IJLT | THE INDIAN JOURNAL OF LAW AND TECHNOLOGY

Volume 16 | Issue 1 | 2020

[Cite as: 16 IJLT, < page no. > (2020)]

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 16 | Issue 1 | 2020

IJLT | THE INDIAN JOURNAL OF LAW AND TECHNOLOGY

Volume 16 | Issue 1 | 2020

Contents

ARTICLES

Facing up to the Risks of Automated Facial-Recognition Technologies in Indian Law Enforcement

Ameen Jauhar[*]

> "In addition to the admitted lack of precision of the technology, I find it difficult to see how the deployment of a technology that would potentially allow the identification of each single participant in a peaceful demonstration could possibly pass the test of necessity and proportionality."
>
> Joseph Cannataci, UN Special Rapporteur on Privacy

I. Prefatory Remarks

As the world increasingly witnesses numerous dystopian themes transform into reality, the risks posed by emerging technologies driven by *deep learning algorithms* and *artificial intelligence* ('AI') are arguably a prominent theme featuring in many of these conversations. There has been a spate of recent controversies where tech moguls like Facebook, Amazon, Apple, Alphabet,

[*] The author is a Senior Resident Fellow at the Vidhi Centre for Legal Policy, currently heading its Centre for Applied Law & Technology Research, and working on judicial reforms with the JALDI mission. The author would like to acknowledge the tremendous research assistance provided by Mr. Devansh Kaushik (National Law School of India University). The author also thanks Mr. Sebastien Krier (AI policy and ethics adviser) and Mr. Jonas Schuett (Legal Priorities Project), for their valuable inputs on the earlier drafts of this paper.

and Microsoft (infamously christened as the 'Frightful Five')[1] have been at the forefront. These have ranged from illegal data mining to covert development of technology that may evade the necessary regulatory and legal checks and balances in place.[2] These instances certainly warrant the question of how far humanity is prepared to deal with the fallout of deploying these emerging technologies ubiquitously. The answer to that question, for now, appears to be that our regulatory efforts are work in progress at best, and entirely inadequate at worst.

Within the larger discourse of risk mitigation of emerging technologies, the ever-expanding deployment of *automated facial recognition technology* ('AFRT') is garnering much skepticism amongst privacy advocates, and researchers and academics working on the intersection of law and technology. It is designed and trained on large corpuses of digital images of millions of humans, curated through CCTVs, media, social media, and other sources. Basic facial recognition tools use key features of the face and their respective distances from one another to morph a virtual facial map (something akin to sketches made by sketch artists in police stations).[3] The virtual facial map is then referenced to millions of digital images in databases to assess familiarity. However, AFRT is a more refined tool, allowing automatic referencing to occur from (say) CCTV footages that are being recorded in real time. This is what makes it more promising in preventing crime, since there is capacity for identifying a potential 'preparator' in real time, based on the large troves of digital images such technologies are trained on and have access to.[4] Given the sophistication and time efficiency of AFRT in *facial profiling*,[5] it is most commonly being utilised by law enforcement officials across the globe.

The frequently touted benefit of AFRT in law enforcement is its accuracy in discerning unique features, facial tics, potential disguises, and other facets

---

1 Farhaad Manjoo, 'Tech's Frightful Five: They've Got Us' (*The New York Times*, 10 May 2017) <> accessed 2 August 2020.

2 Paul Nemitz, 'Constitutional Democracy and Technology in the Age of AI' *International Review of Law, Computers & Technology* <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3234336> accessed 30 April 2020 (forthcoming).

3 Nila Bala and Caleb Watney, 'What are the Proper Limits on Police Use of Facial Recognition?' (*Brookings Institution*, 2019) <> accessed 30 April 2020.

4 Christopher Rigano, 'Using Artificial Intelligence to Address Criminal Justice Needs' (*National Institute of Justice (US DoJ)*, 2018) <https://nij.ojp.gov/topics/articles/using-artificial-intelligence-address-criminal-justice-needs#sidebar-the-national> accessed April 30, 2020

5 Monique Mann and Marcus Smith, 'Automated Facial Recognition Technology: Recent Developments and Approaches to Oversight' (2017) 40(1) *University of New South Wales Law Journal* 121.

of a human face.[6] Furthermore, unlike conventional security checks, AFRT allows the ability to simultaneously screen numerous individuals from a safe distance.[7] On the other hand, as aforementioned, its inaccurate results, and the dire impact it can cause on individual liberties and informational privacy, are massive risks that have generated a vocal debate against its rampant adoption.[8] In India too, there has been a reported rise of states and law enforcement officials enthusiastically resorting to the use of AFRT.[9] In fact, AFRT has become a pivotal cornerstone in the larger scheme of *predictive policing* in India. A recent empirical study, conducted by two Indian researchers on such practices in Delhi, reiterated the aforementioned risks that have regularly featured in Western literature.[10] Problems of bias, arbitrariness, opacity, and discrimination are hard-coded into the law enforcement officials' unbridled use of such technologies.[11]

In this background, this paper seeks to serve as a primer on the use of AFRT by law enforcement officials. It will initiate readers into some key discussions on the risks posed by AFRT and some proposals for their regulation (within the Indian context) through a doctrinal analysis of existing scholarship. It is pertinent to acknowledge how vast each theme touched upon in this paper is, encompassing an expanding and nuanced discourse. However, by aiming to be adequately referenced, this paper should provide a layperson with enough sources to garner a more meticulous understanding of these numerous debates.

---

6 ibid. See also Andy Adler and Michael E. Schuckers, 'Comparing Human and Automatic Face Recognition Performance' (2007) 37(5) *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)* 1248 <> accessed 20 May 2020.

7 Mann and Smith (n 6); Rigano (n 5).

8 Joy Buolamwini and Timnit Gebru, 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification' (2018) 81 Proceedings of Machine Learning Research <> accessed 30 April 2020. See also Larry Hardesty, 'Study finds Gender and Skin-type Bias in Commercial Artificial-Intelligence Systems' (*MIT News Office*, 11 February 2018) <> accessed 30 April 2020; Arindrajit Basu and Siddharth Sonkar, 'Automated Facial Recognition Systems and the Mosaic Theory of Privacy: The Way Forward' (*The Centre for Internet and Society*, 2 February 2020) <https://cis-india.org/internet-governance/automated-facial-recognition-systems-and-the-mosaic-theory-of-privacy-the-way-forward> accessed 20 May 2020.

9 Smriti Parsheera, 'Adoption and Regulation of Facial Recognition Technologies in India: Why and Why Not?' (2019) Data Governance Network Working Paper 5 <tps://papers.ssrn.com/sol3/papers.cfm?abstract_id=3525324> accessed 2 August 2020. See also Vasudevan Sridharan, 'India Setting up World's Biggest Facial Recognition System' (*Deutsche Welle*, 7 November 2019) <-up-worlds-biggest-facial-recognition-system/a-51147243> accessed 20 April 2020.

10 Vidushi Marda and Shivangi Narayan, 'Data in New Delhi's Predictive Policing System' (2020) Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency 317 <DOI:10.1145/3351095.3372865>.

11 ibid 321-323.

The author will first delve into some of the controversial risks associated with AFRT, analysing them through the lens of Article 21 and the principle of *due process* under the Indian Constitution. The paper will then identify some of the regulatory solutions that are currently part of the discourse on minimising risks of AFRT and balancing their use with constitutional values, and fundamental and human rights. In particular, this discourse will examine an arguable temporary moratorium on AFRT, or alternatively, imposing statutory limitations on their prevalent use. For this, the paper will delve deeper into the governance and regulatory frameworks being deliberated and designed in the United States ('US') and the European Union ('EU'), which are two jurisdictions putatively leading this discourse. The final segment of this paper will propose a way-forward strategy for India, drawing from the international discourse.

II. AFRT and the Perils of Intelligent Surveillance – A Discursive Overview

While surveillance and intelligence gathering has been an inherent part of law enforcement, it has always required checks and balances in modern democracies, to fulfill the promise of individual freedoms and liberties unimpededly. Maintaining this balance has always been precarious – as states resort to increasingly sophisticated, surreptitious and technologically-enhanced methods for conducting surveillance, the law has largely played the unfortunate role of catching up with these trends of modernization.[12] AFRTs are perhaps the most discreet and arguably dangerous of these technologies. They present a high risk, high reward scenario (i.e. large-scale, cost-efficient surveillance *vis-à-vis* furthering the growth of a 'police state'), which as research and experience shows, has many takers in the conventional law enforcement establishments.

The main threats of AFRT's growing usage by the police and state apparatuses are three-fold. *First*, there are legitimate concerns about the accuracy of such tools, which *inter alia* demonstrate biases against certain vulnerable populations (including racial minorities and women).[13] *Second*, despite these evident inaccuracies, the fact that these tools are becoming an integral part of law enforcement, resulting in the potential indictment and incarceration

---

[12] Christopher S. Milligan, 'Facial Recognition Technology, Video Surveillance, and Privacy' (1999) 9 Southern California Interdisciplinary Law Journal 295, 297-298.

[13] Buolamwini and Gebru (n 9).

of an individual, raises concerns about violation of due process.[14] To make matters worse, there is a significant *automation bias* which is at play in the deployment of such technologies.[15] Automation bias creates a false 'trust' in algorithmic decision-making tools and processes. It stems from the lay-person notion that machine learning and sophistication of algorithms will always improve the quality of human decision-making, eventually resulting in a blind and uncritical favouring of any algorithmic decisions.[16] *Third*, in the absence of a robust data protection and privacy guaranteeing legal framework, AFRT-driven surveillance risks undermining civil liberties, and instead imposing the trappings of a 'police state' which is antithetical to the tenets of constitutional democracies. As aforementioned, this paper aims to delve deeper into how an unregulated, unbridled adoption of AFRT by law enforcement agencies in India can vitiate due process. Hence, the author will be limiting the discussion to the first two issues, as the implications of AFRTs on civil liberties are not germane to that discussion.

A. Questionable Accuracy and the Threat of Criminal Sanction

The accuracy of AFRT has been the central contention in most discourses. One of the seminal instances for this debate was when a group of researchers from MIT and Stanford University undertook a pioneering exercise to evaluate Amazon's *facial recognition tool* called Rekognition.[17] This research paper demonstrated how facial recognition algorithms, despite their inherent design sophistication, were still significantly inaccurate in their results. The problem was compounded by the fact that the error rate was significantly higher when women with a darker skin-tone were the subject of *facial profiling*.[18] Furthermore, since this technology was being deployed by law enforcement agencies in different states in the US, the conversation adopted a strong undertone of racial inequality and the vulnerability of African-Americans

[14] Abhinav Chandrachud, 'Due Process' in Sujit Choudhry, Madhav Khosla and Pratap Bhanu Mehta (eds), *The Oxford Handbook of the Indian Constitution* (OUP 2010).

[15] Mary Cummings, 'Automation Bias in Intelligent Time Critical Decision Support Systems' (2004) Collection of Technical Papers - AIAA 1st Intelligent Systems Technical Conference 2 <DOI: 10.2514/6.2004-6313>.

[16] ibid. See also Solon Barocas, Moritz Hardt and Arvind Narayanan, *Fairness in Machine Learning: Limitations and Opportunities* (2020) <s://fairmlbook.org/> accessed 2 August 2020 (Incomplete working draft).

[17] Buolamwini and Gebru (n 9).

[18] The research showed that Amazon's Rekognition tool was misidentifying darker-skinned women as men 31% of the times; lighter-skinned women were incorrectly identified 7% of the times, and darker-skinned men had an error rate of 1%. See Hardesty (n 9).

particularly from the use of such technologies.[19] Similar problems have also featured in other countries. For instance, there have been a rising number of protests against the London Metropolitan Police's use of AFRT.[20] In fact, this tool too has been criticised of severe inaccuracies in its results, in some cases, "*getting it wrong 81% of the time*".[21]

These results clearly puncture some erroneous notions lying at the heart of inducting AFRT and similar modern tech interventions into the criminal justice system. The first assumption is that such technologies will bolster human efficacy in monitoring and surveillance, to preemptively detect criminals and improve the overall law and security situation within a community.[22] The second assumption is about the speed and accuracy with which such technology conducts such crime detection, justifying its rapidly burgeoning adoption across the world.[23] However, given the high rate of errors in identifying individuals, the use of these machines poses serious risks and undermines their viability. It is pertinent here to reference how even the most impressive accuracy numbers in AFRT have usually been registered close to 70 to 80%.[24] In purely numerical values, this would translate into misidentifying two lakh to three lakh people for every one million people, even with the most accurate AFRTs. The implications of such large discrepancies are far-reaching, which are discussed hereinafter.

Despite its inaccuracies, AFRT is being used ubiquitously by law enforcement officials across the globe.[25] In India too, numerous state police forces have already started using different types of AFRT within their surveillance and monitoring functions.[26] This means that AFRT can become a decisive

---

[19] Natasha Singer, 'Amazon is Pushing Facial Recognition Technology that a Study says could be Biased' *(The New York Times*, 24 January 2019) <ps://www.nytimes.com/2019/01/24/technology/amazon-facial-technology-study.html> accessed 24 April 2020.

[20] Adam Satariano, 'Police Use of Facial Recognition is Accepted by British Court' (*The New York Times*, 4 September 2019) <https://www.nytimes.com/2019/09/04/business/facial-recognition-uk-court.html> accessed 20 May 2020.

[21] Charlotte Jee, 'London Police's Face Recognition System Gets it Wrong 81% of the Time' (*MIT Technology Review*, 4 July 2019) <296/london-polices-face-recognition-system-gets-it-wrong-81-of-the-time/> accessed 2 August 2020. See also Vikram Dodd, 'Met Police to Begin Using Live Facial Recognition Cameras in London' (*The Guardian*, 24 January 2020) <an.com/technology/2020/jan/24/met-police-begin-using-live-facial-recognition-cameras> accessed 2 August 2020.

[22] Rigano (n 5).

[23] ibid.

[24] Singer (n 20); Hardesty (n 9).

[25] Pamela Bump, 'Facial Recognition in Law Enforcement – 6 Current Applications' (*Emerj*, 2018) <> accessed 2 June 2020.

[26] These include the police forces of Delhi, Punjab, Andhra Pradesh, Tamil Nadu, and Gujarat, deploying these tools in different cities. See Anand Murali, 'The Big Eye: The Tech is all Ready for Mass Surveillance in India' (*Factor Daily*, 2018) <> accessed 24 July2020.

variable to determine an individual's guilt in a particular situation, resulting in her criminal prosecution and in some cases, arguably endangering such individual's liberty. This threat becomes particularly dangerous and could arguably add a new menace to the larger problem of malicious prosecution, which is well documented in Indian scholarship and jurisprudence.[27]

B. Is Due Process Vitiated?

While the language of Article 21 in the Indian Constitution uses the phrase "*process established by law*", this has been read as inclusive of both *procedural* and *substantive* due process elements, in numerous judgments.[28] Procedural due process mandates the deprivation of *individual life or liberty* only through "*fair, just and reasonable*" legal procedures.[29] It serves as judicial oversight on legislative or executive overreach in implementing arbitrary procedures, even if such procedures are provided through a legislation mandate. On the other hand, substantive due process evaluates even substantive provisions of the law, ensuring that any procedures do not vitiate the substantial legal and constitutional rights guaranteed to the citizens (and non-citizens in some cases).

Axiomatic to the Supreme Court's reading of *procedural* due process is the need for legal processes to prevent arbitrariness and abuse of power. Therefore, under Article 21, no process of law may arbitrarily result in the forfeiture of individual life or liberty. The present unregulated use of AFRT seemingly vitiates this very standard. As Marda and Narayan argue in their seminal empirical study of Delhi's predictive policing system, *arbitrariness* is being hard-coded into these frameworks.[30] This is visible in the inexplicable manner in which datasets for training machine learning tools (including AFRTs) are collated. Furthermore, the entire process operates in blatant opacity on how AFRTs are being deployed, devoid of any public scrutiny of such drastic interventions, and finding considerable exemptions even under the Right to Information Act.[31]

These patently questionable processes in the deployment of AFRTs specifically, and predictive policing in general, indicate our failure in recapitulating our lessons from the past. Indian law enforcement's experiments with modernisation in collection of evidence have a checkered history. The most

---

[27] N.C. Asthana, 'Malicious Prosecution: A Deep Dive into Abuse of Power by Police' (*The Wire*, 2020) <> accessed 30 August 2020.
[28] Chandrachud (n 15).
[29] *Maneka Gandhi v Union of India* (1978) 1 SCC 248.
[30] Marda and Narayan (n 11) 322-323.
[31] ibid. 323.

notorious of these instances was the growing dependence on *narco-analysis* which was used to place an accused into drug-induced stupor to answer questions, akin to a lie-detector test. Narco-testing was initially legitimized, after several judgments accepted its evidentiary value. However, there were numerous contentions raised against it, ranging from violation of the fundamental right against self-incrimination,[32] to how the statements induced through these tests were often unreliable and fictional.[33] These techniques were also considered involuntary, with a dangerous potential of police targeting innocents to expedite investigations, rather than resorting to more conventional but legal methods of interrogation. After numerous challenges, it was in the landmark decision of *Selvi* v. *State of Karnataka*[34] that the apex court held narco-tests and other involuntary mechanisms like brain-mapping techniques and polygraphs to be unconstitutional, unless the accused consented to them.

The problem with the use of AFRT overlaps in some ways with the challenges we confronted with narco-analysis. Like the latter, AFRT is presently unregulated and left to the absolute discretion of states and police forces to deploy them. These are institutions that have an inherent conflict of interest in overlooking (or bending) *due process* norms, to hasten investigative procedures. This bias is precisely the reason why the Constitution places careful checks and balances on the power of the Executive. Add to this the complete secrecy in which these tools are being designed and deployed, which fuels the apprehension of use of excessive force by law enforcement officials.

At present, in the conspicuous vacuum of any governing legislation, regulation, guidelines, or policy statement identifying the circumstances wherein AFRT can deployed, it is being used ubiquitously and arbitrarily. Such an unchecked system, allowing the police to undertake large-scale surveillance of innocent civilians and potential criminals alike, seems to be an overkill for maintaining law and order. Therefore, a warranted question occurs on how the use of AFRT can be regulated to ensure minimal risks and maximise its benefits.

---

[32] Constitution of India, art 20(3).
[33] *Selvi v State of Karnataka* (2010) 7 SCC 263 : AIR 2010 SC 1974.
[34] ibid.

III. Governance of AFRT – Statutory Regulation Versus Usage Moratorium

A growing debate on risk mitigation regarding the use of AFRT has featured prominently in two regions – the US[35] and the EU[36]. While the US has taken a more formal statutory route of regulation and governance of AFRT, the EU published its White Paper on AI, earlier this year, wherein it contemplated a wide-ranging deliberation to determine specific cases where AFRT could be utilized, without undermining human and fundamental rights of the citizens of EU member states.[37]

A. The Regulation of Facial Recognition Tools in the US

The US appears to have a relatively better regulatory framework in place to monitor the use of AFRT by law enforcement agencies. This comprises proposed legislation,[38] government oversight bodies,[39] and independent civil rights groups[40] working as the three pedestals upholding this oversight ecosystem.

As previously highlighted, the potential risks in use of AFRT by law enforcement agencies became a contentious issue after the uncovering of the high error rates in identifying people of colour, especially darker-skinned women, by Amazon's *Rekognition* tool.[41] In fact, there are further concerns

---

[35] Senator Roy Blunt (Chairman Senate RPC), 'Facial Recognition: Potential and Risk' (*Policy Papers Senate RPC*, 2019) <> accessed 28 August 2020.

[36] European Commission, *On Artificial Intelligence – A European Approach to Excellence and Trust* (White Paper, 2020) <ttps://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf> accessed 30 April 2020.

[37] ibid. See also Elena S. Nicolás, 'EU Backtracks on Plans to Ban Facial Recognition' (*EU Observer*, 2020) <euobserver.com/science/147500> accessed 30 April 2020.

[38] Khari Johnson, 'US Senators Propose Facial Recognition Moratorium for Federal Government' (*The Machine*, 12 February 2020) <ecognition-moratorium-for-federal-government/> accessed 24 June 2020.

[39] US Government Accountability Office, *Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy* (Report to the Ranking Member Subcommittee on Privacy, Technology, and the Law, Committee on the Judiciary, US Senate, 2016) <> accessed 24 June 2020. See also US Government Accountability Office, 'Face Recognition Technology: DOJ and FBI have Taken some Actions in Response to GAO Recommendations to Ensure Privacy and Accuracy, but Additional Work Remains' (Testimony before the Committee on Oversight and Reform, House of Representatives 2019) <> accessed 24 June 2020.

[40] See e.g., *Carpenter v United States* 198 L Ed 2d 657 : 137 S Ct 2211 : 582 US ___ (2017); *City of Los Angeles v Naranjibhai Patel* 2015 SCC OnLine US SC 7 : 192 L Ed 2d 435 : 135 S Ct 2443 : 576 US ____(2015), *Riley v California* 2014 SCC OnLine US SC 71 : 180 L Ed 2d 285 : 573 US ___ (2014); *United States v Davis* 785 F 3d 498 (11th Cir 2015).

