven to a 'higher than *prima facie*' threshold.

B. Element 2: Necessary to Issue an Order of Restraint

The second leg of the *Steel Authority of India Ltd*. test to grant interim relief under section 33 involves an evaluation of the balance of convenience[103] and whether justice would be best served by passing the interim order- whether the extant position can be restored at a later stage or the likely damages be compensated.[104]Amazon is a multi-sided platform which services two broad categories of 'consumers': (i) end-consumers who purchase products on the platform; and (ii) sellers or retailers who utilize the platform for selling their products and reaching the consumer. Notwithstanding the Neo-Brandeisian critique of the 'consumer welfare' standard,[105] even the conventional nar-

---

[100] Dana Mattioli, 'Amazon Changed search algorithm in ways that boost its own products' *The Wall Street Journal* (16 September 2019) <https://www.wsj.com/articles/amazon-changed-search-algorithm-in-ways-that-boost-its-own-products-11568645345> accessed 6 December 2021.

[101] *The Capitol Forum* (n 95); Shane Shifflett and others (n 33).

[102] Dana Mattioli and others, 'Amazon Restricts How Rival Device Makers Buy Ads on its Site' *The Wall Street Journal* (22 September 2020) <https://www.wsj.com/articles/amazon-restricts-advertising-competitor-device-makers-roku-arlo-11600786638?mod=article_inline> accessed 6 December 2021; Adrianne Jeffries & Leon Yin (n 98).

[103] *Federation of Hotel & Restaurant Associations of India v MakeMyTrip India (P) Ltd* 2021 SCC OnLine CCI 12 (India) [106].

[104] *Confederation of Real Estate Developers Assn of India v Department of Town and Country Planning, Government of Haryana* 2018 SCC OnLine CCI 6 (India) [22].

[105] This presupposes that competition law is concerned with harm to 'consumer welfare'. This premise is now the subject of much debate and has been questioned by Neo-Brandeisian scholars who claim that traditional notions of 'consumer welfare' are too narrow and that competition law should be concerned more broadly with concentration of power or market structure. Without expressing an opinion on whether 'consumer welfare' is or should be the basis of Indian competition law assessment- this article argues that even if competition law is narrowly concerned with 'consumer welfare', a consumer welfare assessment would also need to account for the impact on retailers as they are also consumers of Amazon. For an overview of primary Neo-Brandeisian ideas see Tim Wu, The Curse of Bigness: Antitrust in

row notion of 'consumer welfare' would examine the impact of Amazon's conduct on both categories of consumers, that is, end-consumers as well as retailers.[106]A common mistake often committed in competition assessment of Amazon's conduct is omitting to include retailers as a category of 'consumer' while assessing 'consumer welfare.' Such inadvertent exclusion of retailers from the category of 'consumers' allows Amazon to over-emphasize the benefits that Amazon brings to end-consumers such as wide choice, discounted prices, ease of access etc. Apparent damage to retailers is excluded from 'consumer welfare' assessment by painting them as 'competitors' rather than 'consumers.' However, it must be remembered that at its core, Amazon is a platform connecting sellers to buyers. Retailers on Amazon's platform are Amazon's 'consumers' first and only in certain scenarios do they become competitors which in turn creates the conflict of interest that incentivizes Amazon to engage in anti-competitive conduct. Thus, when determining the necessity of interim relief even the conventional stringent standard of 'consumer welfare' would analyse the impact of Amazon's conduct on both categories of consumers, namely, end-consumers and retailers.

Impact on End-Consumers

Through preferential treatment of private labels and preferred sellers, end-consumers are denied choice and access to potentially higher-quality or even cheaper products that are suppressed in the ranking.[107] Especially when preferentially placed products are not identified as such then their prominent placement might run antithetical to consumers' belief that the ranking of products on Amazon's results page is done on the basis of relevance or price

---

the New Gilded Age (2018); Lina M Khan, 'Amazon's Antitrust Paradox' (2016) 126 Yale Law Journal.

[106] The definition of 'consumer' under the Competition Act 2002 is broad and would cover both end-consumers and retailers. See the Competition Act 2002, s 2(f):

"consumer" means any person who –

(i) buys any goods for a consideration which has been paid or promised or partly paid and partly promised, or under any system of deferred payment and includes any user of such goods other than the person who buys such goods for consideration paid or promised or partly paid or partly promised, or under any system of deferred payment when such use is made with the approval of such person, whether such purchase of goods is for resale or for any commercial purpose or for personal use;

(ii) hires or avails of any services for a consideration which has been paid or promised or partly paid and partly promised, or under any system of deferred payment and includes any beneficiary of such services other than the person who hires or avails of the services for consideration paid or promised, or partly paid and partly promised, or under any system of deferred payment, when such services are availed of with the approval of the first-mentioned person whether such hiring or availing of services is for any commercial purpose or for personal use.