[41] Brief filed on behalf of the ACLU, *Willie Allen Lynch v State of Florida* Florida SC, No SC2019-0298 <https://www.aclu.org/lynch-v-state-amici-brief> accessed 24 June 2020.

about how the use of AFRT in the criminal justice system can further target different segments of the population, who are already arguably unjustly victimized through unfair arrests and police harassment.[42] In this background, two bills were tabled in the last year alone (i.e. 2019) to regulate the use of AFRT in law enforcement processes. The *Facial Recognition Technology Warrant Bill, 2019* ('FRT Bill') was tabled in the US Congress to provide judicial oversight.[43] This Bill mandates and establishes the procedure for securing a warrant to undertake surveillance by deploying AFRT.[44] Furthermore, the FRT Bill also includes a termination clause, ending any ongoing surveillance through AFRT if the petition for a warrant is denied, and imposes a limitation of thirty days on the duration of the surveillance (subject to extension).[45] With respect to reporting and oversight, there are detailed provisions setting out the requirement of governmental disclosures of the use of AFRT by federal agencies, which are to be tabled before the Judiciary Committees of the US Congress, thus, granting legislators the authority to audit and curtail the abuse of AFRT.[46] In quick succession to the FRT Bill, two Democratic legislators also introduced the *Ethical Use of Facial Recognition Bill, 2019* ('EFR Bill'). In contrast to the FRT Bill, this one proposes a complete moratorium on the use of AFRT, until adequate guidelines and regulations are put in place for its governance.[47]

While these legislative efforts are one part of the proposed regulation of AFRT, established government agencies within the US have already expanded their scope of jurisdiction to also monitor the use of AFRT. For instance, the US Government Accountability Office published two reports on how the use of AFRT by the Federal Bureau of Investigation ('FBI') was not concomitant to existing privacy laws and policies, and also questioned the accuracy of this technology.[48]

Lastly, through a gradually rising number of cases, civil rights groups are becoming more involved in independently taking stock of the actual and potential abuse of AFRT in the criminal justice system. Numerous *amici* briefs have been filed by renowned groups like the American Civil Liberties Union ('ACLU'), and even university research centres like Georgetown Law's Centre on Privacy & Technology.[49] These briefs have helped in the evolution

---

[42] Ethical Use of Facial Recognition Act (Bill), § 2.
[43] Facial Recognition Technology Warrant Act (Bill) 2019.
[44] ibid § 3 "Limitations on use of facial recognition technology".
[45] ibid.
[46] ibid., § 4 "Reports on government use of facial recognition technology".
[47] Ethical Use of Facial Recognition Act (Bill), perambulatory text.
[48] US Government Accountability Office (n 40).
[49] Brief filed on behalf of the ACLU (n 42).

of useful jurisprudence to the dangers of AFRT biases and how the same can have real-life ramifications for individuals subjected to them.[50]

The result of this trinitarian set up is the formation of a large ecosystem where decisions regarding the development, deployment, and scaling of AFRT are not limited to a privileged few (as aforementioned in the context of the '*Frightful Five*'). The regulation in such an ecosystem tends to be more bottom-up, instead of the reverse. It is by no means a foolproof set up for regulation, but unquestionably more inclusive and holistic, allowing room for a robust discourse to feed into the policy and law-making processes.

B. Ethically Compliant AI – The EU's Governance Framework for AFRT

The debate on regulation of AI in general, and more focused conversations on AFRT's usage, within the EU, have occurred more recently since the adoption of the *General Data Protection Regulation, 2016* ('GDPR').[51] In this background, the EU has vociferously favoured the idea of ethically-designed AI, resulting in the drafting and adoption of the *European Ethical Charter on the Use of AI in Judicial Systems and their Environment* in December 2018.[52]As per the European Commission for the Efficiency of Justice ('CEPEJ'), the body responsible for drafting this Charter, the EU member states will focus on harnessing the transformative potential of emerging technologies like AI to improve judicial efficiency but in a responsible manner.[53] This would entail compliance with the fundamental rights guaranteed by the European Convention on Human Rights and the GDPR.

Following from this Charter, the EU recently put out its white paper on AI.[54] A draft of this white paper, previously leaked, revealed that the EU was contemplating a three to five year moratorium on the use of AFRT.[55] However, the final text has revealed a less radical approach – instead of

---

[50] ibid 9-11.

[51] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1 <europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679> accessed 24 June 2020.

[52] Council of Europe, '*European Ethical Charter on the Use of AI in Judicial Systems and their Environment*' (*European Commission for Efficiency of Justice* (*CEPEJ*) 2018) <https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c> accessed 20 May 2020.

[53] ibid.

[54] European Commission (n 37).

[55] Elena S. Nicolás, 'EU Keen to set Global Rules on Artificial Intelligence' (*EU Observer*, 21 January 2020) <https://euobserver.com/science/147198> accessed 2 August 2020.

banning its use, the EU will undertake large-scale stakeholder consultations to draft a set of rules and regulations regarding risks, safe use and regulations, and liability for AI fallouts.[56]

It becomes evident from this set of documents that while well-intentioned, the EU is currently straggling behind in developing a regulatory framework for AI in comparison to the US. This could also be attributed to the more rapid advancements that the latter has made in designing and deploying AI-driven technologies (including AFRT), thus, necessitating an urgent formulation of a robust regulatory framework. However, the *prima facie* advantage of the EU model is the stakeholder engagement and debate it is encouraging, making the whole process more democratic. Additionally, given its aforementioned Ethical Charter, the EU is seemingly increasingly committed to establishing the balance necessary for minimising risks and maximising benefits from the use of technologies like AFRT. How effectively it manages to translate its ambitious intent into actuality, and what will be the actual implementation gap between proposed policies and end products, are questions that can currently only be speculated at best.[57]

IV. AFRT in Indian Law Enforcement: Regulatory and Governance Lessons

The deployment of AFRT in India is no longer a theory – multiple state governments[58] and the National Crime Records Bureau ('NCRB') are at different stages of deploying such technologies.[59] In a country like India, with tremendous diversity in physical facial features,[60] and a massive population of 1.3 billion people, the idea of unbridled power of state surveillance is laden with risks. Additionally, the absence of a robust data protection law governing the collection of biometric information, and strict procedural law(s) establishing clarity of circumstances wherein AFRT can be deployed for monitoring and collection of evidence, makes the situation worse.

---

[56] Nicolás, 'EU Backtracks on Plans to Ban Facial Recognition' (n38).

[57] It is pertinent to mention here that there have been numerous criticisms of the EU's lack of concrete steps on regulating AI, particularly its failure to impose 'standards' which are arguably crucial for establishing a safe and ethical AI regime. The EU's promise for regulation is, therefore, not an end in itself; the promise must be effectively fulfilled to ensure trust and confidence in its governance of AI.

[58] Murali (n 27).

[59] Parsheera (n 10).

[60] ibid., 33.

Given the NCRB's proposal to establish the *National Automated Face Recognition System* as a nationwide AFRT platform,[61] it is imperative to press for adequate regulatory measures with great expediency. The discussion from the previous section demonstrates a two-pronged approach to regulation of AFRT. *First*, is a strong legislative framework which will provide a definitive and limited use of such technology; however, in the interregnum, a moratorium on AFRT usage is also propped as a solution. *Secondly*, in the absence of a strong legislative framework, it is left to the courts to enforce the balance between security necessities, and individual liberties and civil rights.

Drawing from these jurisdictions, such measures must address the following key areas.

A. Transparency and Accountability

A key concern surrounding the rampant and discretionary use of AFRT in law enforcement has been about how such actions are nebulously justified for security purposes. For instance, in India, the NCRB's aforementioned proposal for constructing a nationwide facial recognition tool has been shrouded in darkness. There are little to no publicly available details about how such decisions have been arrived upon, or what kind of ministerial processes have been followed to this end. Furthermore, there is also ambiguity about which datasets will be harnessed to train these technologies, and whether their usage will be subject to any independent technical and design audits, as well as impact evaluation exercises. All these elements are vital in building the confidence of the citizenry that will ultimately bear the brunt of these technological interventions. In the absence of such confidence building measures, numerous civil society activists and legal academics have criticised the seeming arbitrariness and haste in deploying AFRT in India.[62] It is necessary to put all relevant details about AFRT in the public domain. While the Right to Information Act, 2005 warrants such information to be readily accessible to any citizen, the clandestine manner in which these technologies are being adopted, leave little room for debate regarding the intent of the policymakers, or the machiavellian uses for AFRT. It is, therefore, imperative for the legislatures to enact laws to enforce transparency and accountability around the use of AFRT in law enforcement in their respective jurisdictions.

---

[61] NCRB, 'Request for Proposal to Procure National Automated Facial Recognition System (AFRS)' (National Crime Records Bureau and Ministry for Home Affairs, Government of India) <> accessed 24 July 2020.

[62] Parsheera (n 10) (and more papers cross cited in it).

B. Proportionality in Adoption and Usage

Both the EU and the US have been debating measures to limit the use for AFRT. Most recently, the city of San Francisco effectuated an ordinance wherein the city's departments must specify 'necessary circumstances' warranting the procurement and use of AFRT .[63] In India, the Supreme Court's *proportionality* test laid down in the *Puttaswamy* judgment[64] governs state interventions which may result in vitiation or violation of an individual's right to privacy. As per this test, such interventions must be established by law, in pursuit of a state interest, and must also prescribe checks and balances to prevent abuse of the state's surveillance powers. However, the current use of AFRT is arguably bereft of at least two of these yardsticks. This must be rectified through a prospective regulatory and statutory framework governing and limiting its use to necessary instances.

C. Stakeholder Engagement

It is also imperative to conduct large-scale engagements with numerous civil society activists, privacy advocates, academics, and members of the legal fraternity, to get a fair sense of the legal, constitutional, and regulatory challenges associated with AFRT. Presently, the deployment of these tools by state police forces, and the proposed all India facial recognition grid have inspired little or no confidence, sparking massive doubts around their actual end use (in furthering a surveillance state), given how these have been top-down decisions. A constitutional democracy like India is established on the idea of bottom-up building of policy interventions. *Suo motu* prescriptions like the AFRT are antithetical to the ideas of a participatory democracy.[65] In this background, any proposed legislation(s) must adhere to the tenets of participatory democracy, empowering and actively engaging its citizenry in the lawmaking and policy making processes.[66]

---

[63] Acquisition of Surveillance Technology, Ordinance No 190110. See also Kieren McCarthy, 'San Francisco Votes No to Facial-recognition Tech for Cops, Govt– while its Denizens Create it' (*The Register*, 14 May 2019) <https://www.theregister.com/2019/05/14/san_francisco_facial_recognition_ban/> accessed 2 August 2020.

[64] *K.S. Puttaswamy v Union of India* (2017) 10 SCC 1.

[65] For a larger discourse on how authoritarian states adopt sophisticated state surveillance methods and technologies, see Hannah Arendt, *The Origins of Totalitarianism* (Meridian Books 1958).

[66] Sherry R. Arnstein, 'A Ladder of Citizen Participation' (1969) 35(4) *Journal of the American Planning Association* 216.

V. Concluding Remarks

The deployment of AI in general, and AFRT specifically, seems to be already in motion in India. What is disconcerting is the hastiness with which these interventions are being scaled across states, disregarding constitutional morality and the fundamental tenets of procedural fairness. All this is being advocated on the tenuous premise of greater efficiency which flounders when one reviews the concerns regarding inaccuracies of AFRT across jurisdictions. Even if one was to assume the effectiveness, such radical and disruptive technologies cannot and should not be utilised in an unregulated and arbitrary manner. It is the need of the hour to accept these risks and find solutions to them – if not, like the popular adage, Indian law enforcement, and the criminal justice system, are doomed to repeat some of their ill-fated history.

Conceptualizing an International Framework for Active Private Cyber Defence[1]

Arindrajit Basu[2] *and Elonnai Hickok*[3]

I. Introduction and Scope

The ubiquity of Information Communication Technologies ('ICTs') in the modern day has increased the dependence of individuals, governments and institutions on cyberspace for the discharge of economic, social and political functions. At the same time, the vulnerabilities in information infrastructure have led to its misuse for malicious cyber activity across traditional territorial borders, culminating in economic, national security or political damage - proving it to be a space that is difficult to regulate and govern. This has challenged prevailing conceptions of municipal law, which seeks to govern its own territorial boundaries, and international law, which has been driven by the understanding that sovereign states have been successful in organizing

---

[1] A previous version of this paper was presented at a conference organised by The Hague Program for Cyber Norms, Leiden University in 2018. Subsequently, parts of this paper were used for submissions the Global Commission on the Stability of Cyberspace (GCSC) in 2019 by the Centre for Internet & Society. The full text of CIS's intervention can be found here. <https://cis-india.org/internet-governance/files/gcsc-response>.

[2] Research Manager, Centre for Internet & Society, India.

[3] Chief Operating Officer, Centre for Internet & Society, India.

domestic society and structuring external affairs.[4] Malicious cyber activity by rogue states and actors, regardless of jurisdiction, calls into question the very ability of a state to protect its sovereign interests including those of its citizens and industry. Recent attacks on the private sector coupled with the inability of governments to comprehensively respond has propelled discourse on the extent to which private sector organisations should be involved in this space. This includes the existence and limits of the right and corresponding responsibility that private sector organisations have to protect themselves, their customers, and a nation in cyberspace.[5]

Deployment of cyber defence by the private sector in cyberspace has largely involved passive deflection measures, such as building up robust cyber defence networks and incorporating greater resilience into their organizational cybersecurity strategy.[6] The private sector has traditionally provided similar products and services to governments as well. The increasing complexity and frequency of attacks has led to a deteriorating state of cybersecurity at organization and national levels.[7] Foiling an offensive operation that is already underway becomes particularly difficult if the target network has already been penetrated before detection of the attack.[8] Governments have started responding to this challenge by developing and deploying offensive cyber operations and active cyber defence.[9] Yet, state enabled Active Cyber

---

4 Hendrik Spruyt, *The Sovereign State and its Competitors: An Analysis of Systems Change* (Princeton University Press 1994).

5 Jan E. Messerschmidt, 'Hackback: Permitting Retaliatory Hacking by Non-State Actors as Proportionate Countermeasures to Transboundary Cyberharm' (2013) 52(1) Columbia Journal of Transnational Law <http://jtl.columbia.edu/wp-content/uploads/sites/4/2014/05/MesserschmidtNoteHackback.pdf> accessed November 2, 2018; Carnegie Live,, 'The Private Sector and Active Cyber Defence and Closing Remarks'(*YouTube* April 18 2017) <https://www.youtube.com/watch?v=TYW237udDx0> accessed November 2 2018.>.; Beatrice Walton, 'Duties Owed: Low-Intensity Cyber Attacks and Liability for Transboundary Torts in International Law' (2017) 126(5) Yale Law Journal <https://www.yalelawjournal.org/note/duties-owed-low-intensity-cyber-attacks-and-liability-for-transboundary-torts-in-international-law> accessed November 2, 2018.

6 Robert Anderson, Brian Lum, and Bhavjit Walha, Offense vs. Defence (December 11, 2005) <https://courses.cs.washington.edu/courses/csep590/05au/whitepaper_turnin/OffenseVsDefence.pdf>.

7 Lotte Schou-Zibell & Nigel Phair, 'Cyber-Insecurity: The Dark Side of Digital Financial Services' (*Newsroom*, 1 August 2018) <https://newsroom.unsw.edu.au/news/science-tech/cyber-insecurity-dark-side-digital-financial-services>.

8 Anderson, Lum, and Walha (n 6).

9 GIP Digital Watch Observatory for Internet Governance and Digital Policy, *UN GGE and OEWG* <https://dig.watch/processes/ungge> accessed November 2, 2018. (Indeed, a map created by the Diplo Foundation identifies 23 countries with state enabled offensive cyber capabilities and 8 countries indicating a move to adopting such measures)

Defence[10] ('ACD') only addresses this challenge from the perspective of individual states.[11]

Indeed, this challenge has propelled private actors to increasingly look beyond government-driven security mechanisms and resort to aggressive measures to protect themselves, either by developing their own cyber capabilities or by hiring third party cyber security companies. At the same time, governments are increasingly looking to the private sector to not only provide security products but also to actively utilize their resources in addressing threats to national cyber space. This paradigm has led to discussions that expand ACD measures to the private sector as a means to further enhance national cyber security and enable companies to protect their own infrastructure. For the purposes of this paper, Active Private Cyber Defence ('APCD') refers to any active defence measure taken by the private sector.

It is interesting to note that these private sector mechanisms are emerging despite existing legislation outlawing use of active defence by individuals and non-state entities. Thus, a key window exists for policy-makers in the possibility of establishing a framework for existing APCD practices that would enable optimal utilisation of private sector capabilities for securing cyberspace at an organizational and national level. This must happen in consonance with circumscribing their operations within the boundaries of the rule of law, both in terms of domestic legislation and international law.

Conceptualizing such a framework is in many ways shaped by national, international, and geo-political dynamics and challenged by the evolving nature of technology. This paper seeks to unpack the complexities that underscore each of these challenges and identify avenues towards resolving some of them.

The paper is divided into four sections. The first section reviews the spectrum of active private defence and demarcates the various kinds of offensive and defensive capabilities that would fit along various rungs in this spectrum. It also maps existing policy initiatives enabling APCD from key jurisdictions. The second section outlines relevant standards of international law and analyzes the extent to which they might help circumscribe the legal

---

[10] For the purposes of this paper, Active Cyber Defence ('ACD') refers to any cyber operation that has an impact in the adversary's network and extends beyond mere passive resilience.

[11] Nelson, Steven, and Marina Hutchinson, 'Active Cyber Defence' or Vigilantism?' *Washington Examiner* (February 8, 2018) <https://www.washingtonexaminer.com/active-cyber-defence-or-vigilantism> accessed November 2, 2018. As noted by Rep. Tom Graves when explaining the proposed APCD Bill in the US, "The status quo is unacceptable, and people are yearning for a solution. Even just minor steps like we're trying to provide here".

limits of APCD and resolve any geopolitical tensions that might arise. The final section projects the potential ramifications of APCD and articulates the drivers that could determine how a robust norm on active cyber defence might shape responsible behaviour in cyberspace by both state and non-state actors alike. The paper concludes with a set of points and questions with the aim of articulating a baseline from which municipal legislators and global policy-makers can take this debate forward.

This paper restricts itself to evaluating the response to low-intensity cyber-attacks: attacks that are below the threshold of 'use of force' i.e., those cyber-attacks that cause physical damage to life or property akin to a traditional kinetic (non-cyber) attack. We have limited the scope for two reasons. First, most of the cyber-attacks presently faced by the private sector do not amount to the 'use of force' as laid out in Article 2(4) of the United Nations Charter. A Hackmageddon report suggests that in 2016 and 2017 only 3.4% and 4.3% of cyber-attacks were conducted with the underlying motivation of causing physical damage akin to the use of force.[12] The attacks are also largely aimed at accomplishing thefts of intellectual property, distributed denial of service attacks and ransomware Second, the perceived monopoly states have over the right to 'use of force' has specific connotations from a global governance and international law perspective. This question deserves to be treated separately from low-intensity attacks and is therefore left for another paper.

II. Mapping the Landscape of Active Private Cyber DefencE

A. Identifying the spectrum

Operations undertaken for the purpose of cyber defence differ greatly from one operation to another. Therefore, these operations must be distinguished from one another and classified based on impact, intention of the attacker and reversibility of the attack.

As a starting point ,'active' and 'passive cyber defence' should be separated when discussing cyber defensive operations.[13] Activities whose impact

[12] Passeri, Paolo, '2017 Cyber Attacks Statistics' (*Hackmageddon*, 30 September 2018) <https://www.hackmageddon.com/2018/01/17/2017-cyber-attacks-statistics/> accessed November 2, 2018.

[13] Paul Rosenzweig, Steven P Bucci, and David Inserra, *Next Steps for U.S. Cybersecurity in the Trump Administration: Active Cyber Defence* (*The Heritage Foundation*, 5 May 2017) <https://www.heritage.org/sites/default/files/2017-05/BG3188.pdf>.

is only felt within the defendant's network may be termed passive cyber defence. These include measures like basic security controls, antivirus and patch management.[14]To qualify as active cyber defence, the operation must, at least partially impact external networks – networks which belong either to adversaries or are proxy networks utilised by adversaries.[15] Several scholars have attempted to classify both offensive and defensive cyber operations on a spectrum. Paul Rosenzweig has drafted a comprehensive spectrum of ACD measures based on the effects the measures could have on information infrastructure—including observation, access, disruption, and destruction.[16] The Centre for Homeland Security at George Washington University (CHSGWU) have created a spectrum of active cyber defence tactics, ranging from offensive to defensive, based on the intent of the actor implementing them.[17] For example, the use of tarp its, sandboxes and honey pots which are technical tools that prevent the hacker from entering a network's perimeter are on the defensive end of the spectrum.[18] On the other hand, the use of botnets or hackbacks[19] to infiltrate the adversary's networks and recover stolen information would fall within the offensive end of the ACD spectrum. Table 1 shows examples of measures at various rungs of the Active Cyber Defence Spectrum.

TABLE 1: SPECTRUM OF ACTIVE CYBER DEFENCE MEASURES

PASSIVE DEFENCE MEASURES (BUILDING RESILIENCE IN DEFENDANT'S NETWORK)	Basic security controls, firewalls, anti-virus, scanning and monitoring, security controls
ACTIVE CYBER DEFENCE (LOW IMPACT/LOW RISK)	Information sharing, tar pits, sandboxes, honeypots, Intelligence Gathering in dark web

[14] Active Defence Task Force, *Into the Gray Zone: The Private Sector and Active Defence Against Cyber Threats* (Centre for Homeland Security, George Washington University, October 2016) <https://cchs.gwu.edu/sites/g/files/zaxdzs2371/f/downloads/CCHS-ActiveDefenceReportFINAL.pdf>

[15] Wyatt Hoffman, Ariel Levite, 'Rethinking Corporate Activity Cyber Defence' (*Lawfare*, 17 July 2017) <https://www.lawfareblog.com/rethinking-corporate-active-cyber-defence>.

[16] Paul Rosenzweig, 'International Law and Private Actor Active Cyber Defensive Measures' (2014) 50(1) Stanford Journal of International Law 2.

[17] Active Defence Task Force (n 14).

[18] Joseph Menn, 'Hacked Companies Fight Back with Controversial Steps' *Reuters* (17 June 2012) <http://www.reuters.com/article/2012/06/17/us-media-techsummit-cyber-strikeback-idUSBRE85G07S20120617>.

[19] Hackbacks are the most offensive ACD measure and refers to operations intended to destroy the networks of adversaries without any form of authorization. See Farzaneh Badil, 'Legalizing Hackbacks' (*Internet Governance*, 4 May 2017) <https://www.internetgovernance.org/2017/05/04/legalizing-hackbacks/> accessed 02 November 2018.

ACTIVE CYBER DEFENCE (HIGH IMPACT/HIGH RISK)	Botnet take downs, 'hot pursuit' to recover assets
ACTIVE CYBER DEFENCE ('HACKBACK')	Operations intended to disrupt or destroy external networks without authorization

(*Source: Adapted from Into the Gray Zone)*

B. Configuring models of state-private actor relationships in the APCD context

Historically, governments used to engage with the private sector in two ways. First was by co-opting their capabilities within the framework of a national cyber-security ecosystem, and the second was by putting in place a law that prohibited individual entities from infiltrating external networks, thereby effectively banning APCD. While these two configurations remain the official status quo, APCD is increasingly being considered, as States are beginning to view the role of the private sector in the cybersecurity ecosystem differently.

In understanding the developments around ACD and APCD, their complexities, and finding a way forward, it is important to place APCD in the larger context of the relationship between governments and the private sector. Maurer has articulated three major models for government engagement with private actors in cyberspace.[20] The first model is *delegation* - where the government exercises clear oversight over their actions through screening and selection of actors, exercise of punitive sanction and a clear demarcation of potential effects. The second model is *orchestration*, where the government passively supports the private actor but does not establish clear oversight mechanisms.[21] Finally, *sanctioning* entails that the state does not acknowledge the actions taken by the private actors operating from their territory and effectively turns a blind eye.[22] We attempt to extend these models to the configurations we observed when mapping developments in the APCD space. We have also added two additional configurations that reflect the trends we observed in our research. Articulating these configurations and mapping the state of private-public partnerships is crucial for identifying the different kinds of challenges and opportunities within each configuration,

[20] Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power* (Cambridge University Press 2017) 29.
[21] ibid.
[22] ibid.

As a note, policy or use-cases in a country may fall within multiple configurations. For example, some countries sanction an underground market that allows for APCD despite having a law that bans it.[23] In the context of APCD, a private sector company may work with multiple governments, multiple companies, and across multiple jurisdictions - which poses an additional complexity which we address in Part IV of this paper.

C. "PRE"-APCD Configurations

Often private-public partnerships in cyber defence are confused with those engaging in active cyber defence. Further, private-public partnerships that are 'pre-APCD' configurations often start to engage in active cyber defence at some point. Thus, our mapping takes into account private-public partnerships that do not necessarily engage in active cyber defence.

i. Configuration 1: Co-optation

This configuration covers scenarios where private sector actors, security researchers and commercial cyber-security researchers work with law enforcement authorities, military, and other nodal agencies responsible for cyber security as part of a multi-stakeholder unit. Decisions are taken by the unit as a whole rather than by individual actors.

Various models of co-optation have been deployed by countries across the globe. The first model is a permanent unit that synchronizes the planning of cyberspace operations in collaboration with various stakeholders. The United States Cyber Command is an example of this.[24]It is one of the ten unified commands that come under the aegis of the United States Department of Defence.[25] Israel's cyber strategy also involves an ecosystem approach which includes both passive and active defence and offensive capabilities across military domains.[26] Singapore's Cyber Security Agency, which was set up in 2015 under the Prime Minister's Office (PMO) was set up to protect critical information infrastructure and " coordinate efforts across

---

[23] *See* example of cyber defence contractors in U.S. below.

[24] US Cyber Command, 'Achieve and Maintain Cyberspace Superiority' (*Cybercom.mil*, April 2018) <https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM Vision April 2018.pdf?ver=2018-06-14-152556-010> accessed 2 November 2018.

[25] US Cyber Command, 'Mission and Vision'(*Cybercom.mil*) <https://www.cybercom.mil/About/Mission-and-Vision/> accessed 2 November 2018.

[26] Michael Raska, 'Confronting Cybersecurity Challenges: Israel's Evolving Cyber Defence Strategy' (S. Rajaratnam School of International Studies, January 2015) <https://www.rsis.edu.sg/wp-content/uploads/2015/01/PR150108_-Israel_Evolving_Cyber_Strategy_WEB.pdf> accessed 2 November 2018.

government, industry, academia, businesses and the people sector, as well as internationally."[27]

Other instances of co-optation are voluntary cyber response units that deploy civilians working in the private sector on a voluntary basis. The Cyber Defence Unit[28] of the Estonian Defence League[29] is a case in point. The league was set up as a voluntary unit in 1918 and was re-established when Estonia broke away from the Soviet Union.[30] The voluntary nature of the force allows private actors to aid governmental authorities - Estonian State Information System Authority, who are responsible for coordinating the group's efforts.[31]

The cyber unit has two main functions.[32] The first is improving capacity across society, through regular trainings and cyber security exercises. The second is working as a cohesive unit when called upon to respond to specific cyber emergencies.[33]

The United States has taken some steps towards emulating the Estonian model. Lawmakers have put forward a bill that would create special units in the National Guard to respond to cyber-attacks.[34] The National Cyber Guard Civil Support Teams will work to co-ordinate state, federal and local level resources and assist the private sector with response and recovery.[35]

---

[27] Cyber Security Agency of Singapore, 'Singapore's Cybersecurity Strategy' (2016) <https://www.csa.gov.sg/~/media/csa/documents/publications/singaporecybersecuritystrategy.pdf> accessed 2 November 2018.

[28] Kaitseliit, 'Estonian Defence League's Cyber Unit' <http://www.kaitseliit.ee/en/cyber-unit> accessed 2 November 2018. "EDL CU objectives:
- development of cooperation among qualified volunteer IT specialists
- raising the level of cyber security for critical information infrastructure through the dissemination of knowledge and training
- creation of a network which facilitates public private partnership and enhances preparedness in operating during a crisis situation
- education and training in information security
- participation in international cyber security training events"

[29] Monica M. Ruiz, 'Is Estonia's Approach to Cyber Defence Feasible in the United States?'(*War on the Rocks*, 9 January 2018) <https://warontherocks.com/2018/01/estonias-approach-cyber-defence-feasible-united-states/> accessed 2 November 2018.

[30] ibid.

[31] ibid.

[32] Kaitseliit (n 28).

[33] CCDCOE, 'Locked Shields 2017'(21 April 2017) <https://ccdcoe.org/locked-shields-2017.html> accessed 2 November 2018. Former Estonian President Thomas Hendrik Ilves stated "we have lots of talented people who work in the private sector and we offered them the possibility of working once a week for a more patriotic cause."

[34] Cimpanu, Catalin, 'New US Bill Wants to Create National Guard Cyber Units' (*Bleeping Computer*, 22 May 2018) <https://www.bleepingcomputer.com/news/government/new-us-bill-wants-to-create-national-guard-cyber-units/> accessed 2 November 2018.

[35] Ruiz (n 29).

Like the Estonian model, individuals on the cyber force will be civilians with full-time jobs in the private sector who will work with the government when called upon.[36]

ii. Configuration 2: Banning

Country has a law banning ACD measures by private companies or individuals. These laws are largely worded in the form of a prohibition against infiltrating external computer networks due to the risks posed by allowing a private sector to undertake government functions, and accessing security devices and the challenges with fostering accountability in this regard. For example, the Computer Fraud and Abuse Act ('CFAA') in the United States criminalizes 'unauthorized access' to a computer and 'unauthorized transmission of malware' and damage of computer networks.[37]

D. Configurations Where APCD is Enabled

i. Configuration 3: Delegation

In this configuration, *a country enables, through law, the private sector to undertake specific ACD actions to achieve specific and defined goals*.

This configuration comes in various forms through which clear and specific responsibilities are assigned to a private sector actor within the strict confines of relevant law and policy. Singapore has recognized the role of the private sector in protecting national security for the protection of national information infrastructure, including by taking pre-emptive strikes against perceived cyber threats[38] on critical infrastructure.[39] After being subject to an inordinate number of breaches, Singapore amended its Computer Misuse Act (amended to the Computer Misuse and Cybersecurity Act - CMCA) to reflect this recognition.[40] The 2014 Amendment is a clear example of delegation as it creates a middle ground where it does not fully legalize APCD but enables state-sanctioned APCD for the protection of critical

---

[36] ibid.

[37] 18 USC § 1030.

[38] Amanda N. Craig, Scott J. Shackelford, and Janine S. Hiller, 'Proactive Cybersecurity: A Comparative Industry and Regulatory Analysis' (2015) 52(4) *American Business Law Journal* 721.

[39] Phneah, Ellyne, 'S'pore Beefs up Cybersecurity Law to Allow Preemptive Measures' *ZDNet* (14 January 2013) <http://www.zdnet.com/sg/spore-beefs-up-cybersecurity-law-to-allow-preemptive-measures-7000009757/>.

[40] ibid.

information infrastructure after the issuing of certificates to 'specified persons.'[41] Singapore's approach to engagement with the private sector offers a hybrid as a model of co-optation through the Cyber Security Agency that "coordinates nationwide efforts coordinate efforts across government, industry, academia, businesses and the people sector, as well as internationally"[42] combined with government-delegated Active Defence Measures by the private sector when needed.

In the USA, Representatives Tom Graves (U.S. Representative, Georgia - Republican), Kyrsten Sinema (U.S. Representative, Arizona – Democrat), have attempted to follow suit by introducing a bill, titled the Active Cyber Defence Certainty Act (ACDC), as per this configuration.[43] The new draft legislation provides an exception to liability under the Computer Fraud and Abuse Act ('CFAA'). This bill would allow victims to enter the networks of their adversaries for evidence gathering purposes to identify the attacker and gather evidence to prove who the attacker was.[44] It has been improved after taking into account certain legitimate concerns.[45]

ii. Configuration 4: Orchestration

A government may recognize or underscore the importance of APCD but not regulate it. Unlike in delegation, where permitted capabilities are clearly defined and framed, in this configuration a whole range of capabilities may

---

[41] Computer Misuse and Cybersecurity Act (Cap 50A, 2013 Rev Ed), s 15(A)(1); Cybersecurity Act (Amendment Bill) 2018, cl 23.

[42] Cyber Security Agency of Singapore (n 27).

[43] Active Cyber Defence Certainty Act 2017 (USA).

[44] Chris Cook, 'Hacking Back in Black: Legal and Policy Concerns with the Updated Active Cyber Defence Certainty Act' (*Just Security*, 20 November 2017) <https://www.justsecurity.org/47141/hacking-black-legal-policy-concerns-updated-active-cyber-defence-certainty-act/> accessed 2 November 2018.

[45] Tom Graves, Rep. Tom Graves Formally Introduces Active Cyber Defence Bill <https://tomgraves.house.gov/news/documentsingle.aspx?DocumentID=398840> accessed 2 November 2018.

"Key changes to the bill that were made to address the concerns include.

- A voluntary review process that individuals and companies can utilize before using active-defence techniques;
  - This provision allows defenders to benefit from review of their proposed active-defence measures by the FBI Joint Taskforce, which will assist defenders in conforming to federal law and improving the technical operation of the measure;
  - The authority to conduct these reviews would exist under a two-year pilot program, and could be amended or renewed at a later date.
- Requires notification to the government for the use of active-cyber defence measures that go beyond beaconing;
- Clarification that the bill does not interfere with a person's right to seek damages;
- Requires an annual report on the federal government's progress in deterring cybercrime.

The updated legislation also makes other minor and technical change"

be possible. *We have observed that such a configuration is often enabled through a range of mechanisms including commitments to cooperation in national cyber security frameworks and strategies, MOU's and contracts framing public private partnerships in the framing of strengthening national security.*

For example, recently some governmental policy stances have worked towards serving as enablers of APCD in the context of it strengthening national security. For example, in its National Cyber Security Strategy 2016–2021, the UK government has claimed that it "will draw on its capabilities and those of industry to develop and apply active cyber defence measures to significantly enhance the levels of cybersecurity across UK networks."[46] However, the UK government is yet to state clearly the role and freedoms given to private sector corporations in discharging this role.

Loosely worded policy documents that encourage the private sector to engage in 'proactive' cyber-security measures without charting out guidelines detailing how these measures are to be implemented or the limits on their use could also be considered *orchestration*. For example, India's 2013 Cyber Security Policy states "To encourage all organizations to develop information security policies duly integrated with their business plans and implement such policies as per international best practices. Such policies should include establishing standards and mechanisms for secure information flow (while in process, handling, storage & transit), crisis management plan, **proactive security posture** assessment and forensically enabled information infrastructure."[47]

Another example of orchestration might be governments working with cybersecurity companies without a clearly defined policy framework underscoring this co-operation. There are multiple instances of companies dismantling botnets with various degrees of collaboration with law enforcement officials. One such example is INTERPOL's collaboration with numerous cyber security companies to dismantle the Simda botnet that had infected 190 countries.[48]

---

[46] UK Government, National Cyber Security Strategy 2016–2021.

[47] Parliament of India, National Cyber Security Policy, 2013 (2013) <http://164.100.94.102/writereaddata/files/downloads/National_cyber_security_policy-2013(1).pdf> accessed 2 November 2018. This policy is set to be updated in 2020. The National Cybersecurity Co-ordinator has already sought responses to consultation from various stakeholders and is in the process of drafting a public version of this strategy. It is likely that this will serve as a complete overhaul of the 2013 cybersecurity policy.

[48] O'Brian and Dick, 'Simda Botnet Hit by Interpol Takedown'(*Symantec Security Response*, 13 April 2015) <https://www.symantec.com/connect/blogs/simda-botnet-hit-interpol-takedown> accessed 2 November 2018.

The orchestration configuration may be confused with the co-optation configuration in certain instances as both involve the government working with private actors. However, a key difference in this configuration is that the actors work with the government and are enabled through a variety of mechanisms but stop short of becoming a part of the government-as is the case with the co-optation configuration.

iii. Configuration 5: Sanctioning

Security companies developing these capabilities and using the same in contexts where governments explicitly prohibit such actions or in the absence of such legal frameworks. In such a relationship, *a company deploys ACD to secure its own organization or another private sector organization despite this relationship being illegal*. Though large companies like Google and Microsoft have the capability to carry out APCD and have done so in one-off instances in the past,[49] many companies rely on third party security companies to bring in these capabilities. Globally, the security market has been expanding. Private cyber security companies are increasingly resorting to taking active cyber defence measures include large defence-contractors such as Lockheed Martin in the US, BAE Systems in the UK and Airbus in Europe.[50]

These contractors have largely developed their own cyber security solutions and services,[51] although some have also hired commercial cyber security firms to bolster their capabilities. Lockheed Martin, for example, has developed its own portfolio and hired its first cybersecurity contractor, Industrial Defender[52] which added to Lockheed portfolio of intelligence-driven security solutions.[53] Start-ups such as Crowd Strike and CloudFare have attracted

---

[49] Matt Buchanan, 'Google Hacked the Chinese Hackers Right Back' (*Gizmodo*, 18 June 2013) <https://gizmodo.com/5449037/google-hacked-the-chinese-hackers-right-back> accessed 2 November 2018.

[50] Maurer (n 20); Peggy Hollinger, "Defence Groups Take Aim at Cyber Security" *Financial Times*, Mar 28, 2016 <https://www.ft.com/content/45aedb82-e676-11e5-bc31-138df2ae9ee6> (The record of their use for commercial security purposes remains sketchy at best and their largest customer base remains the government).

[51] 'About Us' (*Airbus CyberSecurity*) <https://airbus-cyber-security.com/about./> accessed 2 November 2018; 'Cyber Security Services' (*BAE Systems | Cyber Security & Intelligence*) <https://www.baesystems.com/en/cybersecurity/capability/cyber-security-services> accessed 2 November 2018.

[52] Loren Thompson, 'Lockheed Martin Moves To Dominate Cyber of Electric Grid & Energy Complex' (*Forbes*, 14 March 2014) <http://www.forbes.com/sites/lorenthompson/2014/03/14/lockheed-martin-moves-todominate-cyber-defence-of-electric-grid-energy-complex/>.

[53] ibid.

significant investment from corporations to engage in ACD.[54] Smaller cybersecurity companies like ManTech[55] in the US or NICE in Israel are also engaging in these measures.[56] It has been found that a cluster of companies have formed a cyber security-military industrial complex that work in the development and deployment of cyber weapons if the government is unable or unwilling to do so.[57] An under-cover market in the Netherlands has enabled the hiring of cyber security companies, including those located in foreign territory to attack the networks of potential adversaries.[58] This market operates largely without any oversight and potentially can replace the government as the final guarantor of financial security, as per one Dutch expert.[59]

The damage caused by Operation Aurora through 2009[60] signalled that passive cyber defence mechanisms may not be sufficient to ward off Advanced Persistent Threats ('APTs').[61] Operation Aurora is the name given to a series of cyberattacks from China which targeted U.S. private sector companies back in 2010.[62] This included a phishing company which compromised the networks of several large American companies including Yahoo, Adobe, Dow Chemical, Morgan Stanley, Google and several others, in a gambit to steal trade secrets.[63] Cyber security companies CrowdStrike,[64] FireEye,[65]

---

[54] The Economist, 'Firewalls and Firefights' (August 10, 2013) <https://www.economist.com/business/2013/08/10/firewalls-and-firefights> accessed 2 November 2018.

[55] Securing the Future (*ManTech*) <https://www.mantech.com/> accessed 2 November 2018.

[56] Maurer (n 20), 18.

[57] Shane Harris, *@War: The Rise of the Military-Internet Complex* (New York: Houghton Mifflin Harcourt Publishing, 2014) 119–120.

[58] Dennis Broeders, 'Investigating the Place and Role of the Armed Forces in Dutch Cyber Security Governance' (Netherlands Defence Academy, 2015).

[59] ibid.

[60] Operation Aurora (Sophos Security Topics) <https://www.sophos.com/en-us/security-news-trends/security-trends/operation-aurora.aspx> accessed 2 November 2018. ("Operation Aurora is a targeted malware attack against at least 30 major companies—including Google and Adobe—which exploited a zero-day flaw in Internet Explorer. The exploit allowed malware to load onto users' computers. Once loaded, the malware could take control of the computer to steal corporate intellectual property").

[61] Kim Zetter, 'Google Hack Attack was Ultra Sophisticated, New Details Show' *WIRED* (14 January 2010) <http://www.wired.com/2010/01/operation-aurora/>.

[62] Council on Foreign Relations, *Operation Aurora* (January 2010) <https://www.cfr.org/interactive/cyber-operations/operation-aurora>.

[63] ibid.

[64] 'Cybersecurity Solutions' (*CrowdStrike*) <https://www.crowdstrike.com/solutions/> accessed 2 November 2018.

[65] 'Cyber Security Experts & Solution Providers' (*FireEye*) <https://www.fireeye.com/> accessed 2 November 2018.

Hexis,[66] and MITRE[67] have attempted to develop the Active Cyber Defence (ACD) industry by developing a range of solutions and articulating justifications for its legalization.[68]

A burgeoning industry of cybersecurity companies are providing honeypots and more aggressive ACD services.[69] These ACD services are part of a rapidly expanding cybersecurity industry that might reach 248.26 billion by 2023, in which ACD services occupy a fair share.[70] 36 per cent of respondents (private companies) to a survey conducted at the Black Hat Security conference claimed to have indulged in active cyber defence.[71] Due to fears of prosecution, many companies outsource their ACD measures to companies at home or abroad.[72] Some cybersecurity companies also reportedly set up entire divisions abroad so that they can engage in ACD measures that are at present, illegal in the United States.[73]

It is important to note that much of the cybersecurity market is concentrated in the United States, Israel, United Kingdom and Western Europe[74] with North America holding the largest market share by continent.[75] This is crucial to note as the market for ACD might be similarly skewed in favour

---

[66] 'Hexis Cyber Solutions' <https://www.immixgroup.com/hexis/> accessed 2 November 2018.

[67] 'Resiliency' (*The MITRE Corporation*, 27 January 2014) <https://www.mitre.org/capabilities/cybersecurity/resiliency>

[68] Amanda N. Craig, Scott J. Shackelford, and Janine S. Hiller, 'Proactive Cybersecurity: A Comparative Industry and Regulatory Analysis' (2014) 52(4) American Business Law Journal 721.

[69] Whatt Hoffman & Ariel E. Levite, '*Private Sector Cyber Defence: Can Active Measures Help Stabilise Cyberspace?*' (Carnegie Endowment for International Peace, 2017) <https://carnegieendowment.org/files/Cyber_Defence_INT_final_full.pdf>.

[70] 'Cybersecurity Market Worth $248.26 Billion by 2023' (Markets and Markets) <https://www.marketsandmarkets.com/PressReleases/cyber-security.asp> accessed 2 November 2018.

[71] 'Firewalls and Firefights' *The Economist* (10 August 2013) <https://www.economist.com/business/2013/08/10/firewalls-and-firefights> accessed 2 November 2018.

[72] Hoffman & Levite (n 69).

[73] Michael Riley and Jordan Robertson, 'FBI Probes if Banks Hacked Back as Firms Mull Offensives' *Bloomberg* (30 December 2014)<http://www.bloomberg.com/news/articles/2014-12-30/fbiprobes-if-banks-hacked-back-as-firms-mull-offensives> accessed 2 November 2018.