[107] Adrianne Jeffries & Leon Yin (n 98).

or quality of the product. Thus, end consumers might even be unaware of the harm being inflicted on them. Additionally, by suppressing and eventually excluding sellers and retailers, Amazon potentially dampens innovation and affects choice and quality of future products for end consumers.

Impact On Retailers

On the other side of the platform, Amazon's conduct harms the sales and profit margins of small retailers and sellers and even results in their exclusion. As its power grows and it becomes an unavoidable trading partner for many retailers, Amazon's ability to inflict damage on them and the severity of such damage by preferential treatment of private brands also increase. The gradual diminution of profits and market share as well as eventual exclusion from the market are potentially irreversible for smaller players. Amazon creates an uneven playing field and builds entry barriers through preferential treatment which cannot be overcome by an equally efficient or even superior retail competitor of Amazon's private labels. The true extent of the damage might be impossible to calculate as some of Amazon's brands or its association with certain retailers are unknown and even otherwise difficult to discern.[108]

Thus, Amazon's anti-competitive conduct harms consumers on both sides of its platform.

Potential Benefits of Amazon?

Amazon, for its part, claims that it connects small sellers to consumers and in fact, helps consumers on both sides of the platform. It helps retailers and entrepreneurs grow their business[109] and brings several benefits to

---

[108] Julie Creswell (n 34).

[109] 'Amazon enables digitization of over 1 million small businesses in India' *Business Standard* (21 December 2020) <https://www.business-standard.com/article/companies/amazon-enables-digitisation-of-over-one-million-small-businesses-in-india-120122000674_1.html> accessed 6 December 2021; 'Amazon Small Business Days 2021 Sees Record Sales for 84,000 SMEs' *The Economic Times* (12 July 2021) <https://economictimes.indiatimes.com/small-biz/sme-sector/amazon-small-business-days-2021-sees-record-sales-for-84000-smes/helping-smes/slideshow/84336483.cms> accessed 6 December 2021; 'Amazon India Ramps up SMB Participation for Prime Day, Calls Ecommerce an 'Amplifier' for Small Businesses' *The Economic Times* (20 July 2021) <https://economictimes.indiatimes.com/small-biz/sme-sector/amazon-india-ramps-up-smb-participation-for-prime-day-calls-ecommerce-an-amplifier-for-small-businesses/articleshow/84573900.cms> accessed 6 December 2021; Manish Singh, 'Amazon to Invest $1 Billion to Help Digitize Small Businesses in India' (*TechCrunch*, 15 January 2020) <https://techcrunch.com/2020/01/14/amazon-to-invest-1-billion-to-digitize-small-businesses-in-india/> accessed 6 December 2021; See also 'Amazon's Impact on Economic Growth in India' (*Amazon*) <https://www.aboutamazon.

the end-consumer in the form of wider choice, discounted products, ease of shopping (especially during the pandemic) etc.[110] However, this claim obfuscates the illegality of certain selected practices of Amazon behind the overall utility of the platform. Overall, the benefits which Amazon brings as an e-commerce platform are conspicuous and, in that sense, Amazon's appeal to the consumers and to retailers which has resulted in its unprecedented rise is a testament to the utility of the platform. However, while considering the anti-competitive nature of certain specific practices of Amazon (namely, its vertical agreements with preferred sellers or retailers selling private labels, preferential treatment etc.), one cannot consider the utility of the entire platform. As per this logic, there would never arise any finding of appreciable adverse effect on competition since all products or services available in the market are of some utility to the consumers- the question which needs to be asked is whether the specific practices in question (such as self-preferencing or exclusive tie-ups etc.) bring any benefits to the consumer and not whether the overall product or service (i.e., Amazon's online marketplace) is of utility to the consumer. The anti-competitive impact of Amazon's practices as a seller must be considered in isolation and should not be confused with the benefits which may arise when Amazon operates in a different role that of a marketplace platform. Even the proposed interim relief is limited to curtailing only specific anti-competitive practices of Amazon without prohibiting

---

in/impact/economy/growth> accessed 6 December 2021; 'Amazon SMB Impact Report Highlights Success of Indian Small and Medium Businesses Despite Covid-19 (*Amazon,* 20 December 2020) <https://www.aboutamazon.in/news/small-business/amazon-smb-impact-report-highlights-success-of-indian-small-and-medium-businesses-despite-covid-19> accessed 6 December 2021.