[74] 'Cybersecurity 500 List, 2018 Edition,' *Cybercrime Magazine* (22 May 2018) <https://cybersecurityventures.com/cybersecurity-500-list/>; Hadar and Tomer, 'How Did Israel Become a Leader in Cybersecurity?' *Automotive News* <http://www.autonews.com/article/20181001/SHIFT/181009995/israeli-intelligence-cybersecurity> accessed 2 November 2018 (There are over 400 cybersecurity companies active in Israel).

[75] Research and Markets,'Cybersecurity Market - Global Forecast to 2023: Innovation Spotlight on Splunk, Cyberbit, Carbon Black & Balbix' *PR Newswire* (28 September 2018) <https://www.prnewswire.com/news-releases/cybersecurity-market---global-forecast-to-2023-innovation-spotlight-on-splunk-cyberbit-carbon-black--balbix-300720906.html> accessed 2 November 2018.

of economically and militarily powerful countries, if enabled globally. The geo-political spill-off from this distribution is a major challenge for conceptualizing APCD at the global level and will be discussed in Part IV.

TABLE 2: MODELS DENOTING APCD CONFIGURATIONS

	MODEL	APCD CONFIGURATION	RELATIONSHIP BETWEEN AND PRIVATE ACTOR	EXAMPLES
ENABLES APCD	**DELEGATION**	Private actors engaging in ACD under 'effective control' of the government after delegation by a clearly defined legal/policy instrument	'Effective control'; every decision must be approved by the government	Singapore
	ORCHESTRATION	Government not being clear about the legality of APCD	Government gives tacit approval without explicitly invoking APCD in law or policy instruments	India, UK, INTERPOL
	SANCTIONING	Private actors operating under the radar despite ACD being illegal	Government does not recognize existence of the private actors operating under the radar	Markets in USA, Israel, UK and Western Europe

"PRE"-APCD	**CO-OPTATION**	Private sector actors work with the government in the form of a multi-stakeholder unit	Collective decisions are taken by the unit as a whole	USA Cyber Command, Estonian Cyber National Guard
	BANNING	Law explicitly banning ACD measures by the private sector	Despite the existence of a law, private sector actors often operate under the radar, which means that this model co-exists with 'sanctioning'	Albania, Antigua & Barbados, Kenya, Fiji, Japan, USA, Ghana, Austria[76]

III. The Role of International Law

The normative framework of international law often acts as a tool for resolving conflict and creating governance frameworks for actions where policy vacuums exist. Successful cyber security measures depend on cooperation between different stakeholders. The transboundary nature of the internet, the broad scope of cyber security itself, and the range of actors impacted by the same - means that the level of international cooperation influences the level of national cyber security as it enables information sharing, development of best practice, and *increases the interoperability and compatibility of cyber defence*.[77] Grounding APCD in international law can help in ensuring the compatibility and interoperability of APCD across national borders and in improving the level of trust that nations repose in the modus operandi of such measures.[78] Furthermore, as demonstrated by the section above, the use of APCD as is currently being carried out, is complex and raises important

[76] See Amanda N. Craig, Scott J. Shackelford, and Janine S. Hiller, 'Proactive Cybersecurity: A Comparative Industry and Regulatory Analysis' (2015) 52(4) American Business Law Journal 721 et al for more detailed sampling

[77] Secretariat of the Security Committee, Finland, 'Finland's Cyber Security Strategy: Background Dossier' (2013) <https://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf>.

[78] Martha Finnemore and Duncan Hollis, 'Constructing Norms for Global Cybersecurity'(2016) 110(3) American Journal of International Law 425, 427; Lawrence

questions about legality and jurisdiction. Furthermore, the understanding of how international law applies to APCD measures is an extension of the issues being negotiated in the UN Group of Governmental Experts (UN-GGE) and other international forums- particularly on the right to self-defence and international law of state responsibility and countermeasures. International law is by no means a panacea and would not substitute the domestic governance frameworks and discursive practices that would determine the framing of domestic policy. However, by devising model universal best practices, it could nudge nations into devising and implementing effective policy on this front. To get there, however, a doctrinal application and interpretation of the existing standards of international law to existing scenarios must be the starting point.

There exists a body of legal scholarship that has sought to evaluate the doctrinal validity of APCD capabilities as enabled by a state. For example, Messerschmidt makes three analytical assertions that demonstrate how APCD measures can comply with existing standards of international law, if it is at the receiving end of cyber-attacks. Towards understanding how international law may apply to APCD we examine Messerschmidt's three assertions and attempt to call out various legal complexities that arise with each.

A. Violation of International obligations

Is there a violation of an international obligation by the state from whose territory an attack emanates from?

The customary international law on the responsibility of states for the commission of internationally wrongful acts, which have been codified in the Articles on State Responsibility,[79] recognize that a state can be held responsible in International Law if two elements are fulfilled:

1. the act or omission that leads to the breach of an international obligation and
2. attribution of that act or omission to the state in question.[80]

On the first point, it is clear that active cyber defence measures that intrude into external computer systems could be internationally wrongful

Lessig, 'The Regulation of Social Meaning'(1995) 62 University of Chicago Law Review 943.

[79] Adopted by UNGA in 2005

[80] International Law Commission, Articles on the Responsibility of States for Internationally Wrongful Acts, Report of the International Law Commission on the Work of its 53rd session, A/56/10, August 2001, UN GAOR, 56th Sess Supp No 10, UN Doc A/56/10(SUPP) (2001), art 4(1) ("Articles on State Responsibility").

acts. First, they may violate the prohibition on the use of force in Article 2(4) of the UN Charter. The Tallinn Manual- sponsored by NATO and authored by an International Group of Experts (IGE) proposes eight criteria to determine when a cyber operation amounts to a use of force: severity, immediacy, directness, invasiveness, measurability, military character and presumptive legality.[81] ACD measures on the active end of the spectrum such as hack backs or botnet attacks could in certain cases be counted as a use of force based on this criterion. Second, these could violate the norm against norm-intervention, which is a part of customary international law, by violating the territorial sovereignty of another nation in cyber space.[82] Finally, active cyber defence measures might also be considered cybercrimes as per the framework of The Budapest Convention. The Budapest Convention, entered into force in 2004, is the only binding international instrument in this regard and has thus far has sixty four signatories including Australia, Canada, US, Japan, and most European Union States (but notably not India.)[83] It requires state parties to adopt legislation or other measures to criminalize the international commission of certain offenses. These include: illegal access to computer systems, illegal interception of data, data interference, system interference, misuse of devices, computer-related forgery, and computer-related fraud.[84] Active cyber defence measures used on external systems will amount to the aforementioned offenses under The Budapest Convention as they are likely to damage infrastructure in another state party's jurisdiction than other purely investigative measures.[85] While the Budapest Convention has not been

---

[81] Michael N. Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Warfare* (Cambridge University Press, 2017) "(a) Severity: How many people were killed? How large an area was attacked? How much damage was done within this area? (b) Immediacy: How soon were the effects of the cyber operation felt? How quickly did its effects abate? (c) Directness: Was the action the proximate cause of the effects? Were there contributing causes giving rise to those effects? (d) Invasiveness: Did the action involve penetrating a cyber network intended to be secure? Was the locus of the action within the target country? (e) Measurability: How can the effects of the action be quantified? Are the effects of the action distinct from the results of parallel or competing actions? How certain is the calculation of the effects? (f) Military character: Did the military conduct the cyber operation? Were the armed forces the target of the cyber operation? (g) State involvement: Is the State directly or indirectly involved in the act in question? But for the acting State's sake, would the action have occurred? (h) Presumptive legality: Has this category of action been generally characterized as a use of force, or characterized as one that is not? Are the means qualitatively similar to others presumed legitimate under international law?"

[82] Thomas Payne, 'Teaching Old Law New Tricks: Applying and Adapting State Responsibility to Cyber Operations' (2016) 20(2) Lewis & Clark Review 699.

[83] Chart of Signatures and Ratifications of Treaty 185, Council of Europe <http://perma.cc/57D7-XPBF>

[84] Convention on Cybercrime 2001 ('Budapest Convention').

[85] Alexandra Van Dine, 'When is Cyber Ddefence a Crime? Evaluating Active Cyber Ddefence Measures under the Budapest Convention' (2020) 20(2) Chicago Journal of International Law 562.

universally accepted, it has been ratified by a number of states engaging in active cyber defence measures and therefore it is clear that they need to adopt legislation that constrains the same.

A plain reading of the articles would indicate that acts of private persons or groups are not attributable to the state, unless the non-state actor operating under the 'effective control' of the state.[86] However, the Commentary published along with the articles by the International Law Commission declares that a state may be held responsible for the acts of private parties if they failed to take necessary measures to prevent the wrongful acts.[87]

The obligation to take 'necessary preventive measures' indicates a due diligence obligation to prevent the use of its territory for the commission of wrongful acts.[88] Messerschmidt approaches this question through the customary international law on the prevention of significant transboundary harm, which results in 'liability' rather than state responsibility.[89] The key difference between liability and responsibility lies in the fact that the act which caused significant transboundary harm need not be an internationally wrongful act.[90] A state is liable if any activity from its territory causes significant transboundary harm, even if the state did not exercise 'effective control' over the private party. In such scenarios, even if a state is not responsible in international law, they could potentially be held liable. Messerchmidt traces the evolution of this obligation in international law from its origin in the *Trail Smelter* arbitration[91] through its recognition by the International Court

---

[86] State responsibility is imputed if imputes state responsibility "if the conduct of a non-state actor is "acting under the instructions of or under the direction and control of the state carrying out the said conduct." This test, known as the 'effective control' test was laid down by the International Court of Justice in Nicaragua and imported by the ILC into Article 8. The test essentially requires a state to "exercise such a degree of control in all fields, as to justify the non-state actors on its behalf". It implies that the state must have directed each allegedly wrongful act in order to attract international responsibility. This test has been criticized by several scholars as being too high a threshold and therefore limiting greatly the scope of state responsibility.

[87] "For example, at page 39,, "a receiving State is not responsible, as such, for the acts of private individuals in seizing an embassy, but it will be responsible if it fails to take all necessary steps to protect the embassy from seizure, or to regain control over it."

[88] Timo Koivurova, 'Due Dilligence' in Max Planck Encyclopedia of Public International Law (2013) <https://www.arcticcentre.org/loader.aspx?id=78182718-d0c9-4833-97b3-b69299e2f127> accessed 2 November 2018.

[89] Messerschmidt (n 5).

[90] See M.B. Akehurst, 'International Liability for Injurious Consequences Arising out of Acts not Prohibited by International Law' (1985) 16 NYIL 3; A.E. Boyle, 'State Responsibility and International Liability for Injurious Consequences of Acts not Prohibited by International Law: A Necessary Distinction?' (1990) 39 International and Comparative Law Quarterly 1.

[91] Trail Smelter (*United States v Canada*), 3 RIAA 1905, 1924-33 (1938).

of Justice in the *Corfu Channel Case*[92] to its codification in the Draft Articles produced by the International Law Commission in 2001.[93]

Even though some commentators have argued that *Trail Smelter* arbitration advocated for a strict liability standard,[94] the ILC Draft Articles have laid down a due diligence obligation.[95] The Commentary articulates that a due diligence obligation requires reasonable efforts by a State to inform itself of factual and legal components that relate foreseeably to a contemplated procedure and to take appropriate measures in a timely fashion to address them."[96]

The International Court of Justice has stated that due diligence is an obligation of conduct and not of result.[97] The due diligence standard should be evaluated on a two-pronged test - of knowledge and capacity.[98] The knowledge prong entails assessment of whether the state possessed the knowledge of a specific cyber-attack or whether it ought to have known about the operation given the means at its disposal ('Constructive Knowledge')[99]. The capacity prong entails that the state makes full use of its institutional, resource and territorial capacity to detect cyber threats and prosecute them, if need be. [100]

The due diligence principle has also been flagged off by Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Rule 7) which " requires a state to take all measures that are feasible in the circumstances to put an end to cyber operations that affect a right of and produce serious adverse consequences for other states."[101] The commentary does not lay down any guidelines on the duty of host states to prevent potential attacks, the duties of states through which the attack is routed and how the 'constructive knowledge' test applies to cyber operations.[102] At the same time, the

---

[92] Corfu Channel (*United Kingdom v Albania*), 1949 ICJ 4, 22 (April 9).

[93] The Draft Articles are yet to be adopted by the General Assembly but are widely recognised as an authoritative codification of the customary international law on the subject.

[94] Trail Smelter (*United States v Canada*), 3 RIAA 1905, 1924-33 (1938).

[95] Commentary to Draft art 71.

[96] ibid.

[97] J.G. Lammers, *Pollution of International Watercourses: A Search for Substantive Rules and Principles* (Martinus Nijhoff Publishers, 1984) 524.

[98] Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia & Montenegro) [2007] ICJ 2 (Feb. 26) [430].

[99] Kimberley N. Trapp, 'State Responsibility for International Terrorism: Problems and Prospects' (2011) 23(1) European Journal of International Law 67.

[100] ibid.

[101] Schmitt (n 81).

[102] (1) Clearly defined cyber security policy and/or legislation, (2) Use of government funds to create nodal agencies responsible for cybersecurity, (3) Continuous communication if any hazardous cyber activities are detected, (4) Response to any requests for evidence by international bodies.

Manual is clear that there is no duty to monitor cyber activities originating from their territory owing to surveillance concerns.[103]

It is clear that international law imposes an obligation of due diligence when there is actual or constructive knowledge and capacity to prevent transboundary harm. However, jurisprudence and scholarship on the practical ramifications came out before the proliferation of cyber-attacks and the unique challenges states face with regard to detecting and attributing cyber-attacks. Existing scholarship fails to apply doctrinal theory to cyberspace, which renders it difficult for host states and the rest of the international community to determine whether due diligence obligations in cyberspace are being fulfilled.[104] This in turn complicates the assessment of legal active countermeasures that can be undertaken by the private sector.

B. ACD under International Law

Do active cyber defence mechanisms qualify as legal counter-measures under international law?

The right to take counter-measures against internationally wrongful acts has been understood by experts as an essential feature of a decentralized global political set-up that lacked a global law enforcement authority.[105] It is key to note that counter-measures are only available against internationally wrongful acts committed by other states and not available against states that are liable for prevention of acts that are not internationally wrongful and merely caused significant transboundary harm.

The customary international law doctrine of counter-measures has been codified by the International Law Commission in Articles 49-54 of the Articles on State Responsibility.[106] Article 49 sets out three important conditions which restrain the use of counter-measures:

1. Counter-measures are only available in response to and attributable to a state.

---

[103] Dan Efrony and Yuval Shany, 'A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice'(2018) 112(4) American Journal of International Law 583.

[104] ibid.

[105] Oona Hathaway and Scott J. Shapiro, 'Outcasting: Enforcement in Domestic and International Law' (2011)121 Yale Law Journal 252, 300-320; Louis Henkin, *How Nations Behave: Law and Foreign Policy* (2nd edn, 1979) 24.

[106] Draft articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries, arts 4-6, Vol II, *Yearbook of the International Law Commission*, 2001. <http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf>.

2. Their aim is a restoration of legality between the two states, rather than the imposition of punitive sanction. For that reason, they are usually temporary or provisional.

3. As far as possible, counter-measures chosen should be reversible. Paragraph 1 of Article 50 further states that countermeasures should not change, in any way:

    a. The obligation set out in Article 2(4) to refrain from the use of force;

    b. Obligations relating to the protection of fundamental human rights. They must also not violate peremptory norms of International Law known as jus cogens.

    c. Further, they must be proportionate to the injury suffered both in terms of the gravity and the rights infringed.

    d. The Commentary mentions that every countermeasure must have a clearly defined purpose that is designed to ensure that the wrongful act ceases and not extend to purposes of retribution.

Ideally, states are also expected to notify the state engaging in the wrongful act before taking counter-measures, although in urgent cases this may not be feasible.[107] In his articulation of the UK's position on the application of International Law in cyberspace, the UK Attorney-General has stated prior notification may not be a legal obligation in the case of cyber counter-measures due to the need for a rapid response in many cases and the sensitive nature of cyber capabilities involved.[108] The Attorney-General's argument may be valid if there are instances of repeated cyber-attacks being directed at one state from the territory of another. For example, a one-off notice[109] may be sufficient to justify future counter-measures in the case of China repeatedly transgressing its obligation to prevent transboundary

[107] However, the injured State may take "such urgent counter-measures as are necessary to preserve its rights" even before any notification of the intention to do so.

[108] Office of Attorney General, 'Cyber and International law in the 21st Century' (Government of UK, 23 May 2018) <https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century> accessed July 13, 2018 [hereinafter Wright speech].

[109] Press Release, U.S. Department of State, 'Statement on Google Operations in China' (U.S. Department of State, 12 January 2010) <http://www.state.gov/secretary/rm/2010/01/135105.html> ("We have been briefed by Google on these allegations, which raise very serious concerns and questions. We look to the Chinese government for an explanation. The ability to operate with confidence in cyberspace is critical in a modern society and economy. [Secretary of State Clinton] will be giving an address next week on the centrality of internet freedom in the 21st century, and we will have further comment on this matter as the facts become clear."

harm from its territory against U.S. firms. The Tallinn Manual suggests that if notification of the intent to take a countermeasure would defeat the objective of taking the counter-measure, then notice need not be provided.[110] The majority of experts who drafted the Manual claimed that prior negotiations with the erring state was not a requirement before taking countermeasures.[111] The Tallinn Manual thus fails to provide any guidance on the parameters that states might use to decide whether to provide notice or engage in negotiations.[112]

This position may not be tenable as it vitiates the purpose of counter-measures, which is to bring about a cessation of the wrongful act and restore status quo. *Without notification to, and communication with, the host state, one-off counter-measures might result in continued escalation, particularly when private sector actors are involved*. Apart from the Tallinn Manual, no document has clearly resolved this tension. While it is true that prior notification might jeopardize the success of certain active cyber defence measures, at the bare minimum states need to develop confidence building mechanisms and other frameworks of co-operation that prevent the escalation that the Articles on State Responsibility were designed to protect against.

C. Private sector and ACD

Can the private sector engage in countermeasures?

The Articles on State Responsibility (‘**ASR**’) clearly articulates that only states can engage in legal countermeasures. Messerschmidt attempts to get around this legal hurdle by invoking reciprocity.[113] His claim rests on the premise that the internationally wrongful act is the breach of an obligation to prevent transboundary harm by a private actor. Therefore, it is justified for the victim state to enable the private sector to engage in counter-measures.

This argument is unfeasible. Neither the ASR nor other principles of customary law of international responsibility recognize that reciprocity is an exception to the rule that only states can engage in counter-measures. The right vests solely with states because they are better equipped than non-state actors to detect an internationally wrongful act, attribute it to a state and determine the responses that would be most appropriate for bringing about a cessation of the act.

---

[110] Schmitt (n 80), 120.
[111] ibid.
[112] Efrony & Shany (n 103).
[113] Messerschmid (n 5), 279.

Private actors can take legal counter-measures only if its relationship with the state is such that it is acting on behalf of the state. Drawing from the categorisation in the Articles on State Responsibility, Maurer lays down a workable typology of proxy-state relationships in conjunction with the international law perimeters laid down in the Law on State Responsibility.[114] Within this framework, three kinds of relationships between the state and non-state groups demarcated in the Articles on State Responsibility can come within the ambit of delegation or active-state sponsorship, which would entail that the state is held responsible for the commission of any wrongful act. This includes:

1. Non-state actor exercising **governmental authority** (**Arts 4-6**),
2. Non-state actor acting under the **direction or control of a state** satisfying the **'effective control' criteria** (**Art. 8**) which means that the state is in control of the specific operation through planning, direction and support. As per the ICJ, the satisfaction of the effective control requires the state to "exercise such a degree of control in all fields, as to justify the non-state actors on its behalf"[115] and direct every act undertaken by the private actor.
3. **Overall control**, which means that the state exerts general control and influence in terms of planning and supervising of the group in general but not in the execution or direction of the specific operation.[116]

The Articles on State Responsibility attribute the acts of non-state actors to the state in the first two models i.e. when they are effectively acting on behalf of the state and taking direct instructions for each act. Therefore, providing individual companies the discretion to engage in counter-measures without direct state authorisation, supervision, and accountability would not be in compliance with International Law.

D. Analysis vis-à-vis APCD configurations

The present international legal framework clearly renders configurations of sanctioning and orchestration illegal simply because private actors are the key decision-makers in those configurations. In the case of orchestration,

---

[114] Maurer (n 20), 126.

[115] Nicaragua v. United States of America, 1986 I.C.J 14 at 62-64, 65..

[116] *Prosecutor v Tadić*, Case No. IT-94-1-T, Appeal Judgment, ¶ 120 (July 15, 1999) (As per existing international law, proving that a state has overall control over is not sufficient to hold the state responsible for an internationally wrongful act. The overall control test was evolved in a different legal context by the International Criminal Tribunal for Yugoslavia for the purpose of determining whether an international armed conflict existed and is yet to be accepted by any tribunal for the purposes of invoking state responsibility).

loosely worded policies like the Indian Cyber Security Strategy prevent the state from exercising effective control over each cyber operation.[117] When turning a blind eye, the state effectively gives a free reign to private actors, thereby violating their due diligence obligations to prevent cyber harm.