[110] Vijay Govindrajan & Anita Warren, 'How Amazon Adapted its Business Model to India' (*Harvard Business Review* 20 July 2016)<https://hbr.org/2016/07/how-amazon-adapted-its-business-model-to-India> accessed 6 December 2021; Nidhi Singal, '65% Customers Order from Tier 2 and Beyond on Amazon India, Says Amazon India V-P' *Business Today* (11 October 2021) <https://www.businesstoday.in/latest/corporate/story/65-customers-order-from-tier-2-and-beyond-on-amazon-india-says-amazon-india-v-p-309065-2021-10-11> accessed 6 December 2021; Digbijay Mishra, 'Business Back to Normal, Non-metros Driving Growth, New Customer Addition: Amazon's Tiwary' *The Economic Times* (9 July 2021) <https://economictimes.indiatimes.com/tech/technology/business-back-to-normal-non-metros-driving-growth-new-customer-addition-amazons-tiwary/articleshow/84248760.cms?from=mdr> accessed 6 December 2021; See also 'Price Gouging has no Place in Our Stores' (*Amazon*, 24 March 2020) <https://www.aboutamazon.com/news/company-news/price-gouging-has-no-place-in-our-stores> accessed 6 December 2021; 'How Amazon is Supporting India in Response to COVID-19' *(The Amazon Blog*, 4 May 2021) <https://blog.aboutamazon.co.uk/company-news/how-amazon-is-supporting-india-in-response-to-covid-19> accessed 6 December 2021; 'Amazon to Airlift, Import and Donate 100 ICU Ventilator Units from the US to Ramp up India's Supplies for Fighting COVID-19' (*Amazon,* 27 April 2021) <https://www.aboutamazon.in/news/company-news/amazon-to-airlift-import-and-donate-100-icu-ventilator-units-from-the-us-to-ramp-up-indias-supplies-for-fighting-covid-19> accessed 6 December 2021.

or affecting its operations as a marketplace platform in any way. Thus, any benefits brought to end-consumers and retailers through Amazon's overall marketplace platform cannot be part of the equation while judging the anti-competitive impact of specific practices.

In addition to the potential harm done to both categories of consumers, the need for interim relief becomes even more evident in light of the protracted and time-consuming nature of competition investigation and proceedings in India. The Commission itself has noted in the past that cases where the inquiry is expected to take time thereby exaggerating the risk of irreparable and irretrievable consequences are especially suited for the passing of interim orders.[111]Although the competition investigation against Amazon commenced in 2020, the investigation by the Director General itself is still continuing and will take some time especially given the technical and complex nature of the issues involved. Unlike some other jurisdictions, the Indian competition regulator does not yet have the power to settle the case or other tools (such as commitments) to avoid the protracted investigation and litigation process. In jurisdictions such as the European Union where such mechanisms exist, Amazon is reportedly already in talks to settle its antitrust cases.[112] In India where none of these mechanisms are yet available, the investigation will be followed by written and oral submissions of all parties and multiple hearings before the Commission.[113] Altogether it would take a few years for the Commission to give its final order and several more years for the (inevitable) appeals to be concluded.[114] The extensive use of appeals and associated delay is already on display in the case of Amazon where even the CCI's *prima facie* order initiating investigating was subjected to a string of appeals going all the way up to the Supreme Court.[115] These appeals have already delayed the investigation. Even after the issuance of the final order and conclusion of appeals, enforcement of the order and litigation around enforcement could still take many more years. Too much (unquantifiable

---

[111] *Confederation of Real Estate Developers Association of India* (n 102) [23]; *Nuziveedu Seeds Ltd v Mahyco Monsanto Biotech (India) Ltd* 2016 SCC OnLine CCI 48 (India) [24].

[112] Foo Yun Chee, 'Amazon Seeking to Settle EU Antitrust Investigations, Sources Say' *Reuters* (9 November 2021) <https://www.reuters.com/business/retail-consumer/exclusive-amazon-seeking-settle-eu-antitrust-investigations-sources-say-2021-11-09/> accessed 6 December 2021.

[113] The Competition Act 2002, s 36; The Competition Commission of India (General) Regulations, regs 36, 20, 21, 29, 44, 45, 48.

[114] The final order of the CCI can be appealed to the National Company Law Appellate Tribunal and the Supreme Court. *See* The Competition Act 2002, ss 53B, 53T.

[115] *Amazon Seller Services (P) Ltd v CCI* 2021 SCC OnLine Kar 12626, High Court of Karnataka (India); *Flipkart Internet (P) Ltd v CCI* SLP (C) No. 11558 of 2021 decided on 9-8-2021, Supreme Court of India.

and irreversible)[116] harm might already have been inflicted on both the end consumers and the retailers if we were to wait for the final order against Amazon. Thus, there exists an urgent need for interim relief.

C. Element 3: Likelihood of Irreparable and Irretrievable Damage or Definite Apprehension of Adverse Effect on Competition

As per the third leg of the *Steel Authority of India Ltd*. test, while granting interim relief under section 33, the CCI would consider the balance of convenience and look at the consequences of granting such relief on both parties.[117] Which interests if harmed can be subsequently compensated and which interests will be irreparably harmed and hence need to be protected through interim measures. The CCI recently in *FHRAI v MMT* noted that the third element of the *Steel Authority of India Ltd*. test consists of two limbs and the satisfaction of either of these two conditions is sufficient to make a case for interim relief.[118] Either there should be a likelihood of irreparable and irretrievable harm or there should be a definite apprehension of adverse effect on competition in the market. In the case against Amazon, it is clear as discussed above that the second limb has been satisfied and there is a definite apprehension of adverse effect on competition by making the field uneven through unfair and preferential treatment.

A case can be made that the first limb has also been satisfied as there is a likelihood of irreparable and irretrievable damage. The CCI has previously noted that where damage cannot be quantified in terms of money, interim relief ought to be granted.[119] In this case, it is extremely difficult to measure the extent or quantum of damage being inflicted on end-consumers through preferential ranking and the damage done to sellers by making the playing field uneven. For instance, if Amazon is found to have engaged in preferential treatment of products sold by certain preferred sellers, then how does one measure the damage done to the end-consumer as a result of such preferential treatment. Final penalty orders even if they were to prescribe behavioural changes would be unable to reverse the damage already done given the

---

[116] See Part C titled 'Element 3: Likelihood of irreparable and irretrievable damage or definite apprehension of adverse effect on competition'.

[117] *Nuziveedu Seeds Ltd v Mahyco Monsanto Biotech (India) Ltd* 2016 SCC OnLine CCI 48 (India) [25]; *Federation of Hotel & Restaurant Associations of India. MakeMyTrip India (P) Ltd* 2021 SCC OnLine CCI 12 (India) [106].

[118] *Federation of Hotel & Restaurant Associations of India v MakeMyTrip India (P) Ltd* 2021 SCC OnLine CCI 12 (India) [108].

[119] *Indian National Shipowners' Assn v ONGC Ltd* 2018 SCC OnLine CCI 48 (India),[11]; *Fast Track Call Cab (P) Ltd v ANI Technologies (P) Ltd* 2017 SCC OnLine CCI 36,[14].

dynamic nature of the market. Importantly, the Indian competition regime in addition to penalizing enterprises engaging in anti-competitive conduct also envisages compensation for the victims.[120] However, computing compensation even after the issuance of the final order in such a case would be potentially futile and would probably underestimate the extent of the damage.[121] Identifying even the direct victims of Amazon's anti-competitive conduct (end-consumers and sellers) would be almost impossible. Formulation of acceptable damage quantification techniques and eventual disbursement of monetary compensation to victims also seems extremely difficult if not entirely unfeasible. For instance, even if preferential treatment by Amazon is established, would all customers and sellers on Amazon's platform during that time period be eligible to be compensated and how could the damage done to customers or sellers by repression of the more relevant results in the ranking be calculated. All of this indicates the unquantifiable and irreparable nature of the damage that is caused by Amazon's anti-competitive conduct which cannot be *post facto* adequately calculated or compensated and must be curtailed at the earliest through the issuance of interim relief.

On the other hand, prohibiting Amazon from operating in the capacity of seller at the interim stage would not cause irreparable damage to the enterprise. Even if the conduct in question is finally determined to not have been anti-competitive, the underlying infrastructure, big data, supply and distribution chains etc. which have enabled Amazon to expand its private label business would continue to exist and could be leveraged at a later point, making it easier for the company to re-enter as a seller. Thus, the balance of convenience lies in favour of granting interim relief and protecting retailers and end-consumers from irreparable and irretrievable damage.

VI. Operationalization of Interim Relief

While the proposed interim relief which prohibits Amazon to act in the capacity of a seller on its own marketplace is easy to prescribe in principle, the exact phrasing and operationalization of this interim relief might admittedly pose some issues. For instance, Amazon could ensure that it is not directly selling on its own platform but is doing so through other entities whose association with Amazon is hidden behind several layers of complex corporate structures. In fact, the foreign direct investment rules in India have already encountered this problem on numerous occasions while attempting

[120] The Competition Act 2002, s 53N.

[121] cf as an example see the discussion around identification of affected class of consumers and problems of quantification of damages in *Mastercard Incorporated v Walter Hugh Merricks*, (2020) UKSC 51.

to prohibit FDI in inventory-based e-commerce.[122] The rules prohibiting FDI in inventory-based e-commerce should have had the same effect as the proposed interim relief of prohibiting Amazon from holding inventory and operating as a seller on its platform.[123] However, these FDI rules have failed to have the desired effect and several instances have been brought to light where e-commerce companies have devised creative corporate restructuring techniques to bypass the FDI rules.[124]

To avoid a similar fate, the interim relief could be made clearer by specifying that neither Amazon nor its associate companies nor its subsidiary companies directly or indirectly operate as sellers on its platform and by emphasizing that the prohibition should be followed in letter and in spirit. However, even then Amazon could dilute its investment in the sellers or make other structural changes just to create enough wriggle room to subsequently argue that the sellers on its platform do not fall within the definition of 'associate company'[125] or 'subsidiary company'.[126] Thus, in spite of best efforts at precision, there is always a chance that corporate restructuring or creative interpretation could be used to subvert the essence of the prohibition.