A strictly defined model of delegation may be legal if the following criteria are met. First, the state retains 'effective control' over the private actor such that its actions are attributable to the state. Second, there must be a framework for communication and confidence-building in lieu of notification as per the Articles on State Responsibility. The Singapore Cyber Security Act is an example of a well-drafted law that enables the government to retain effective control over the private actor. As per the Bill, the Minister needs to satisfy himself of the need for engaging a private actor to use ACD and also issue a certificate that specifies the measures that the actor can take. [118]

While the doctrinal analysis of international law is important, we are still left with important and unresolved questions-not least because international law is unclear and ill-equipped in its present form to deal with the frequency, pace and stealth of cyber conflict. We therefore must consider the geo-political and practical ramifications that might help fill some of the grey zones in international legal theory and help identify parameters that can make this theory relevant in the present factual scenario.

IV. Projecting Consequences

The developments and legal hurdles mapped out in the preceding sections present a key set of benefits and risks before policy-makers. In this section, we put forward a set of potential consequences of developing APCD globally and the regulatory challenges involved. First, we map out the benefits and risks at a high-level before evaluating how they apply at the level of each configuration.

High-level challenges

The first set of challenges arises from the political dynamics of governing a phenomenon as unique as cyberspace.[119] First, the dynamic and possibly

[117] While this strategy is likely to be updated in 2020, as of now there is no clarity on offensive cyber operations and India's cyber doctrine, including in relation to active cyber defence

[118] Parliament of Singapore, 'Cybersecurity Bill' <https://www.parliament.gov.sg/docs/default-source/default-document-library/cybersecurity-bill-2-2018.pdf> accessed 2 November 2018.

[119] Lucas Kello, *The Virtual Weapon and International Order*, (Yale University Press 2017) 82. He identifies three orders of cyber-revolution. Third-order revolution or systemic

quasi-anarchic nature of cyberspace and the diffusion of power to individual actors means that regulation and attribution capabilities driven by the government will always be playing catch-up with technological advancements spearheaded by the private sector. As the private sector is driving technological innovation, the state-centric model of security is under threat. Second, the incentive structure and strategic intent of various states behind launching operations in cyberspace differs, based on their current geopolitical ambitions. This has an impact on the relationship each state wishes to forge with private actors operating in cyberspace. The United States and China, for example, choose to hold their cyber proxies 'on a tight leash'[120], whereas Iran - reminiscent of the tactics used during and since the Iranian revolution[121]- grants them far more autonomy in their actions.[122] The democratic nature of the state enabling APCD also raises questions about the legitimacy of these measures in the eyes of the international community. Third, there is still no consensus among states on how the standards of international law apply to operations in cyberspace, which makes evolving a universally accepted set of standards difficult to gauge. While it is true that certain acts might be legal at a national level but still have negative geo-political consequences, a determination of legality lends a level of universal certainty to global policy and serves as the edifice for the demarcation of norms of responsible behaviour. Fourth, if the state enables the private sector to engage in increasingly aggressive action in cyberspace, a key challenge is ensuring that they remain accountable to the government and the government is able to enforce punishment for any collateral damage.

Proponents of APCD see the evolution of this practice as a necessity. The greater digitisation of key infrastructure means an increase in vulnerabilities that can be exploited by attackers, which has caused security experts to recognise a diminishing value to ramping up cyber defence mechanisms.[123] A hacker will be able to exploit a zero-day vulnerability at some point,

---

disruption results in drastic changes within the confines of the existing state structure. The drastic changes happen in both the material ingredients of power which are, in this case, defined by (1) A change in the physical architecture that defines power at the international level and (2) A change in the norms and rules which govern interactions between states. He then identifies second-order cyber revolution, which is brought about when a state or a group of states reject the shared purpose of the existing units, (systems revision) which may be exemplified by North Korea's weaponization of cyberspace.

120 Maurer (n 20), 71–80.

121 Daniel L. Byman, 'Proxy Power: Understanding Iran's Use of Terrorism' (*Brookings*, 26 July 2006) <https://www.brookings.edu/opinions/proxy-power-understanding-irans-use-of-terrorism/>.

122 Maurer (n 20), 81-93.

123 Michael V. Hayden, 'The Future of Things "Cyber" (2011) 5(1) Strategic Studies Quarterly 3, 5.

regardless of how robust the defence mechanisms are.[124] Proponents from the private sector argue that traditional remedies involve lengthy prosecution times and jurisdictional challenges, that are ineffective in responding to and deterring viruses and worms that move at extraordinary speed.[125] Further, law-enforcement authorities arguably lack adequate capacity to comprehend and respond to attacks infiltrating national information infrastructure or that of private actors. By responding aggressively to attackers, APCD has the potential to deter future attacks by increasing the cost to attackers in mounting a cyber-attack.

The detractors argue that it is unlikely that APCD will enable the swift recovery of data or prevent its further dissemination. First, it is estimated that the time lag between the occurrence of a breach and its detection is roughly 100 days.[126] Second, attribution is difficult for most private sector entities who lack the data, intelligence and knowledge of the adversary, which could result in them taking action on the wrong machines or attackers.[127] While this is also possible in the case of government action, historically the government has had diplomatic, intelligence and confidence building tools at its disposal-something that international relations scholars have found lacking with private actors.[128]This could lead to escalation, both in terms of continued offensive cyber operations by the attacker and counter-measures taken by victims, with the potential of bringing more actors into the equation when incorrect machines or actors are targeted through APCD measures.

Challenges within each configuration

These escalatory outcomes are far more likely in sanctioning or orchestration models where private actors act alone or with parts of the government machinery without co-ordination either between themselves or with various units of the government. Hence, geopolitical realities affirm the doctrinal logic behind banning these configurations-something that was discussed in the previous section.

---

[124] ibid 7.

[125] Messerschmidt (n 5). For example, the devastating Sapphire/Slammer worm doubled in size every eight and a half seconds.

[126] Roi Perez, 'FireEye Says Criminals Now as Sophisticated as Nation States' *Cybersecurity News, Reviews and Opinion* (16 March 2017) <https://www.scmagazineuk.com/fireeye-says-criminals-sophisticated-nation-states/article/1475041> accessed November 2, 2018.

[127] Andrea Limbagao, 'The 'Hacking Back' Bill Isn't the Answer to Cyberattacks' (*War on the Rocks*, 31 October 2017) <https://warontherocks.com/2017/10/the-hacking-back-bill-isnt-the-solution-to-cyberattacks/> Accessed November 2, 2018.

[128] Brandon Valeriano and Ryan C. Maness, *Cyber War Versus Cyber Realities: Cyber Conflict in the International System* (Oxford University Press 2015).

The advantages of co-option which lie in pooling resources at various levels of government-including the military, the Computer Emergency Response Team (CERT) teams, law enforcement and intelligence agencies are absent in a model that relies on the government failing to clearly lay the boundaries of private action. Further, there is a need for a clearly defined national policy framework that restricts APCD coupled with implementation of the policy such that an illegal underground market does not get sanctioned and legitimized. Lacunae in these two core requirements could further geo-political instability as other states and private actors would be unsure of the range of responses they can expect in the form of offensive cyber action. As was seen with the uncertainty that prevailed during the arms race during the Cold War between USA and USSR[129], uncertainty in the cyber context might cause all parties to ramp up both their offensive and defensive capabilities.

TABLE 3: BENEFITS AND RISKS OF APCD

	Benefits	**Risks**
Accuracy and expediency	Avoids legal fetters such as jurisdictional issues, lengthy prosecutions and lack of capacity	Time and accuracy constraints in attribution of the cyber-attack coupled with lack of intelligence
Impact	Swift response to attack vectors, thereby mitigating impact and increased chances of recovery of data	Collateral damage if the response penetrates third-party networks
Geo-political consequences	Deterring future attacks by raising the immediate cost to the attacker	Potential for escalation of conflict due to continued retaliation by private actors

(Source: Adapted from Hoffman and Levite)

A clearly established framework of delegation, on the other hand, ensures that governments play a key role in demarcating the limits of private action and holding companies to account for the same, while also utilising the private sector to craft a credible perception of national cyber resilience. This could enable the private sector to play a defined and understood role in the protection of information infrastructure from both existing and future

[129] Thomas C. Schelling, *The Strategy of Conflict* (Whitefish, MT: Literary Licensing 2011).

threats at an organizational, sectoral, and national level. Though a delegation framework can easily be applied at a national level, the complicated nature of the private sector and private sector security market raises geopolitical and jurisdictional concerns that national frameworks are not necessarily equipped to resolve.

However, delegation may not rectify all deficiencies that arise when a core governmental function is delegated to a private actor. One major challenge is holding the private actor accountable. The accountability problem is explained by the problem of divergent interests, that Singer has explained in the context of Private Military Security Companies ('PMSCs'). The state might have an interest in stability due to fear of retaliation and responsibility in International Law.[130] However, the non-state actor carrying out the operation will not bear the brunt of retaliatory responses or be held responsible or liable under international law. They would solely be driven by the mandate issued by the government (and the profits resulting from it), which is to carry out the measure successfully unless the government imposes accountability obligations on the private actor. To do so however would require the government to monitor the actions of the private actor, which would require further deployment of private resources. One potential way of doing this efficiently would be combining delegation with co-optation, where the private actor does not act alone but in cohesion with an ecosystem of both state and non-state actors working on cyber-security.

Further, the adoption of APCD measures need to be considered in terms of geopolitical realities also. First, cyberspace is intricately interconnected and crosses jurisdictional boundaries. Therefore, a situation where different countries adopt different models of APCD could result in continued cyber-attacks against countries that restrict the autonomy given to private sector actors. This is the scenario in status quo. Second, cyber security companies might work for multiple governments, which would lead to a conflict of interest. Further, the legal and policy implications of a company headquartered in one country using APCD in another country after being authorized by the second government are unclear. Third, delegation and co-opting can be accomplished effectively only if the government of a country is sufficiently more powerful than the private sector operating in that country. This is not necessarily the case in many countries in the developing world. We are also seeing this trend in relation to large tech-corporations in the developing world- where there is a high level of dependency on technology

[130] P.W. Singer, *Corporate Warriors: The Rise of the Privatized Military Industry* (updated ed., Ithaca: Cornell University Press 2008) 151–152.

companies from the US or China. Even in states that are able to exercise regulatory authority more effectively, technology companies can influence a number of decisions through excessive lobbying. Finally, the cyber security market is skewed in favour of countries in the developing world as they have a larger talent pool and financial resources. This could lead to a scenario where APCD mechanisms is being deployed more frequently by the developed world, even though the developing world has the same legal and policy enablers-thereby putting the Global South at a disadvantage.

Cyber defence analysts have often pointed out the perils of being complacent regarding the potential of regulating cyberspace solely through international law or norms. The geo-political risks, as documented above, remain prevalent and need to be grappled with and complacency in silver bullet solutions are undoubtedly misguided-particularly given that there is no certainty in the rules of international law that shape this space. However, the well-established tenets of international law offer a starting point to identify behaviour that could receive international sanction and facilitate continuous discourse and engagement between both states and non-state actors over a period of time.[131]

V. Looking Ahead

TOWARDS A CYBER STABILITY NORM HARNESSING ACTIVE PRIVATE CYBER DEFENCE AND AREAS FOR FURTHER RESEARCH.

Norm evolution can happen through three potential vectors. Existing research has shown that the development of standards by global bodies such as the International Standards Organization, spurred on through commercially driven norm-entrepreneurship by insurance companies led to the proliferation of universal standards[132] for the regulation of conduct by maritime security companies.[133] Standards enable the harmonised transmission of information across different contexts and help determine the roles of various actors. Applying this to private sector entities working on private defence allows for greater stability and predictability. The second vector is

[131] Monica Hakimi, 'The Work of International Law' (2017) 58(1) Harvard International Law Journal 1.

[132] Wyatt Hoffman & Ariel E. Levite, 'Private Sector Cyber Defence: Can Active Measures Help Stabilise Cyberspace?', <https://carnegieendowment.org/files/Cyber_Defence_INT_final_full.pdf 4>.

[133] Marc-Antoine & Carreira Da Cruz, 'Regulating Private Maritime Security Companies by Standards: Causes and Legal Consequences' (2017) 3 Maritime Safety and Security Law Journal <http://www.marsafelawjournal.org/wp-content/uploads/2017/12/MarSafeLaw_Carreira-Da-Cruz_Issue-3.pdf>.

increasingly empowered private sector organisations themselves engaging in norm entrepreneurship. Microsoft's Digital Geneva Convention, Siemen's Charter of Trust and the recently published tech accords are cases in point.[134] Realising the entanglement of economic dimension of cyberspace which relies on consumer trust to thrive, private actors have sought to develop norms that would ferment clearer standards of cyber security. While they seek to engage in active defence mechanisms, they should keep in mind the benefits of having predictability and certainty in the international normative framework driven by deference to structures of International Law.

We made a number of unique contributions to existing scholarship. The first section of this paper mapped the existing scenarios and put forward five configurations that illustrated the relationship between the government and the private sector. The first two-banning and co-optation do not envisage autonomy given to the private sector actor and therefore cannot be classified as APCD. The remaining three envisage varying degrees of autonomy. We observed that law and policy across nations conformed to a model that compelled restraint, such as banning but was disconnected from reality. The second section examined the enabling provisions of international law and highlighted the gaps in this field, particularly in terms of applying settled debates in traditional international law to the cyber domain. Multilateral efforts at the United Nations and across jurisdictions need to identify and plug this gap The final section looked at the five models from the perspective of geo-political risk and concluded that having a strong government through delegation or co-optation was less likely to result in escalation than mechanisms that delegated more decision-making power to the private sector.

This predictability will have an overall positive effect on the global cyber ecosystem. Deterrence is furthered on the basis of 3Cs - capability, credibility and communication.[135] Roping in private sector capabilities by optimizing the use of APCD and communicating this both through international channels but also through robust municipal legislation may work to further each of the 3Cs. The international legal standards outlined in Part III are not obsolete but need to be made relevant by ensuring that legislation implementing these standards are workable for today's pragmatic challenges. Further

---

[134] Chris Bing, 'Hoping to Fill a Global Void, Private Companies Push for 'Cyber Norms' (*Cyberscoop*, 22 February 2018) <https://www.cyberscoop.com/siemens-cybersecurity-charter-of-trust-airbus-dxp-cyber-norms/>. Jessica Woodall, *Cyber Norms and the Australian Private Sector* (*International Cyber Policy Centre*) <https://s3-ap-southeast-2.amazonaws.com/ad-aspi/import/ICPC-Private-sector-cyber-norms.pdf?EDM_hjeuRpko0j54MPGHjm234TPXAio1>.

[135] Jesse C. Johnson, Brett Ashley Leeds & Ahra Wu, 'Capability, Credibility, and Extended General Deterrence' (2015) 41(2) International Interactions 309.

research on possible regulatory models, insurance schemes and particularly, how the developing world fits into this scheme are important for determining its future.

However, for now, 'reining in' through clearly enforced delegation and co-optation, rather than banishing or letting loose these private sector companies has the potential to improve cyber security standards across the globe. The state must still retain its position as the final arbiter and guarantor of peace and security, while recognizing that the advances of modern society dictate that it cannot walk this path alone.

Sharing of children's health data by health professionals and parents – a consideration of legal duties

*Dr. Carolyn Johnston**

Abstract *Children's health data such as blood pressure, X-rays and written notes of medical examinations are produced in a clinical setting through health professionals' interaction with their minor patients. Health care practitioners owe legal and professional obligations not to disclose such information without consent or other legally recognised authorisation. With the increasing advent of data generated by patients themselves from wearable devices such as continuous glucose monitors and health apps, the patient, or parents, have initial control of the data and decide who to share it with. Where wearable devices have been provided to parents by the child's health care provider to monitor the child's health condition, there is an expectation that parents will share that information with the healthcare practitioner, who owes legal and professional duties to maintain the confidentiality of such data. Naturally, parents share information about their children with family and friends and increasingly on social media networks. They may also choose to share their children's health data on closed social media sites in order to gain support from members of that group for management of their children's health condition. This paper identifies obligations of privacy and confidentiality owed by healthcare professionals in Australia and India in respect of children's health data. I contrast how parents freely share information about their children on social media sites —'sharenting' —and address the adequacy of protections against future harms arising from dissemination of children's health data and suggest the limits of appropriate sharing.*

* Dr Carolyn Johnston is Senior Research Fellow, Law and Biotechnology, at the University of Melbourne.

I. Introduction

Children's health data is typically generated through the actions of a healthcare professional in a clinical setting. This data includes information derived from tests such as CT scans, X-rays and blood pressure readings. Increasingly, individuals are generating their own health data from a range of digital tools, including wearable devices and apps which collect and analyse data, for example, for stroke prediction and mental health. Patient-generated health data ('PGHD') has been described as health-related data 'created, recorded, gathered, or inferred by or from patients'[1] to address a health concern and for which the patient controls data collection and data sharing. In a White Paper on patient-generated health data, prepared for the United States Department of Health and Human Services, the authors note that PGHD is different from data generated in clinical settings in two important ways. First, patients, not providers, are primarily responsible for capturing or recording these data. Second, patients direct the sharing or distributing of these data to health care providers and other stakeholders.[2] This paper explores the second aspect –the boundaries of appropriate sharing of PGHD. I consider as a paradigm, the data generated by a continuous glucose monitor worn by children to manage type 1 diabetes ('T1D').

Diabetic patients are often called 'expert patients' because theircondition is largely self-managed, by themselves as adults or by parents of young children with T1D. Being in control of their condition means less day-to-day support is required from medical practitioners.[3] Self-management is enhanced through continuous glucose monitoring ('CGM') technology which measures glucose levels in real time.

---

1 RTI International, Patient-Generated Health Data (White Paper, Prepared for Office of Policy and Planning, Office of the National Coordinator for Health Information Technology, 2012).

2 ibid 2.

3 S.R. Shrivastava, P.S. Shrivastava and Jegadeesh Ramasamy, 'Role of Self-care in Management of Diabetes Mellitus' (2013) 12(14) Journal of Diabetes & Metabolic Disorders.

Data generated from the device is provided to the healthcare professional and then forms a part of the patient's (electronic) health record.

Increasingly, there has been a patient-led movement to design do-it-yourself ('DIY') technology to manage T1D. Under the hashtag 'WeAreNotWaiting',[4] people with T1D and their families are developing an open source software which links a CGM and an insulin pump, so that insulin is delivered automatically, based on real time readings, with little user input.[5] Users of such systems are colloquially known as 'loopers.'[6] In Australia, the Therapeutic Goods Act, 1989 regulates medical devices, including software used as or in connection with a medical device. No application has been made to register the open source software and, as a result, these DIY looping systems are not listed on the Australian Register of Therapeutic Goods. Healthcare professionals are, therefore, wary of their legal liability while supporting patients who use DIY looping systems.[7]_[8] Loopers get support from a community of loopers through closed Facebook groups such as 'Aussie, Aussie, Aussie, Loop, Loop, LOOP!' to gain advice and troubleshoot issues. Information is shared on these sites on the understanding that it is a shared enterprise for the benefit of the user group and codes of conduct (written and implied) promote the understanding that the information disclosed is not taken outside the group. Social media use in healthcare has many beneficial outcomes; it can complement information provided by healthcare professionals, allows patients to receive support and may lead to patient empowerment.[9]

---

4 #Open APS <> accessed 29 April 2020.

5 The results from the CGM are applied to a computer-controlled algorithm which calculates the insulin dose to be delivered by the pump to keep background insulin at consistent levels.

6 Tien-Ming Hng and David Burren, 'Appearance of Do-It-Yourself Closed-loop Systems to Manage Type 1 Diabetes' (2018) 48(11) Internal Medicine Journal 1400.

7 Carolyn Johnston and Lynn Gillam, 'Legal and Ethical Issues Arising from the Use of Emerging Technologies in Paediatric Type 1 Diabetes' (2019) 18(2) QUT Law Review 93.

8 Carolyn Johnston and others, 'Parents Using Unregulated Technology to Manage Type 1 Diabetes in Children' (The University of Melbourne 2020) <https://www.researchgate.net/publication/340884841_Parents_Using_Unregulated_Technology_to_Manage_Type_1_Diabetes_in_Children>.

9 Edin Smailhodzic and others, 'Social Media Use in Healthcare: A Systematic Review of Effects on Patients and on Their Relationship with Healthcare Professionals' (2016) 16(1)

This paper focusses on the adequacy of legal restrictions on disclosure of a child's health data by his/her clinicians, and by his/her parents on social media. Health data is considered particularly sensitive because of the influence that such information can have on employment, insurance and relationships. I first consider the privacy law in Australia and India and the scope of codes of practice framing the ethical obligations of healthcare professionals. I then address parents' legal and moral duties in the sharing of information about their children, comparing social and health information. I conclude that whilst a child's health data is offered adequate legal protection against unauthorised disclosure by health professionals, parents are accorded autonomy to share their child's datathrough the broadly defined legal concept of 'best interests' of the child, which may give inadequate protection to the future interests of the child.

This paper compares the legal provisions in Australia and India. As the renowned Australian jurist Michael Kirby stated, 'there are many basic similarities between the Indian and the Australian legal systems',[10] both are common law systems, have similar legal classifications, and are developing the concept of informational privacy. The 'best interests of the child' is used as the legal framework for decision-making for children in both jurisdictions, since both India and Australia have ratified the United Nations Convention on the Rights of the Child. In both countries, the use of the internet and sharing of information on social media is prolific and developed health systems use modern therapies to manage T1D in children. So, it is fruitful to consider the legal response to the sharing of a child's health data in both countries.

II. Obligations of Healthcare Professionals

A. Privacy

The fundamental right, or concept, of privacy guards against government and non-state actors' intrusions into personal liberty, providing protection against "invasion into the sanctity of a person's home or an intrusion intopersonal security"[11] and allowing "individuals to make autonomous

BMC Health Services Research 442.