However, even if precise drafting of interim relief is difficult and there is a risk of subversion of interim order in spirit through corporate restructuring, the interim relief should nevertheless be issued. At the very least it would compel Amazon to change its practices to avoid the most direct and obvious infringements of the prohibition. Even otherwise, mounting regulatory pressure through the issuance of an interim order might have an important signaling effect and might influence Amazon to refrain from engaging in the use of corporate restructuring or other techniques to subvert the essence of the order. For instance, ongoing investigations by the Enforcement Directorate and the CCI have already resulted in some domestic entities announcing that they will discontinue their joint ventures with Amazon even as they assert that these partnerships have always been 'technically compliant' with Indian

[122] 'India Plans Foreign Investment Rule Changes that Could Hit Amazon' *Reuters* (19 January 2021) <https://www.reuters.com/world/india/exclusive-india-plans-foreign-investment-rule-changes-that-could-hit-amazon-2021-01-19/> accessed 6 December 2021; 'Amazon Changes Business Structure in India After New E-commerce Rules' *The Hindustan Times* (7 February 2019) <https://www.hindustantimes.com/business-news/amazon-changes-business-structure-in-india-after-new-e-commerce-rules-report/story-CxRClbBMr1kv5feZEGXh2N.html> accessed 6 December 2021.

[123] Note that although import of the existing FDI regulations and the proposed interim relief might be the same, the two would be in response to very different regulatory objectives. The proposed interim relief would be in direct response to Amazon's anti-competitive practices and in exercise of the Commission's powers to curtail such practices.

[124] See (n 120).

[125] The Companies Act 2013, s 2(6).

[126] The Companies Act 2013, s 2(87).

laws.[127]Thus the threat of regulatory intervention seems to have at least some effect on the practices of these companies. Hence, even if there exists a risk that Amazon would try to subvert the interim order through corporate structures, the order should nevertheless be issued.

VII. Suo Moto Action Taken by the CCI on the basis of the Reuters Report

It is notable that the CCI recently took *suo moto* cognizance of the Reuters report but ultimately decided not to pursue an inquiry purely on the basis of the submissions made by Amazon in its affidavit.[128] Primarily, Amazon raised corporate structuring defences which obfuscated Amazon's interests in the sale of products carrying its own brand name. Amazon submitted an affidavit that Amazon Seller Services Pvt. Ltd. ("ASSPL"), the entity engaged in operating Amazon's online marketplace in India does not directly or indirectly sell anything on its own marketplace. Instead, Amazon.com, Inc., the parent company, has two other wholly owned subsidiaries which license the IP of Amazon brands to third-party sellers that sell these Amazon branded products on the online marketplace.[129] This obfuscates the fact that the biggest third-party sellers of Amazon-branded products, such as Cloudtail and Appario are the result of Amazon's joint ventures with domestic players. Undoubtedly, the Amazon entity entering into a joint venture to operate Cloudtail and Appario would also not be directly related to ASSPL, the entity operating the online marketplace, but it would still be a part of the Amazon group. For instance, it is evident from recent combination review filings before the CCI that another wholly owned subsidiary of Amazon.com, Inc., Amazon Asia-Pacific Resources Pvt. Ltd. owns the majority share in Cloudtail, a major third-party seller on the Amazon marketplace (see Fig.1 below).[130] Thus, it is clear that all entities, the one operating Amazon's marketplace (ASSPL) or the one selling Amazon-branded products on the

---

[127] 'Amazon, Catamaran to End Cloudtail Joint Venture Next Year' *The Times of India* (9 August 2021) <https://timesofindia.indiatimes.com/business/india-business/amazon-catamaran-to-end-cloudtail-joint-venture-next-year/articleshow/85181383.cms> accessed 6 December 2021; 'Amazon May not Renew Venture with Patni Group' *The Hindu Business Line* (11 November 2021) <https://www.thehindubusinessline.com/companies/amazon-may-not-renew-venture-with-patni-group/article37424077.ece> accessed 6 December 2021.

[128] *Amazon India Marketplace*, *In re* 2022 SCC OnLine CCI 19.

[129] ibid [5]-[7].

[130] Acquisition of Prione Business Services Pvt. Ltd. by Amazon Asia-Pacific Resources Pvt. Ltd., Combination Registration No. C-2021/12/893, approved on 9 March 2022 <https://www.cci.gov.in/combination/order/details/summary/77/0>; <https://www.cci.gov.in/combination/press-release/details/17/0>.

marketplace (such as Cloudtail) are directly or indirectly related to the ultimate parent entity of the Amazon group i.e., Amazon.com, Inc. The inherent conflict of interest (discussed in Section V) doesn't just arise when ASSPL (the entity operating the online marketplace) itself sells Amazon-branded products. It persists even when the entities involved are legally distinct but are still part of the same group and have unified economic goals and interests.