[10] Michael Kirby, 'Book Review: Shaun Star (Ed), Australia and India: A Comparative Overview of the Law and Legal Practice' <https://www.michaelkirby.com.au/sites/default/files/speeches/2832%20-%20BOOK%20REVIEW%20-%20AUSTRALIA%20AND%20INDIA%20-%20A%20COMPARATIVE%20OVERVIEW%20OF%20THE%20LAW%20AND%20LEGAL%20PRACTICE.pdf>.

[11] K.S. Puttaswamy v Union of India (2017) 10 SCC 1, 508 (Chandrachud J).

life choices."[12] Privacy addresses the issue of who has access to personal information[13] and its collection, storage and use. Privacy legislation deals with the handling of personal information about individuals. Health data is sensitive and personal and it is accorded the highest degree of protection in legislative frameworks in Australia and India.

In Australia, privacy of medical data is regulated by the federal and the state laws. The Privacy Act, 1988 (Commonwealth) imposes legal obligations on the use and disclosure of health information. 'Health information', defined in Section 6 FA of the Privacy Act can be used or disclosed for the primary purpose for which it is collected. It can also be disclosed between members of the treating team or to the patient's general practitioner. Healthcare professionals are required to comply with the Australian Privacy Principles[14] in relation to the collection, storage, use and disclosure of personal data. The Privacy Act does not provide for any substantive remedies, rather the Office of the OAIC deals with complaints about mishandling of personal data. Australian privacy legislation imposes duties on governmental organisations and agencies, but it does not apply to individuals who are merely conducting their personal, family or household affairs.[15]

State legislations such as the Health Services Act, 1988 (Vic) and the Health Records Act, 2001 (Vic) impose obligations not to share information, unless it is for the provision of health services or it is shared with a body recognised as authorised to receive that information. The Health Records Act, 2001 regulates health information collected and handled in Victoria by the Victorian public sector and the private sector. However, the Act does not apply to health information if used/disclosed only in connection with personal, family or household affairs (Section 13). In Australia, therefore, parents are not constrained by statutory obligations in respect of disclosure of their children's health data.

As for India, privacy protection for health data has been addressed by recent legislative proposals. The Draft Digital Information Security in Healthcare Act ('DISHA') provides an individual with a say in what happens with their data.[16] There are provisions requiring consent or refusal at every

---

[12] ibid 634 (Sanjay Kishan Kaul J).

[13] Institute of Medicine, Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health through Research (Sharyl J Nass, Laura A. Levit and Lawrence O. Gostin eds, National Academies Press 2009).

[14] Australian Privacy Principles <https://www.oaic.gov.au/privacy/australian-privacy-principles/> accessed 29 April 2020.

[15] Privacy Act 1988 (Cth), s 16.

[16] Digital Information Security in Healthcare Act 2018 (DISHA 2018), s 28.

stage of processing –generation, collection, storage, transmission, access and disclosure. An individual can withdraw consent for storage and transmission of his or her data. In addition to this is the requirement for explicit prior permission for every use of data in an identifiable form.[17] Under DISHA, non-consent-based processing under a law is only allowed for using, accessing or disclosing data for the limited purposes specified under DISHA, such as advancing the delivery of patient care or improving public health activities.[18] Section 28 of DISHA recognises that the owner of the data shall have rights to privacy, confidentiality, and security of the data.

Additionally, the Ministry of Electronics and Information Technology is in the process of enacting the Personal Data Protection Bill, 2019 ('PDP Bill') which would be applicable in all domains including health, and which would subsume DISHA. The PDP Bill defines 'sensitive personal data' as including heath data.[19] Chapter IV of the Bill specifically deals with the sensitive personal data of children.[20] The personal data of a child must be processed in such manner that protects the rights of, and is in the best interests of, the child.[21] The PDP Bill introduces the concept of a fiduciary relationship into Indian privacy jurisprudence. A 'data fiduciary' is defined as any person, including the State, a company, any juristic entity or any individual who alone or in conjunction with others determines the purpose and means of processing of personal data (Section 3(13)).

The relationship between entities processing personal data ('data fiduciaries') and individuals ('data principals') is based on a fundamental expectation of trust. In their Working Paper (No. 4),[22] the Data Governance Network argues that the PDP Bill imposes duties that are akin to traditional fiduciary obligations, but that 'fiduciary framing in the PDP Bill appears largely cosmetic'[23] and adds little to the law. The authors conclude that the use of the fiduciary concept does not implement any particularly novel rights or duties when compared to non-fiduciary based privacy frameworks such as the European General Data Protection Regulation. I consider below the

[17] DISHA 2018, s 28(8)(b).
[18] DISHA 2018, s 29.
[19] Personal Data Protection Bill 2019 (PDP Bill 2019), s 3(36)(ii).
[20] PDP Bill 2019, s 16.
[21] ibid.
[22] Rishab Bailey and Trishee Goyal, 'Fiduciary Relationships as a Means to Protect Privacy: Examining the Use of the Fiduciary Concept in the Draft Personal Data Protection Bill, 2018' (2019) Data Governance Network Working Paper 04 <https://datagovernance.org/files/research/NIPFP_Rishab_Trishee_fiduciaries_-_Paper_4.pdf>.
[23] ibid 63.

concept of fiduciary duties owed by parents to their children and whether this could frame an obligation not to disseminate their child's health data.

A number of statutes in India recognise and give effect to confidentiality in specific areas of healthcare, including mental health treatment,[24] termination of pregnancy,[25] and biomedical research.[26] Nevertheless, there is currently no concrete statutory mechanism in place to secure health data in whatever context it arises.The DISHA still has not yet become effective in India and the PDP Bill is currently pending before a Parliamentary Committee.

In addition to the protections afforded byprivacy legislation, the common law in India and Australia has recognised the importance of the right to control dissemination of personal information. India has recognised privacy as a constitutionally protected right under Article 21 of the Constitution of India, which provides, "No person shall be deprived of his life or personal liberty except according to procedure established by law". The Supreme Court of India in K.S. Puttaswamy v Union of India[27] reasoned that "privacy is an incident of fundamental freedom or liberty. Privacy is the ultimate expression of the sanctity of the individual. It is a constitutional value which straddles across the spectrum of fundamental rights and protects for the individual a zone of choice and self-determination."[28]

The right to privacy includes protection against State interference as well as the positive right to be protected by the State. In Puttaswamy, the Court recognised that this right encompasses protection of personal information, including the right to control the dissemination of health records.[29] Justice Bobde, in his judgment, observed that consent was essential for distribution of inherently personal data such as health records. The Court noted that individuals have a reasonable expectation of privacy in certain circumstances and that medical information would be a category to which a reasonable expectation of privacy attaches.[30] The right to privacy is not absolute, however, and a restriction on the right to privacy must be provided by a just, fair and reasonable law; it must correspond to a legitimate aim of the State and must be proportionate to the objective it seeks to achieve.

---

[24] Mental Health Act 1987, s 13.
[25] Medical Termination of Pregnancy Regulations 2003, s 5(3).
[26] National Ethical Guidelines for Biomedical and Health Research Involving Human Participants 2017.
[27] K.S. Puttaswamy (n 12).
[28] ibid 432.
[29] "An unauthorised parting of the medical records of an individual which have been furnished to a hospital will amount to an invasion of privacy." K.S. Puttaswamy (n 12) 438.
[30] ibid 436.

In addition to the statutory protections against the misuse of personal information, healthcare professionals' disclosure of health data is constrained by the common law duty of confidentiality. The duty is owed in respect of confidential information received in the context of their professional relationship. In the Spycatcher[31] case, Lord Goff accepted the broad general principle that,

> "a duty of confidence arises when confidential information comes to the knowledge of a person (the confidant) in circumstances where he has notice, or is held to have agreed, that the information is confidential, with the effect that it would be just in all the circumstances that he should be precluded from disclosing the information to others."[32]

This is characterised as a public interest in confidential medical care,[33] which enables and encourages full disclosure of health conditions to promote best care.

Prior to the Puttaswamy judgment, the High Courts in India made important pronouncements on the law on breach of confidence, where the duty arises across a range of contexts. In Surupsingh Naik v. State of Maharashtra,[34] the Bombay High Court recognised confidentiality in the medical records of a patient, framed through the Indian Medical Council Code of Ethics, but held that the obligation of confidentiality was overridden by the provisions of the Right to Information Act. The case of 'X' v. Hospital 'Z'[35] concerned a hospital divulging the HIV status of a patient to his family, which then reached his fiancée's family. A breach of the duty of confidentiality was pleaded as a ground for damages. Although the Supreme Court of India recognised the right to privacy/confidentiality, this was in conflict with the fundamental right of another to be informed about the 'dangerous' disease which was a threat to her life. Thus, the right to be informed overrode the right to confidentiality.

Australian common law gives effect to the equitable duty of confidence.[36] The basis for a tortious claim for invasion of privacy has been reviewed by the courts. The decision of the High Court of Australia in Victoria Park Racing

---

[31] Attorney General v Guardian Newspapers Ltd (No 2) [1990] 1 AC 109 : [1988] 3 WLR 766 (Spycatcher case).
[32] ibid 805.
[33] Recognised in the Spycatcher case and General Medical Council, 'Confidentiality: Good Practice in Handling Patient Information' (2017) para 22.
[34] 2007 SCC OnLine Bom 264 : AIR 2007 Bom 121.
[35] (1998) 8 SCC 296 : AIR 1999 SC 495.
[36] Smith Kline and French Laboratories v Department of Community Services and Health [1990] FCA 206; 17 IPR 545.

& Recreational Grounds Co Ltd v. Taylor[37] was considered an authority for the view that there is no common law right to privacy in Australia. In 2001, however, the Court was invited to depart from old authority and recognise a tort of invasion of privacy. In Australian Broadcasting Corp v. Lenah Game Meats Pty Ltd,[38] Gleeson CJ noted that,

> "It seems to me that, having regard to current conditions in this country, and developments of the law in other common law jurisdictions, the time is ripe for consideration whether a tort of invasion of privacy should be recognised in this country, or whether the legislatures should be left to determine whether provisions for a remedy for it should be made."[39]

In its 2014 Report titled 'Serious Invasions of Privacy in the Digital Era',[40] the Australian Law Reform Commission ('ALRC') recommended a new tort of serious invasion of privacy, which would be actionable only where a person in the position of the plaintiff would have a reasonable expectation of privacy in all the circumstances.[41] As recognised in Giller v. Procopets,[42] the "development of such a tort would require resolution of substantial definitional problems."[43] The ALRC recommendations have not been implemented.[44]

B. Guidance from Professional Bodies

Healthcare professionals' use and disclosure of information of a child patient's data is controlled through privacy legislation and common law duties of confidentiality. In addition, codes of practice recognise that confidential information must be protected. In the United Kingdom ('UK'), the General Medical Council ('GMC') professional guidance'0–18 years: guidance for all doctors'[45] identifies the professional duty of confidence owed to children: respecting patient confidentiality is an essential part of good care;

---

37 (1937) 58 CLR 479.
38 [2001] HCA 63.
39 ibid [335] (Gleeson CJ).
40 Australian Law Reform Commission, Serious Invasions of Privacy in the Digital Era (Final Report 123, 2014).
41 ibid Recommendation 6.
42 (2008) 24 VR 1.
43 ibid [167] (Ashley JA).
44 The Australian Competition and Consumer Commission has recommended that a new statutory cause of action be created to cover serious invasions of privacy. Australian Competition and Consumer Commission, Digital Platforms Inquiry: Final Report (2019) <https://www.accc.gov.au/publications/digital-platforms-inquiry-final-report> accessed 2 June 2020.
45 General Medical Council, '0-18 Years: Guidance for All Doctors' (2018).

this applies when the patient is a child or young person as well as when the patient is an adult (para 42).

Nevertheless, the child's health information will need to be shared with parents where the child is too young to be able to make healthcare decisions, in order that parents can exercise their parental responsibilities in the child's best interests. For older children who do have decision-making capacity, GMC guidance 'Confidentiality: good practice in handling patient information'[46] identifies the importance of their autonomous choice about who their health information is shared with. Teenagers may be particularly concerned about keeping confidential information from their parents, schools, children's services, the police and other statutory agencies (para 29).

The Medical Board of Australia's guidance 'Good Medical Practice: A Code of Conduct for Doctors in Australia'[47] provides that 'patients have a right to expect that doctors and their staff will hold information about them in confidence, unless release of information is required by law or public interest considerations' (para 4.4). It provides no particular guidance in respect of children's data. The Australian Medical Association's Code of Ethics[48] states that doctors should maintain the confidentiality of the patient's personal information including their medical records, disclosing their information to others only with the patient's express up-to-date consent or as required or authorised by law (para 2.2.2).

The Medical Council of India, replaced in September 2020 by the National Medical Commission, is the chief regulating body in India that governs doctors. Through the Indian Medical Council (Professional conduct, Etiquette and Ethics) Regulations, 2002, it seeks to govern the ethical conduct of doctors in India. Physicians are obliged to protect the confidentiality of patients with regard to all aspects of the information provided by the patient to the doctor, including information relating to their personal and domestic lives. The only exception to this mandate of confidentiality is if the law requires the revelation of certain information, or if there is a serious and identifiable risk to a specific person and/or community of a notifiable disease. The Regulations do not include any provision relating to confidentiality of children's data.

---

[46] General Medical Council, 'Confidentiality: Good Practice in Handling Patient Information' (2017).

[47] Medical Board, Australian Health Practitioner Regulation Agency, 'Good Medical Practice: A Code of Conduct for Doctors in Australia' (2020).

[48] Australian Medical Association, Code of Ethics (2016).

Broadly speaking, a child's health data can be disclosed only for the purpose of the child's healthcare or where there is an overriding public interest in sharing that information. Guidance issued by professional bodies which regulate healthcare professionals underscores the importance of appropriate sharing of a child's health data.

III. Obligations of Parents

Exchange of a child's health data between parents and healthcare professionals who care for the child demands legal and ethical obligations of healthcare professionals to not disseminate that information further, which are clearly identified in legislation, common law duties and professional guidance. However, it is less clear what obligations parents owe in respect of sharing their children's information with others, such as relatives, or on social media. Once data has been shared, parents, and indeed the child, lose control over it. In the following section, I consider the spectrum across which parents share their child's data,on closed social media sites and publicly available sites such as Instagram, and the nature of that data – social and health data. I consider the legal framework which may be appropriate to regulate 'sharenting', and endeavour to identify a point on a spectrum where parents may be considered appropriate to share their child's data.

A. 'Sharenting'

Internet usage trends are similar for India and Australia and research demonstrates prolific use of social media sites in both countries. Indians now downloads more apps than residents of any other country – over nineteen billion apps were downloaded by Indian users in 2019. Facebook is the most popular social networking site in India, with about 270 million users, and India has the largest Facebook user base in the world.[49] The average Indian social media user spends seventeen hours on such platforms each week. It is estimated that in 2021, there will be around 448 million social network users in India.

Parents readily share information about their children on social media. This concept has been termed 'sharenting.'[50] Research commissioned by Nominet in the UK in 2015 found that on average, 973 photos are posted online by a child's fifth birthday, equating to an average of 195 photos shared

---

[49] 'Digital and Social Media Landscape in India' <>.

[50] Stacey B. Steinberg, 'Sharenting: Children's Privacy in the Age of Social Media' (2017) 66 Emory Law Journal 839.

by parents every year.[51] 'Sharenting' is prevalent in both India and Australia. In 2018, McAfee commissioned market research firm OnePoll to conduct a survey of one thousand parents of children aged one month to sixteen years old, across Mumbai, Delhi and Bengaluru. The survey revealed that 40.5% of parents in India (mostly from Mumbai) post a photo or video of their child at least once a day on social media, while 36% post their child's picture once a week.[52] Although 55% of parents only share images of their child on private social media accounts, 42% share images on public social media accounts. Similarly, McAfee conducted a survey of 1000 Australian parents (of children aged from one month to sixteen years old), which found that 30% of them post a photo or video of their child at least once a week on their social media accounts, and 12% post at least once a day.[53]

Holiday and birthday photos which provide information about a child's height, location, age, hair, and eye colour may seem innocuous enough but are items of identifying information, which help piece together a child's profile. There are potential harms of sharing such information. "Personal data are now used to construct profiles of people that can have major implications for their life opportunities, such as their access to employment, travel, health and life insurance and credit."[54]_[55] If mere 'social' information can have implications for the future interests of the child, then inappropriate disclosure of health information by parents will have an even greater impact. Steinberg has noted that 'sharenting includes a moral obligation to act with appropriate discretion and with full regard for the child's safety and well-being'[56] and that 'the individuals responsible for sharing the children's information are the same people tasked with protecting the children's privacy – the parents.'[57]

---

[51] 'Todays' Children will Feature in Almost 1,000 Online Photos by the Time They Reach Age 5' (Nominet, 26 May 2015) <https://www.nominet.uk/todays-children-will-feature-in-almost-1000-online-photos-by-the-time-they-reach-age-five/>.

[52] 'Sharenting: Oversharing Your Child's Pictures Online isn't just Risky but Unhealthy too' (The Indian Express, 2 August 2019) <https://indianexpress.com/article/parenting/family/sharenting-oversharing-child-pictures-online-privacy-individuality-safety-5871819/>.

[53] <https://www.nowtolove.com.au/parenting/expert-advice/sharing-photos-children-online-safety-50776>.

[54] Deborah Lupton, Sarah Pedersen and Gareth M. Thomas, 'Parenting and Digital Media: From the Early Web to Contemporary Digital Society' (2016) 10(8) Sociology Compass 730, 736.

[55] Jessica Baron, 'Posting about Your Kids Online Could Damage their Futures' (Forbes, 16 December 2018) <https://www.forbes.com/sites/jessicabaron/2018/12/16/parents-who-post-about-their-kids-online-could-be-damaging-their-futures/#1dcab34a27b7> accessed 30 April 2020.

[56] Steinberg (n 51) 882.

[57] ibid 883.

Bessant notes that parents are considered 'gatekeepers' of their children's personal information and, therefore, the best people to decide with whom to share that information.[58] However, she recognises that, in the context of sharenting, "a conflict of interests exists between parents, and their rights to freedom of expression and respect for family life, and their child's right to privacy."[59]

B. Reasonable Expectation of Privacy

The Court in Puttaswamy noted that, "the lives which individuals lead as members of society engender a reasonable expectation of privacy."[60] This reasonable expectation of privacy 'ensures that while on the one hand, the individual has a protected zone of privacy, yet on the other, the exercise of individual choices is subject to the rights of others to lead orderly lives.[61] In R. Rajagopal v. State of T.N., the Supreme Court recognised the importance of securing a person's privacy and that of his family.[62] Data such as medical information would be a category to which a reasonable expectation of privacy attaches. So, how are the freedoms of parents to share information about their children on social media sites constrained by their child's reasonable expectation of privacy?

Two important cases which have considered relevant principles of a reasonable expectation of privacy were concerned with well-known celebrities, namely the UK House of Lords decision in Campbell v. MGN Ltd[63] and the decision of the European Court of Human Rights in Von Hannover v. Germany.[64] In Von Hannover, the Court considered that an individual's private life can include ordinary activities, such as family holidays or expeditions, which are not public in any sense beyond the fact that they are conducted in a street or some other public place.[65]

In Murray v. Big Pictures (UK) Ltd[66] brought on behalf of JK Rowling's young son, concerning publication of his photos taken in a public place, the Court of Appeal restated the application of reasonable expectation to the privacy interests of children. The Court noted,

---

[58] Claire Bessant, 'Sharenting: Balancing the Conflicting Rights of Parents and Children' (2018) 23(1) Communications Law 7.
[59] ibid 7.
[60] K.S. Puttaswamy (n 12) [169].
[61] ibid.
[62] R. Rajagopal v State of T.N. (1994) 6 SCC 632 : AIR 1995 SC 264 [26].
[63] [2004] 2 AC 457 : [2004] 2 WLR 1232 : [2004] UKHL 22.
[64] [2005] 40 EHRR 1.
[65] ibid [45] (Tomlinson LJ).
[66] [2008] EWCA Civ 446.

> "The origin of the cause of action relied upon is breach of confidence, since information about an individual's private life would not, in ordinary usage, be called 'confidential', the more natural description of the position today is that such information is private and the essence of the tort is better encapsulated now as misuse of private information."[67]

The Court of Appeal in Murray concurred with the view of the trial judge, that the purpose of the claim is to carve out for the child some private space in relation to his public appearances. It considered that small children may have a reasonable expectation of privacy in respect of 'routine acts such as a visit to a shop or a ride on a bus',[68] depending upon the circumstances. There is no guarantee of privacy, however. The judicial approach in the UK is to recognise a reasonable expectation of privacy, as an aspect of a right to private and family life under Article 8 of the European Convention on Human Rights. The autonomy that Article 8 protects is qualified by the fact that very young children lack the capacity to exercise it. How the parents choose to conduct their family life with the child has an impact on the child's reasonable expectation of privacy. Thus, if parents choose to bring a young child onto the red carpet at a premiere or awards night, it would be difficult to see how the child would have a reasonable expectation of privacy or how Article 8 would be engaged. In such circumstances, the parents have made a choice about the child's family life and the type of interactions that it will involve. A child's reasonable expectation of privacy must be seen in light of the way in which his family life is conducted.[69]

Thus, a child's reasonable expectation of privacy is constrained by the actions of the parents, who may effectively waive that right of the child by their actions in exposing information about the child in a public sphere. A child may have a reasonable expectation of privacy in relation to information, whether photos or medical data, that parents share on social media. If a parent uploads a photo of their child on a social media site, could this be considered to have effectively waived a child's reasonable expectation of privacy? There is a need to strike a balance between the rights of young people under Article 8 and the rights of parents to determine how they lead their lives under Article 8[70] (and the right to freedom of expression under Article 10).[71] The exercise of parental powers and duties must be in the child's best

---

67 ibid [24] (Sir Anthony Clarke MR).
68 ibid [56].
69 Weller v Associated Newspapers Ltd [2015] EWCA Civ 1176 [33] (Dingemans J).
70 R v Secy of State for Health [2006] QB 539 : [2006] 2 WLR 1130 : [2006] EWHC 37 (Admin).
71 The cases considered in this article have balanced the child's rights under Article 8 with the right of newspapers to freedom of expression under Article 10.

interests and, "in the overwhelming majority of cases, the best judges of a child's welfare are his or her parents".[72] However, although a child's right is not a trump card in the balancing exercise, the primacy of the best interests of a child means that, where a child's interests would be adversely affected, they must be given considerable weight.[73] If claims are brought by children for sharenting, it will be interesting to see the judicial approach in balancing the interests of the children and those of the parents.

When the ALRC considered 'Serious Invasions of Privacy in the Digital Era', Professor Butler made a submission that where 'the plaintiff is a child of vulnerable age, there would normally be a high expectation that he or she is entitled to a measure of privacy'.[74] The ALRC acknowledged that the nature of the relationship between the parties to an action is relevant – noting that 'there do not appear to be many cases in which a person has brought an action for invasion of privacy against his or her spouse, partner or other family member. It would generally not be reasonable to expect the same level of privacy from partners and family members.'[75] As stated above, the proposal for a tort of invasion of privacy has not been progressed in Australia.

C. Overarching Duty of Parents to Act in their Child's Best Interests

Article 3 of the United Nations Convention on the Rights of the Child gives children the right to have their best interests assessed as a primary consideration in all actions or decisions that concern them, in both the public and private sphere. States parties to the Convention must ensure the application of, and respect for, the best interests of the child in judicial and administrative decisions and all other actions concerning the child as an individual. Both India and Australia have ratified the Convention. 'Best interests' is the framework through which parents and healthcare professionals must make decisions in respect of a child, recognised in legislation and common law.

In India, Section 8 of the Hindu Minority and Guardianship Act, 1956, provides that the natural guardian of a Hindu minor has the power to do all acts which are necessary or reasonable and proper for the benefit of the minor or for the realization, protection or benefit of the minor's estate. Section 89 of the Indian Penal Code, 1860, provides for parents being able to take medical decisions for children under 12 years of age, in good faith

---

[72] Gillick v West Norfolk and Wisbech Area Health Authority [1986] AC 112 : [1985] 3 WLR 830, 173 E (Lord Fraser).
[73] Weller (n 70) [40] (Dingemans J).
[74] Des Butler, Submission 10 in Australian Law Reform Commission (n 41).
[75] Australian Law Reform Commission (n 41) para 6.81.

for the benefit of the child. Legislation utilises the best interests of the child approach in matters such as juvenile justice,[76] adoption[77] and mental health.[78] The paramount consideration of the welfare of the child has been recognised in numerous custody cases in India,[79] and the protection of child welfare.[80]

The High Court of Australia in Secy. of the Department of Health and Community Services v. JWB[81] stated that the 'the overriding criterion of the child's best interests is itself a limit on parental power.' Commonwealth and State legislation provides for court intervention where parental powers are not exercised in the child's best interests.[82]

The Children Act, 1989 in England and Wales, with similar provisions in the Children (Scotland) Act 1995, provides that 'parental responsibility' means all the rights, duties, powers, responsibilities and authority which by law a parent of a child has in relation to the child and his property (Section 3). Case law demonstrates the leeway accorded to parents in making health decisions. A court would interfere with decisions of the parent where they are incongruent with the welfare of the child.[83]

The best interests of the child is, therefore, the legal standard by which parents are enabled, and ultimately may be constrained, in disclosure of the child's health data.

D. Health Data Shared with Healthcare Professionals

The sharing of a child's health data between parents and the team of health and social care professionals caring for the child is in the child's best interests, where the child is too immature to make his/her own healthcare decisions. This enables parents to have enough information about their child's health condition in order to exercise their parental responsibilities while making treatment decisions. Lord Templeman in Gillick said that, "confidentiality owed to an infant is not breached by disclosure to a parent responsible for that infant, if the doctor considers that such disclosure is necessary in the

---

[76] The Juvenile Justice (Care and Protection of Children) Act 2015.
[77] Central Adoption Resource Authority Regulations 2017.
[78] Mental Healthcare Act 2017.
[79] Mumtaz Begum v Mubarak Hussain 1986 SCC OnLine MP 11; Kirtikumar Maheshankar Joshi v Pradipkumar Karunashanker Joshi (1992) 3 SCC 573; Kanika Goel v State of Delhi (2018) 9 SCC 578.
[80] Aruna J. Kashyap and Pratibha Menon, 'Demystifying the Best Interests Principle in India' <https://www.cry.org/resources/pdf/NCRRF/Aruna_&_Pratibha_2007_Report.pdf>.
[81] [1992] HCA 15 : (1992) 175 CLR 218.
[82] For example, The Children, Youth and Families Act (Vic) 2005.
[83] Ashya King, In re [2014] EWHC 2964 (Fam).

interests of the infant."[84] Without such exchange of information, the healthcare professional would be hampered in exercising his/her duty of care owed to the child. It is clear from Gillick that older children, who are able to make choices about medical treatment, must give consent for their health data to be shared with their parents.

In Z, In re,[85] the Court of Appeal stated that not only medical staff, but parents too owe a child a duty of confidentiality. Data from a CGM is confidential in nature. Parents share this information with the healthcare professionals treating the child, for the purpose of monitoring and managing the child's T1D, and in this way it is an exercise of the parents' duty to act in the child's best interests.

E. Health Data Shared with Family

Often parents also share their child's health data with others, who are not subject to the same legal obligations as healthcare professionals. Parents disclose information about their child's health to family and friends, in many forms – verbally, by text and emails, and through social media. Parents are under legal and moral obligations to act in their child's best interests by virtue of their role as caregivers and decision-makers for their children.

A child's health data that is shared with family and close friends could be conceived as an aspect of sharing in the child's best interests. If the child becomes ill, family and friends may then step in to look after the child, for which they will need to realize the signs of illness that prompt a need to call for medical services. It is natural, therefore, for parents to share information about their children with those close to them, for support, and to spread any burden of concern. Herring frames this as relationship-based welfare; the interests of the child and parents/caregivers are intertwined, so that the best interests of the child and the parents, although not the same, can point in the same direction. His relationship-based welfare approach recognises that children are raised in relationships and that the best way of promoting a child's welfare is to ensure that the child is brought up in healthy relationships.[86] "Supporting the child means supporting the care-giver and supporting the care-giver means supporting the child."[87]

---

[84] Gillick (n 73).
[85] Z, In re [1997 Fam 1 : [1996] 2 WLR 88 : [1995] 4 All ER 961.
[86] Jonathan Herring, 'Farewell Welfare?' (2005) 27(2) Journal of Social Welfare and Family Law 159, 166.
[87] ibid.

It could be expected that family members and close friends, who are privy to the health data of a child provided by the parents, receive it in the expectation that it will not be spread widely. We can imagine the justified outrage of parents who discover that a family member has been talking about the child's glucose readings to their friends or posting that information on Instagram. Similarly, a parent sharing their child's health data very widely, with an extensive number of friends, would not be acting in the child's best interests, nor would it fall within the concept of relational welfare. It may also have the unwanted effect of the child's medical information no longer remaining confidential.

F. Appropriate Sharing on the Spectrum of Parental Disclosure

Just because there is an increase in the number of parents who disclose social information about their child on social media sites, does not mean that sharenting is always acceptable. Where parents share information about the social lives of their children, with the intent of connecting with their communities and perhaps showing off the attributes of the child, any possible future harm accruing to the child could be outweighed by the important social need of allowing flexibility in parenting. However, as Steinberg notes, "disclosures online may harm their children, whether intentionally or not."[88] It is difficult to see how a parent posting a child's health data on social media sites, which are publicly accessible, serves any benefit to the child. Not only do parents lose dominion over that information, with the possibility that it may be manipulated and shared out of context, but it may lead to future harms, such as loss of future employment opportunities because of a known health condition or difficulty in getting insurance cover.[89],[90]

In comparison, parents sharing health data with healthcare professionals, family and close friends and even on closed social media sites, for the purpose of supporting the management of the child's health condition, could be considered a proper exercise of parental responsibility in the child's best interests.

---

[88] Steinberg (n 51) 843.

[89] Diabetes Australia states that people with diabetes (and many other health conditions) can expect to pay additional costs or premiums compared to someone without a health condition. 'Insurance and Diabetes' <https://www.diabetesvic.org.au/Insurance-and-diabetes> accessed 2 June 2020.

[90] Steinberg (n 51) 849. He notes that data brokers build profiles about people and sell them to employment agencies and college admission offices.

G. Parents as Fiduciaries

Conceptualising parents as owing fiduciary duties may lead to a different approach in identifying appropriate boundaries for sharenting. In Hospital Products Ltd v. United States Surgical Corp,[91] Gibbs CJ stated that fiduciary relationships are sometimes referred to as relationships of trust and confidence, although an actual relation of confidence is 'neither necessary for nor conclusive of the existence of a fiduciary relationship.'[92] Fiduciary relationships are recognised in equity as those relationships where there is an inequality or power differential between the parties, relevant to 'socially or economically important or necessary interactions of high trust and confidence creating implicit dependency and peculiar vulnerability.'[93] In CBSE v. Aditya Bandopadhyay,[94] the Supreme Court of India referred to a fiduciary as someone "having the duty to act for the benefit of another, showing good faith and candour, where such other person reposes trust and special confidence in the person owing or discharging the duty."

Established categories of fiduciary relationships include trustee and beneficiary, agent and principal, solicitor and client, employee and employer, where economic interests are of concern. The critical feature of fiduciary relationships is 'that the fiduciary undertakes or agrees to act for or on behalf of or in the interests of another person in the exercise of a power or discretion which will affect the interests of that other person in a legal or practical sense.'[95]

Could parents owe fiduciary duties to their children, and if so, what impact might that have on a fiduciary obligation not to misuse their power in disclosing their children's health data? According to Smith,

> "the characterization of the parent as a fiduciary towards their child captures a central, indeed a defining, element of the parent-child relationship, which is also a characteristic element of all established fiduciary relationships: namely, the possession of legal powers that are held in a managerial or other-regarding capacity, for the benefit of another person."[96]

---

91 (1984) 156 CLR 41.
92 ibid [31].
93 Leonard I. Rotman, 'Fiduciary Law's "Holy Grail": Reconciling Theory and Practice in Fiduciary Jurisprudence' (2011) 91(3) Boston University Law Review 921.
94 (2011) 8 SCC 497.
95 Hospital Products Ltd (n 92) [68] (Mason J).
96 Lionel Smith, 'Parenthood is a Fiduciary Relationship' (2020) 70 University of Toronto Law Journal 395.

Canadian Courts, have recognised a fiduciary relationship between parent and child, drawing on indicia of a fiduciary relationship; power and vulnerability, confidence and reliance. In K.M. v. H.M., La Forest J said, "even a cursory examination of these indicia establishes that a parent must owe fiduciary obligations to his or her child. Parents exercise great power over their children's lives and make daily decisions that affect their welfare. In this regard, the child is without doubt at the mercy of her parent."[97]

The 'unique focus' of the parental fiduciary duty as considered in KLB v. British Columbia is 'the duty to act loyally, and not to put one's own or others' interests ahead of the child's in a matter that abuses the child's trust.'[98] In the 1992 decision Secy of the Department of Health and Community Services v. JWB,[99] the High Court of Australia recognised a fiduciary relationship between parent and child. McHugh stated that, "in principle, a parent can have no authority to act on behalf of his or her child where a conflict arises between the interests of the parent and the interests of the child."[100]

Breach of parental fiduciary duties have been considered in the context of parental sexual abuse,[101] and has been conceived as the parent taking advantage of the relationship of trust for their own gain. Admittedly, parents posting their children's health data on social media sites, may not be considered to provide a gain for the parent, but it could definitely be considered an action which violates the trust of the children, and betrays their future interest in open possibilities for employment and insurance cover. As Joyce notes, 'doubtless the imposition of fiduciary duties upon parents will require difficult line-drawing.'[102] Traditionally, Australian courts have drawn a line between economic and non-economic interests, refusing to use fiduciary law to protect non-economic interests.[103] However, this distinction may not be so easy to maintain, given that harm to the integrity of the child's identity may lead to future economic harms. Joyce, again, considers that the distinction 'is arbitrary, and pays insufficient regard to the central concept of fiduciary obligations: the wrongful pursuit of self-interest or rival interests.'[104]

The concept of a fiduciary relationship giving rise to a duty of care on those using an individual's data has been recognised in the PDP Bill in India.

---

[97] K.M. v H.M. 1992 SCC OnLine Can SC 90 : (1992) 96 DLR (4th) 289, 325.
[98] KLB v R 2003 SCC OnLine Can SC 51 : [2003] 2 SCR 403, 230 DLR (4th) 513, [48]-[49].
[99] (1992) 175 CLR 218.
[100] ibid [19].
[101] K.M. (n 98).
[102] Richard Joyce, 'Fiduciary Law and Non-Economic Interests' (2002) 28(2) Monash University Law Review 239, 249.
[103] ibid.
[104] ibid 266.

Whether children's trust in their parents appropriately sharing their data can be given effect through the concept of fiduciary duties remains to be seen, but the use of injunction for breach of equitable duty may provide a remedy, whereas a claim in tort for negligence against the parent would be hard to substantiate and provide no financial benefit.

H. Children's Right to an Open Future

In Australia, there has recently been an emphasis on the safety of children in respect of their own online activity. In 2016, the Office of the Australian Information Commissioner (OAIC) published 'Privacy Tips for Parents and Carers' which emphasise that "children need to know that their digital footprint can last forever. They also need to understand that every piece of content they consume, share, upload, and download leaves a digital trace."[105] They advise parents that "sharing personal information online can be risky and it's important to educate your children on how to make good decisions and limit those risks."[106]

The Court in Puttaswamy recognised the scope of technology in creating a digital biography, and noted that,

> "technology results almost in a sort of a permanent storage in some way or the other making it difficult to begin life again giving up past mistakes. People are not static, they change and grow through their lives. They evolve. They make mistakes. But they are entitled to re-invent themselves and reform and correct their mistakes. It is privacy which nurtures this ability and removes the shackles of unadvisable things which may have been done in the past."[107]

But, it is not just children who should be educated about the risks. Parents can create digital footprints for their children. Above I have argued some legal bases for parental protection of children's interests in a digital world – reasonable expectation of privacy, best interests and fiduciary obligations. Another approach is to debate parental obligations from a philosophical-ethical perspective. Feinberg articulated the concept of a child's right to an open future, i.e. the interests of the child against having important life choices determined by others before he/she has the ability to make them for him/herself.[108] A digital biography created in childhood may have the effect of

---

[105] 'Ten Privacy Tips for Parents and Carers' (Office of the Australian Information Commissioner, 2016) <-parents-and-carers.pdf> accessed 1 June 2020.

[106] ibid 5.

[107] K.S. Puttaswamy (n 12) [484].

[108] Joel Feinberg, 'The Child's Right to an Open Future' in William Aiken and Hugh LaFollette (eds), Whose Child?: Children's Rights, Parental Authority, and State Power (Rowman and

limiting that person's future life choices about employment and insurance options, and perhaps other restrictions arising from adverse inferences from the digital biography, which are currently unforeseen. Is this sufficiently 'violating conduct' which justifies restrictions on parental actions, and if so how should that be managed?[109]

Parents' decisions to post their child's information on social media sites can make a difference to the quality of that child's future life. Yet parents share pictures and information about their children online, despite understanding the current risks. The Age of Consent Survey commissioned by McAfee in India found that 76% of parents say they have considered the images of their children they post online could end up in the wrong hands.[110] Facebook has Community Standards[111] which identifies objectionable content, but posts which may not seem objectionable in their current form may, amalgamated over a period of time, have greater impact. The restriction of parental autonomy in order to preserve the autonomy rights-in-trust of the child is ethically difficult to justify where the harms are hypothetical. Nevertheless, posting information about a child's chronic health condition could credibly impact his/her future employment and insurance options in the future. Education of parents on the risks and ethical dimensions of their posting behaviour is more appropriate than a prohibitive approach which would demand excessive resources to monitor.

IV. Conclusion

In this paper, I address the obligations of healthcare professionals and parents in respect of sharing and disclosing a child's health data and endeavour to test where limits on sharing are set. Although parents readily share personal information about themselves and their children, the concept of medical privacy remains uniquely important to them. They would expect health care professionals not to disclose their child's health data, and effective regulation of health care professionals through privacy legislation, the common law duty of confidentiality and ethical obligations gives effect to parental expectations. Parents' sharing of their child's health data on open

Littlefield 1980) 124–153.

[109] ibid 126.

[110] Anindita Mishra, 'McAfee Survey: Parents Share Pictures of Their Kids Online, Despite Understanding the Risks Involved' (McAfee, 27 August 2018) <https://www.mcafee.com/blogs/consumer/mcafee-survey-parents-share-pictures-of-their-kids-online-despite-understanding-the-risks-involved/>.

[111] Facebook, 'Community Standards' <https://www.facebook.com/communitystandards/>.

social media sites effectively publishes this information and, thus, undermines the coexistent duties of healthcare professionals.

When parents share their child's data, they lose control over the future dissemination of that information. The increasing rate of 'sharenting' requires a common-sense approach, a reliance that parents generally do act in their child's best interests and as per their moral sense of doing the right thing. Children may have a reasonable expectation of privacy in relation to their social and health data. Parents are probably acting appropriately in sharing the child's health data on closed Facebook sites, where members support one another to leverage best care. The aim of managing their child's health condition better is the justification, and this falls within the ambit of best interests and does not conflict with the parents' fiduciary duties. In contrast, open site sharing of health data undermines the integrity of the child. Pursuit of parental self-interest would point towards a breach of fiduciary obligations owed to the child, however, breach of legal duties is unlikely to be pursued.

Protecting Privacy in India: The roles of consent and fairness in data protection

Mark J Taylor and Jeannie Marie Paterson***

Abstract *The Indian Personal Data Protection Bill 2019 provides a unique approach to balancing the elements of individual consent and fairness-based limitations that are used in data protection regimes in other parts of the world. Drawing on the fundamental values and interests recognised in KS Puttaswamy v. Union of India (2017) and the report of the Committee of Experts, the Bill requires consent of the data subject to data processing, and puts in place standards that consent must meet to be more than a forced formality. Its novelty lies in also proposing substantive obligations of fair and reasonable data processing, and by making organisations responsible, as statutory 'data fiduciaries', for complying with obligations protecting the interests of the data subject. The requirement that processing be fair, also written into European data protection law, is an opportunity to put data controllers under an obligation to protect the interests of data subjects. Data processing ought not to have a negative impact upon an individual's interests, values and freedoms disproportionate to their positive gains. If robustly interpreted and applied, this could be an effective protection against the shortcomings of consent as a safeguard for protecting individual interests. European data protection law has yet to fully embrace this opportunity. If it did, then there would be less pressure to ensure a data subject's consent meets ideal standards of 'free and informed', which is increasingly unrealistic in a modern information society. Considering the merits of these different approaches, with different degrees of relative emphasis upon individual consent and objective tests of fairness, prompts reflection upon the proper function of privacy and data protection legislation within society. Is it purely to enable individual expressions of informational self-determination — irrespective of whether the deal done is a good one? Or does data protection law also have a role in expressing community expectations by promoting norms and standards of fair dealing that are conducive to individual well-being and to civil society as a whole?*

* Associate Professor in Health Law and Regulation, Melbourne Law School, University of Melbourne, Australia.

** Professor, Melbourne Law School, University of Melbourne, Australia.

I. Introduction

Consent is widely used in data protection legislation as a mechanism for authorising use of personal and sensitive data. The significance and function of consent in such legislation can be understood in different ways. It may be understood to have a central role, perhaps *the* starring role: manifesting respect for informational self-determination and data sovereignty. Or, it may rather be understood to form part of an ensemble cast: existing within a broader complex of social norms and expectations; dictating when, and how, people ought to be asked about uses of information but not investing an individual with primary responsibility to safeguard their relevant interests. Of course, these might better describe points on a spectrum than binary opposites. The further toward the 'self-determination' end of the spectrum, then the greater the (neo-liberal) significance attached to individual autonomy and individual rights including potentially trumping social welfare goals. The further to the opposite end, then the more room there is to contextualise (or constrain) individual expressions of self-determination and to accommodate collective (or communitarian) interests. Both approaches require rules around what amounts to valid, as opposed to forced, consent and protections to ensure individuals are free from misrepresentation or coercion. However, we suggest that both approaches are strengthened from some role being given to measures for requiring 'fair' data processing. This requirement goes beyond consent as the primary safeguard for data protection and justifies the role of other broader considerations. These may be more overtly paternalistic,[1] limiting the types of data use consumers may consent to on grounds that they did not genuinely understand the potential risks in the use, or that the use was potentially harmful to them regardless.[2] It may also open up a

[1] 'The doctrine of paternalism justifies intervention by the state contrary to the wishes of the person whom that intervention is designed to benefit': Peter Cartwright, *Consumer Protection and the Criminal Law: Law, Theory, and Policy in the UK* (Cambridge University Press, 2001) 32.

[2] Adams and Brownsword note the paternalistic principle to be a feature of a consumer-welfarist ideology: 'contractors who enter into imprudent agreements may be relieved from

role for more public interest considerations, such as furthering public goods or protecting groups or society, incurred by individuals' present decisions.