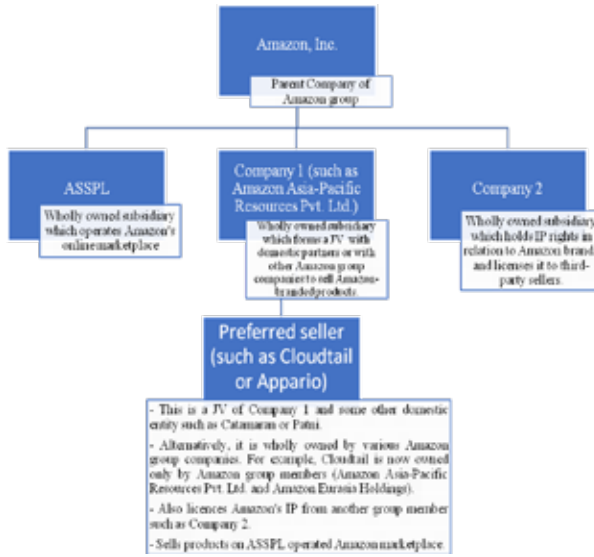

Fig 1: An example of Amazon group companies operating in different capacities on Amazon's online marketplace- although the entity operating the marketplace and the one selling Amazon-branded goods on the marketplace might be legally distinct, the linkages and connections between them are clearly borne out.[131]

Quite apart from the direct or indirect stake of these group members in each other, it is also worth examining how these group companies interact with each other in practice. For instance, how does data collection, processing and sharing work across them. Does ASSPL share the data collected on its online marketplace with Company 1 (from Fig. 1 above)? Merely claiming that ASSPL does not share data with Preferred sellers (directly) is insufficient as the same end could be achieved if the data pool of all the group companies is common or ASSPL shares data with Company 1. It is also worth considering the overt and covert influence of the 'Amazon' brand in the

[131] Based on Amazon's affidavit as outlined in the CCI's suo moto order (n 128) and the acquisition of Prione Business Services Pvt. Ltd. by Amazon Asia-Pacific Resources Pvt. Ltd (n130).

ranking on Amazon's marketplace. Even assuming that the entity operating the marketplace and Preferred sellers (selling Amazon-branded products) are not related entities, does retaining the value associated with the 'Amazon' brand incentivize the online marketplace to ensure that these products are amongst the highest-ranked or top-selling products? Further, what is the economic interest (if any) of Company 2, the Amazon group member which acts as the licensor in ensuring that the Amazon-branded products get higher sales, etc. These are just some of the questions which should be examined in greater detail while looking at the interconnections between the different Amazon group companies and their asserted distinct roles on the Amazon marketplace.

The framework of the Competition Act is also no stranger to the idea that group entities could operate together, have common economic goals and parent companies could exercise 'control' over subsidiaries. For instance, section 4 recognizes that dominance could be abused by an enterprise or a group.[132] Similarly, the concept of 'group' plays an important role in merger review.[133] In fact, in a case involving contravention of section 3 or 4, the CCI also has the power to pass an order against other members of the group to which the enterprise in violation belongs.[134] It could even be argued that the definition of 'enterprise'[135] or 'person'[136] under the Competition Act is broad enough to cover subsidiaries of the enterprise and therefore, a section 3(4) analysis could look at the group members entering into agreements more holistically and attempt to trace the connections and linkages between the parties involved instead of simplistically noting that the legal entities are separate. Constraints against looking at the role of group members more holistically are neither built into the language of the statute nor is it desirable.

Using corporate structures in this manner to argue that the entity operating the online marketplace and the one that is selling Amazon-labelled products on the marketplace (through a JV) are distinct corporate or legal entities are age-old tactics to evade regulatory scrutiny. Amazon itself has

---

[132] The Competition Act 2002, s 4(1): No enterprise or group shall abuse its dominant position.

[133] The Competition Act 2002, s 5.

[134] The Competition Act 2002, s 27- Proviso.

[135] The Competition Act 2002, s 2(h) defines an 'enterprise' as 'a person or a department of the Government, who or which is, or has been, engaged in any activity… **either directly or through one or more of its units or divisions or subsidiaries**… [**emphasis added**].' Detailed analysis of this for instance, under the Single Economic Entity doctrine is outside the scope of this paper.

[136] The Competition Act 2002, s 2(h) defines a 'person' as: '…(iii) a company;… (iv) an association of persons..' Thus, an association of companies could fall within the definition of a 'person' and hence group members and their conduct could be analyzed under section 3(4).

used such corporate restructuring as a workaround for FDI regulations.[137] A useful lesson also emerges from CCI's recent suspension of a prior approval that it had granted to Amazon's acquisition of Future group's promoter entity.[138] When the CCI suspended its own prior approval of the combination, it was criticized on the ground that the factual information about Amazon's control over Future's retail arm and all associated agreements had already been filed before the CCI and therefore, the nature and extent of Amazon's control over Future's retail arm should have been apparent to the regulator. Similar to the present case, the control of Amazon over Future's retail arm in that combination too was hiding in plain sight. Instead, even back then the CCI relied purely on Amazon's framing of the narrative and its representations, only to later claim that Amazon had engaged in 'misrepresentation' and 'suppression of information'.[139] The Amazon-Future Coupon combination suspension raises several interesting legal questions which are outside the scope of this paper. However, the crucial takeaway for the present purpose is that the CCI should be more cautious in perusing the information before it. It should try to unravel the interconnections and linkages which are hiding in plain sight and are deliberately obfuscated by parties through creative corporate structuring or imaginative framing of the narrative.

The CCI order in the Amazon suo moto case also relies solely on the affidavit submitted by Amazon.[140] However, as discussed above the CCI has wide powers and could even call for production of documents which are in Reuters' possession and carry out a more detailed investigation into the working of Amazon.[141] The CCI order in the suo moto case initiated on the basis of the Reuter report does not preclude the Commission from reassessing this information. The order itself states that it is not a finding on merits and shall not come in the way of the CCI examining the conduct of ASSPL or any of its related entities.[142] Hence, the CCI should use the Reuters report to expand and reorient the scope of the investigation against Amazon (as argued in Part IV) and to grant interim relief (as argued in Part V).

---

[137] See Section VI: Operationalization of interim relief.

[138] Proceedings against Amazon.com NV Investment Holdings LLC under Sections 43A, 44 and 45 of the Competition Act 2002, order of Dec. 17, 2021 <https://www.cci.gov.in/combination/order/details/order/1138/0>.

[139] Amazon Future suspension order (n 138).

[140] Amazon suo moto case, (n 128)[14].

[141] The Competition Act, 2002, s36(2); The Competition Commission of India (General) Regulations, Regulation– 44 - 45.

[142] Amazon suo moto case, (n 128)[14].

VIII. Conclusion

In recent times, several journalistic reports and studies have emerged which provide substantial evidence about Amazon's anti-competitive conduct. Such conduct stems from Amazon's relationship with its preferred sellers or retailers selling its private labels and appears to be pervasive across product categories. In light of this evidence, this paper has argued for two things. *First*, the competition investigation against Amazon in India should be broadened and should not be limited to only certain product categories. Instead, the investigation should focus on the interactions and vertical agreements between Amazon and preferred sellers/ third-party retailers more broadly and use that as the axle of the investigation. Any variance in competition dynamics across the different product categories could be examined during the course of the investigation. Such an expansion and reorientation of the scope would also be in line with the spirit and elements of section 3(4) of the Competition Act. *Second*, this paper has argued that the test for granting interim relief against Amazon under section 33 has been satisfied. In order to comprehensively address all the competition concerns, the only viable non-redundant interim relief which is available against Amazon is to prohibit it from acting in the dual capacity of marketplace and seller. The paper has shown that necessity and balance of convenience demand that such interim relief be granted.

The Indian competition regulator has initiated multiple competition cases and investigations against digital platforms.[143] Inspite of CCI's apparent interest in digital platforms, only one of these cases has till date culminated in a final order,[144] exposing the regulator to potential averments of performative regulation. The Indian competition regulator should break away from the mould of waiting for foreign competition regulators to take action first and then simply follow in their footsteps. Instead, the CCI should compete actively in the competition amongst competition regulators[145] and take expeditious action on its own depending on the requirements of the domestic market and statutory framework. For this, the CCI needs to act fast and go beyond merely initiating investigations to taking concrete action to protect competition in dynamic technology markets.

---

[143] The CCI has initiated cases against most big digital platforms including Google, Amazon, Facebook, Apple, Uber etc.

[144] *Matrimony.com Ltd v Google LLC* 2018 SCC OnLine CCI 1 (India).

[145] Ludwig Siegele, 'Antitrust Regulators Face Vibrant Competition- With Each Other' (*The Economist*, 8 November 2021) <https://www.economist.com/the-world-ahead/2021/11/08/antitrust-regulators-face-vibrant-competition-with-each-other> accessed 6 December 2021 (notes that the race amongst antitrust regulators to be the best tech regulator is highly competitive although the article refers primarily to regulators in Western jurisdictions and China and unfortunately, does not identify the CCI as a contender in this race at all).

Information About the Journal

The *Indian Journal of Law and Technology* (ISSN 0973-0362) is an academic journal, edited and published annually by students of the National Law School of India University, Bangalore, India. All content carried by the Journal is peer-reviewed except for special comments and editorial notes. The Journal comprises:

- the Board of Advisory Editors, consisting of professionals and academicians pre-eminent in the field of law and technology, which provides strategic guidance to the Journal;
- the Article Review Board, a panel of external peer-reviewers;
- the Editorial Board, consisting of students of the National Law School of India University, which is responsible for selecting and editing all content as well as contributing occasional editorial notes;

OPEN ACCESS POLICY

The *Indian Journal of Law and Technology* is a completely open access academic journal.

- Archives of the journal, including the current issue are available online with full access to abstracts and articles at no cost.
- Please visit the website of the Indian Journal of Law and Technology at "http://www.ijlt.in" to get additional information and to access the archives of previous volumes.

INFORMATION FOR CONTRIBUTORS

The Indian Journal of Law and Technology seeks to publish articles, book reviews, comments and essays on topics relating to the interface of law and technology, particularly those with a developing world perspective.

MODE OF SUBMISSION

Submissions can be in electronic form or in hard copy form. However, submissions in electronic form are strongly encouraged in order to expedite the submission review process. Please address submissions in electronic form to the Chief Editor of the Indian Journal of Law and Technology at "ijltedit@gmail.com".

REGULAR SUBMISSION REVIEW

The Journal shall communicate an acknowledgement to all authors shortly after the receipt of their submissions. The preliminary review of

the submissions shall be completed within four weeks of receipt in usual circumstances. The submissions that are initially accepted shall be blind-refereed by the Article Review Board. The Journal shall make due efforts to complete the entire peer-review process within a reasonable time frame. The Journal shall notify the authors about the exact status of the peer-review process as required.

EXPEDITED SUBMISSION REVIEW

This option is available to those authors who have received an offer of publication from another journal for their submissions. The authors may request an expedited submission review. However, the decision to grant an expedited submission review shall remain at the discretion of the Editorial Board. Please note that requests for an expedited submission review can only be made in relation to submissions in electronic form. All such requests must be accompanied by the following details:

- Name(s) of the author(s) and contact details;
- Title of the submission;
- Details about the journal(s) which has/have offered to publish the submission;
- Whether the offer is conditional or unconditional and, if the offer is conditional, then what conditions are required to be met for final acceptance;
- The date(s) on which the offer(s) expire(s).

The Journal shall make due efforts to accommodate the existing offer(s) and applicable deadline(s). However, upon an oiler of publication pursuant to the expedited submission review, the authors shall have to communicate their decision within five calendar days of the notification or the offer. If there is no response, then the journal shall have the discretion to withdraw the offer.

SUBMISSION REQUIREMENTS

- All submissions must be accompanied by:
  (1) a covering letter mentioning the name(s) of the author(s), the title of the submission and appropriate contact details.
  (2) the résumé(s)/curriculum vitae(s) of the author(s).
  (3) an abstract of not more than 200 words describing the submission.
- All submissions in electronic form should be made in the Microsoft Word file format (.doc or .docx) or in the OpenDocument Text file format (.odt).

- All text and citations must conform to a comprehensive and uniform system of citation. The journal employs footnotes as the method of citation.
- No biographical information or references, including the name(s) of the author(s), affiliation(s) and acknowledgements should be included in the text of the submission, the file name or the document properties. All such information can be provided in the covering letter.
- The Journal encourages the use of gender-neutral language in submissions.
- The Journal shall be edited and published according to the orthographical and grammatical rules of Indian English that is based on British English. Therefore, submissions in American English shall be modified accordingly. The Journal encourages authors to use British English in their submissions in order to expedite the editing process.
- The authors are required to obtain written permission for the use of any copyrighted material in the submission and communicate the same to the Journal. The copyrighted material could include tables, charts, graphs, illustrations, photographs, etc. according to applicable laws.

COPYRIGHT

The selected authors shall grant a licence to edit and publish their submissions to the Journal but shall retain the copyright in their submissions. The aforementioned licence shall be modelled as per a standard author agreement provided by the Journal to the selected authors.

DISCLAIMER

The opinions expressed in this journal are those of the respective authors and not of the Journal or other persons associated with it.

PERMISSIONS

Please contact the Chief Editor of the Indian Journal of Law and Technology for permission to reprint material published in the Indian Journal of Law and Technology.

ORDERING COPIES

Price Subscription (inclusive of shipping) of the IJLT is as follows:

Hard Copy for 2021	Rs.
Hard Copy for 2020	Rs. 900
Hard Copy for 2019	Rs. 900
Hard Copy for 2018	Rs. 800

Order online: www.ebcwebstore.com

Order by post: send a cheque/draft of the requisite amount in favour of 'Eastern Book Company' payable at Lucknow, to:

Eastern Book Company,

34, Lalbagh, Lucknow-226001, India

Tel.: +91 9935096000, +91 522 4033600 (30 lines)