We do not need here to determine which of these is the correct approach, or if there is indeed *a* correct approach. We outline the alternatives only to draw attention to some ambivalence within existing privacy and data protection law with regards to the function of consent relative to achievement of the purposes of privacy and data protection. This ambivalence can be seen in *KS Puttaswamy* v. *Union of India* (2017) ('*Puttaswamy*').[3] Here the Supreme Court of India recognised a right to privacy inherent to the constitutional right to liberty to be motivated by an imperative to assure the dignity of the individual.[4] The relationship between privacy, liberty, and a respect for human dignity can, however, be configured in different ways; with different implications for the relevance of individual consent. What is the conceptual connection between privacy and autonomy? Is data protection concerned with privacy or more discrete goals such as security or providing protection to individuals in circumstances where there is a significant imbalance of bargaining power? What is the significance of social norms or collective interests to the protection of human dignity? Answers to these questions are needed to properly contextualise the meaning and function of individual consent within a privacy or data protection regime. However, clear answers are rarely forthcoming.

Despite the ambiguity, the Indian Supreme Court in the *Aadhaar-5 Judge* decision[5] found the constitutionally protected privacy interest to be sufficiently certain to strike down elements of the Aadhaar scheme. The Court found that a compelling public interest might place a reasonable limit on privacy, but some parts of the scheme failed to meet this standard. As a consequence, *irrespective of any consent*, it was not permissible for individuals to contract with private individuals or corporations to enable them to seek authentication via the scheme.[6] Individuals were thus protected from making

---

their bargains where justice so requires. The case for paternalistic relief is at its most compelling where the party is weak or naïve': John N Adams and Roger Brownsword, 'The Ideologies of Contract' (1987) 7(2) *Legal Studies* 205, 212.

3 *KS Puttaswamy v Union of India* (2017) 10 SCC 1 ('*Puttaswamy*').

4 'Dignity is the core which unites the fundamental rights because the fundamental rights seek to achieve for each individual the dignity of existence. Privacy with its attendant values assures dignity to the individual and it is only when life can be enjoyed with dignity can liberty be of true substance. Privacy ensures the fulfilment of dignity and is a core value which the protection of life and liberty is intended to achieve': ibid [107]. See also, in particular, [113], [169].

5 *KS Puttaswamy v Union of India* (2019) 1 SCC 1 ('*Aadhaar-5 Judge*').

6 For further challenge on constitutional grounds see <https://www.hindustantimes.com/india-news/sc-to-hear-pleas-challenging-aadhaar-verdict-on-june-9/story-F0fzhuen7DIhtbhIijNlzM.html>.

bargains perceived to represent an unjustified and disproportionate privacy interference. This position has been changed through statutory reform now to allow voluntary use by private entities.[7] The point thus underlined: there is contestation over the extent to which an individual's ability to consent to uses of data that are objectively perceived to be unfair is to be limited.

These themes were comprehensively explored in the subsequent Report of the Committee of Experts, under the Chairmanship of Justice BN Srikrishna, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians*, submitted to the Ministry of Electronics and Information Technology, Government of India in 2018. This report took as threshold premise that, first, 'the primary value that any data protection framework serves must be that of privacy' and second, 'such a framework must not overlook other values including collective values'.[8] The Committee recommended that consent in this framework should be made meaningful through form and substance requirements imposed on entities seeking consent.[9] In addition, to protect data subjects, substantive obligations to ensure fair and reasonable data processing should be imposed on data controllers, who should be termed 'data fiduciaries'.[10] This protectionist approach is largely implemented in the proposed Indian *Personal Data Protection Bill 2019*.[11] The Bill adopts a substantive standard of 'fair and reasonable' that appears to go beyond that previously seen in data protection legislation as well as adopting the nomenclature of the data fiduciary.

In this article we reflect on the approach taken in the Indian *Personal Data Protection Bill 2019* and the insights it might offer for an understanding of 'fair' processing in other data protection legislation. We consider the potential for a 'fair' processing requirement, particularly when combined with the idea of a data controller as a statutory 'fiduciary', to supplement, and in some cases overtake, even the most robust requirements for a valid consent to data processing. Specifically, we suggest that if operating successfully, a requirement for 'fair' processing may mitigate the need for the

---

7 The Aadhaar and Other Laws (Amendment) Act 2019. For commentary: see 'Lok Sabha Passes Aadhaar Amendment Bill', *The Economic Times* (online, 4 July 2019) <https://economictimes.indiatimes.com/news/politics-and-nation/lok-sabha-passes-aadhaar-amendment-bill/articleshow/70078736.cms>.

8 Committee of Experts under the Chairmanship of Justice BN Srikrishna, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (Report to Ministry of Electronics and Information Technology, Government of India, 27 July 2018) 10 ('*Protecting Privacy, Empowering Indians*').

9 ibid 11.

10 ibid 33.

11 Personal Data Protection Bill 2019 (India) <http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf>.

high threshold for valid consent now set by European data protection law: a substantive restriction on unfair processing might complement, rather than conflict with, consent requirements in ways that allow the standards of valid consent to be less demanding.

In our view, privacy and data protection legislation in Europe can sometimes appear internally conflicted between what might be described as 'market individualist' or 'consumer welfarist' modes, which correlate with the spectrum opposites in approaches to data protection we discussed earlier.[12] A 'market individualist' approach is guided by an ideological commitment to idea that the market place is a site for *competitive* exchange and that individual self-determination is to be respected with minimum judicial intervention. A 'consumer welfarist' approach, on the other hand, will tend to support more interventionist policy. According to Adams and Brownsword,

> [t]he consumer-welfarist ideology stands for a policy of consumer protection, and for the principles of fairness and reasonableness in contract. It does not start with the market-individualist premise that all contracts should be minimally regulated. Rather it presupposes that consumer contracts are to be closely regulated.[13]

While concerned with more than contracts and reasonable consumer expectations, European data protection law displays at times the hallmarks of an individualist mindset. It relies on a robust standard of affirmation, more robust even than that required under contract law, and an individual can choose to accept certain risks with regard to data processing so long as that high threshold of consent is satisfied. At other times, it seems more closely aligned with a consumer welfarist or communitarian mindset. It does, after all, explicitly require that processing must be 'fair', as well as lawful. And, lawful processing does not require consent. It is not even 'first amongst equals' when establishing a legal basis for processing, with various individual and collective safeguards inbuilt to alternatives.

Our argument is that, perhaps ironically, the direction of travel proposed under the *Consumer Data Protection Bill 2019* may be beneficial whether the intent is to support a 'market individualist' *or* a 'consumer welfarist' approach. Placing central reliance on consent can be problematic whichever end of the spectrum you are seeking to support. If consent is the principal

---

[12] For the framing of the values see Roger Brownsword, *Contract Law: Themes for the Twenty-First Century* (2nd edn, OUP 2006) 105–8; Roger Brownsword, 'Individualism, Cooperativism and an Ethic for European Contract Law' (2001) 64(4) *Modern Law Review* 628, 630.

[13] Adams and Brownsword (n 2) 205–23.

safeguard, and the aim is to enable informational self-determination, then the tendency will be toward insisting upon a very high standard for valid consent. We have seen this move within European data protection law under the *General Consumer Data Protection Right* ('*GDPR*').[14] However, the risk is that this provides little real protection to data subjects in advancing and protecting autonomy in practice. This might be because data subjects fail to exercise the right to control uses of their data as intended by the legislation. They may, for example, be overloaded by information or suffer consent fatigue.[15] The role of consent in protecting data subjects may also be undermined by data controllers choosing the other pathways for data use in preference to the arduous requirements for collecting consent. It is equally clear that a central reliance upon consent may fail to support a 'welfarist' position, given poor decisions will be allowed to stand regardless of consequences and genuinely beneficial social welfare may be overlooked. The result is that, whether minded toward an 'individualist' or 'welfarist' position, there may be good reason to support contextualising a (more modest) consent standard and, simultaneously, imposing substantive standards of fairness on personal data processing.

The proposed data protection legislation in India contemplates substantive limits being imposed on data processing even where consent is obtained. These limits are imposed through the use of a concept of a data fiduciary, who is under an obligation to only process data where this is fair and reasonable in the circumstances. Such an approach may be seen as paternalistic because it may, in some circumstances, override consent. However, it offers the potential, we suggest, for advancing broader goals. We suggest that mechanisms for promoting substantive standards of fair data protection — the aim of the fiduciary model — can be used to both protect individual data subjects and to advance collective welfare, wherever the ideal balance may be sought. At least in the UK, the fairness qualification on data processing under European data protection law has largely been applied to require procedural requirements of transparency rather than substantive protections on the interests of the data subject. If the limits on consent as a safeguard are not genuinely addressed, then this promotes neither a welfarist nor individualist agenda.

---

[14] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1< https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN> ('*GDPR*').

[15] See also Damian Clifford and Jeannie Marie Paterson, 'Consumer Privacy and Consent: Reform in the Light of Contract and Consumer Protection Law' (2020) *Australian Law Journal* (forthcoming).

We are candid that our view is that there may be significant advantages in a modern information society to adopting a relatively clear 'welfarist' position: with protections not only built into the limits of informational self-determination but into a responsibility on data controllers to act in the best interests of data subjects. As with welfarist positions in contract law, it places less emphasis on a 'gold-plated' consent and instead establishes the effective controls beyond consent. However, our argument is that this recognition of the role for standard-based limitations of fairness on data processing might also be advantageous if you prefer an individualist perspective. The paradox of leaning too heavily on consent as a safeguard is that such reliance may simply overburden that concept. The effect of bounded rationality on individuals' decision-making capacity may mean they do not benefit from the extensive requirements in data protection legislation for obtaining consent. Moreover, these requirements can raise the threshold for valid consent to a point that organisations consider unattainable; thereby encouraging them to rely upon alternatives. Establishing a 'valid' consent is just too hard, and the conditions for even individual control may be diminished.

Given the exponential growth in new technologies in providing both public and private sector services to consumers and citizens, concerns over data protection and privacy are likely to continue to assume prominence in public policy debate and law reform. Like the Court in *Aadhaar*, we are particularly interested in ensuring protections that are adequate to an information age, characterised by novel methods of data mining, machine learning, and ever-expanding big data. The Report of the Committee of Experts on Data Collection and Privacy, as well as the Bill that followed it, make clear that consent-based mechanisms are necessary but not sufficient at this time in history, and that there are compelling reasons to provide protections beyond consent in both promoting individual rights around privacy and collective, welfarist goals.

II. Privacy, Liberty and Human Dignity in Indian Privacy Reform

A. The Decisions in Puttaswamy and Aadhaar

In 2016 the Indian government introduced the Aadhaar scheme, under which demographic and biometric data of individuals is compiled by the government through the Unique Identification Authority of India ('UIDAI'). The UIDAI associates the demographic and biometric data with a 12-digit unique identity number (called 'Aadhaar'). This number is used to access a

number of different government services. There were also demands for it to be used to access commercially provided services.[16] The *Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act* 2016 ('*Aadhaar Act*') governing the uses of the biometric identifier was questioned on the ground that it violated a constitutionally guaranteed right to privacy (under Article 21). Before the question of whether the Aadhaar scheme violated a right to privacy could be properly addressed, it had first to be determined whether the Indian Constitution guaranteed such a right. Previous caselaw had indicated otherwise.

In order to determine whether the Indian Constitution protected a right to privacy, and to address the fact that an eight bench court in *MP Sharma* v. *Satish Chandra* and a six bench court in *Kharak Singh* v. *State of UP* had indicated that it did not, the Supreme Court assembled a nine bench court to consider the question in *Puttaswamy*.[17] The Supreme Court in *Puttaswamy* decided that privacy is a constitutionally protected right. This emerges primarily from the guarantee of life and personal liberty in Article 21 of the Constitution and other provisions under fundamental rights contained in Part III.

The nature of the interest protected, and its relationship with liberty and other concepts — such as human dignity — was articulated in a variety of ways by the Court. The significance of self-determination may be understood to resolve differently according to whether emphasis is upon privacy as emergent from a right to liberty (guaranteed by Article 21) or privacy as a facet of human dignity (guaranteed by the fundamental rights contained in Part III of the Constitution). The right to liberty may be varyingly conceived to permit interference necessary to protect long-term freedoms and reciprocal duties to others. Human dignity itself might be resolved as a motivation for *empowerment* or *constraint*.[18]

If sympathy tends toward ideas of individual liberty and human dignity as empowerment at one end of the spectrum, then a respect for human dignity may support relatively untrammelled respect for autonomy and self-determination. The court favourably quoted Aharon Barak (former Chief Justice of the Supreme Court of Israel):

---

[16] There was media reporting of private firms previously asking customers to 'mandatorily link Aadhaar': Anonymous, 'Sec 57 of Aadhaar Act Struck Down. Here's What it Means for You', *The Quint* (online, 26 September 2018) <https://www.thequint.com/news/india/supreme-court-strikes-down-section-57-of-aadhaar-act-what-it-means-for-you>.

[17] (2017) 10 SCC 1.

[18] Deryck Beyleveld and Roger Brownsword, *Human Dignity in Bioethics and Biolaw* (OUP 2001).

> The best decisions on how life should be lived are entrusted to the individual. They are continuously shaped by the social milieu in which individuals exist. The duty of the state is to safeguard the ability to take decisions — the autonomy of the individual — and not to dictate those decisions.[19]

If sympathy tends toward maintaining the conditions capable of affording freedom and liberty for all members of society across the long-term, or human dignity as constraint, then one might not so readily entrust decisions on data flows to individuals operating under conditions of bounded rationality.[20] Specific choices may be denied to an individual if inconsistent with enduring autonomy or a particular idea of a dignified life[21] or the values of society. That respect for human dignity affords limited individual freedom is reflected in the view that the entitlements to be protected are foundational to social order. This view was also expressed in *Puttaswamy*:

> At a descriptive level, privacy postulates a bundle of entitlements which lie at the foundation of ordered liberty.[22]

The decision, therefore, shows ambivalence about the extent to which self-determination, or at least informational self-determination, should prevail over judicially dictated reasonable expectations regarding information norms. The latter leaves open still a wide range of views of what constitutes a properly ordered society: what 'fair' means.

---

[19] *Puttaswamy*, [105].

[20] On the inferences for consumer protection drawn from the reality of the bounded rationality of consumers: see further Geraint Howells, 'The Potential and Limits of Consumer Empowerment by Information' (2005) 32(3) *Journal of Law and Society* 349, 358–9.

[21] This is consistent with what Beyleveld and Brownsword describe as 'human dignity as constraint': Beyleveld and Brownsword (n 18). This view is also expressed by some theorists that respect for human dignity may require some autonomous choices (e.g. to clone a human being) to be restricted: see, e.g., Leon R Kass, *Life, Liberty and the Defense of Dignity* (Encounter Books, 2002); Francis Fukuyama, *Our Posthuman Future: Consequences of the Biotechnology Revolution* (Picador, 2003).

[22] *Puttaswamy*, [185]. This idea is picked up in the later case of *Cochin Institute of Science & Technology v Jisin Jijo* 2019 SCC OnLine Ker 1800, [298]–[299]: 'the notion that there must exist a reasonable expectation of privacy ensures that while on the one hand, the individual has a protected zone of privacy, yet on the other, the exercise of individual choices is subject to the rights of others to lead orderly lives. For instance, an individual who possesses a plot of land may decide to build upon it subject to zoning regulations. If the building bye laws define the area upon which construction can be raised or the height of the boundary wall around the property, the right to privacy of the individual is conditioned by regulations designed to protect the interests of the community in planned spaces. Hence while the individual is entitled to a zone of privacy, its extent is based not only on the subjective expectation of the individual but on an objective principle which defines a reasonable expectation.'

When it came to applying the decision in *Puttaswamy* to the Aadhaar scheme, a five-judge bench in the Supreme Court[23] concluded that elements of the scheme did not meet the requirement that the right to privacy should be impinged only with a just, fair,[24] and reasonable law. The *Aadhaar* Court held that the Aadhaar scheme served an important social or public interest in general terms, and the constitutionality of the Act could be substantially upheld. The use of the biometric data for accessing government services was constitutional based on the proportionality principle. However, the Court also found it necessary to either strike down or read down elements of the *Aadhaar* scheme on the ground that they were incompatible with the constitutionally protected right to privacy. These included that retention of data beyond a period of six months is impermissible; regulation 27 of the *Aadhaar (Authentication) Regulations 2016* which provided for archiving for a period of five years was struck down. Also, section 57 which allowed for the scheme to be used for any purpose was read down to mean such a purpose as backed by law. The significance of this is that it denied the possibility that contract alone could be sufficient to establish a right to use the Aadhaar number for services such as banking, telecommunications or education.[25] Private organisations, and individuals, were thus denied the possibility of using the scheme to authenticate the identity of individuals; such use was considered a disproportionate interference with privacy.[26]

Since the judgment in *Puttaswamy* was handed down, there has been statutory reform that will now permit private entities to request and use the biometric Aadhaar data.[27] This itself reflects a difference of opinion on whether the use of the Aadhaar scheme by private bodies like telecom companies and banks is a use of personal information to which individuals should be entitled to agree. The welfarist approach of the Court was apparently not accepted by the legislature on this point. The general approach though, one which recognises a data controller's responsibility to protect

---

[23] *Aadhaar-5 Judge* (2019) 1 SCC 1.

[24] It is necessary to distinguish between 'fair' processing, which might be required by a respect for privacy, and 'fair' interference with privacy. Although one might expect a least a degree of consonance between tests of fairness in different parts of the same legal regime our interest is especially in the former.

[25] Lothar Determann and Chetan Gupta, 'India's Personal Data Protection Act, 2018: Comparison with the General Data Protection Regulation and the California Consumer Privacy Act of 2018' (2019) 37(3) *Berkeley Journal of International Law* 481.

[26] We do not explore here the circumstances in which such uses might be considered a proportionate and legitimate curtailment of the right to privacy.

[27] The Aadhaar and Other Laws (Amendment) Act 2019. For commentary: see 'Lok Sabha Passes Aadhaar Amendment Bill', *The Economic Times* (online, 4 July 2019) <https://economictimes.indiatimes.com/news/politics-and-nation/lok-sabha-passes-aadhaar-amendment-bill/articleshow/70078736.cms>.

individual interests through more than the safeguard of consent, was taken up in subsequent recommendations for regulatory reform.

B. Report of the Committee of Experts

Following the decision in *Puttaswamy,* a Committee of Experts — under the Chairmanship of Justice BN Srikrishna — submitted its report to the Ministry of Electronics and Information Technology on *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians*. The Committee clearly acknowledged the need for individual rights, including to privacy, to be balanced by collective interests.[28] Indeed, the Committee framed its recommendations on the twin bases that 'it is the duty of the state to put in place a data protection framework which, while protecting citizens from dangers to informational privacy', also served the 'common good'.[29] The Committee saw these as complementary objectives rather than being in conflict. This was because individual rights of autonomy were only meaningful in the context of a fair and equitable society. Thus

> [t]he growth of the digital economy, which is proceeding apace worldwide, must be equitable, rights reinforcing and empowering for the citizenry as a whole. In this, to see the individual as an atomised unit, standing apart from the collective, neither flows from our constitutional framework nor accurately grasps the true nature of rights litigation.[30]

The report recognised the role for consent in allowing data subjects to exercise autonomy.[31] It also acknowledged the concern that, particularly in an online environment, the operation of notice and consent are not strongly protective of individual rights.[32] However, it was not appropriate to abandon this mechanism altogether.[33] Consent-based mechanisms ensured respect for an individual's autonomy and also provided a clear basis for processing data.[34] Rather, there was a need for 'form and substance'[35] requirements to ensure consent in this context was meaningful; namely that consent be free, informed, specific, clear and capable of being withdrawn.[36]

---

[28] *Protecting Privacy, Empowering Indians* (n 10) 10.
[29] ibid 5.
[30] ibid 9.
[31] ibid 24.
[32] ibid 32.
[33] ibid 33.
[34] ibid 24.
[35] ibid 11.
[36] ibid 37.

Importantly, the Committee advocated strongly for an additional regulatory framework to ensure fairness in data processing which would provide a counter to the inevitable inequities of bargaining power between individuals and data principals.

Fairness pertains to developing a regulatory framework where the rights of the individual with respect to her personal data are respected and the existing inequality in bargaining power between individuals and entities that process such personal data is mitigated.[37]

The Committee recommended that the fair use of individual's data be achieved through the designation of a data fiduciary. Drawing on earlier scholarly work from the US, in particular the work of Balkin,[38] the committee explained that the fit of the fiduciary label arose from the expectations of the individual and the relationship of trust created between individuals and a data principal.[39] The Committee noted that such features were the 'hallmark' of a fiduciary relationship created in equity under common law regimes.[40] The duties of the data fiduciary should be to act consistently with that position of trust by complying with standards of fairness in the use of data.

In the digital economy, depending on the nature of data that is shared, the purpose of such sharing and the entities with which sharing happens, data principals expect varying levels of trust and loyalty. For entities, this translates to a duty of care to deal with such data fairly and responsibly for purposes reasonably expected by the principals.[41]

The Committee was clear that the 'fair and reasonable' requirement was more than a procedural duty but should have substantive content. These obligations should be premised on not processing data for ends that may not be in individuals' best interests or which go beyond their reasonable expectations.[42] Such obligations supplement consent as a safeguard for data privacy, but unlike rules for the way in which consent may be sought, go beyond consent as the determinant of the uses to which data can be put.

---

37 ibid 8.
38 Jack M Balkin, 'Information Fiduciaries and the First Amendment' (2016) 49(4) *UC Davis Law Review* 1183.
39 ibid.
40 See, e.g., *Hospital Products Ltd v United States Surgical Corp Ltd* (1984) 156 CLR 41 ('*Hospital Products*').
41 *Protecting Privacy, Empowering Indians* (n 10) 8.
42 ibid 52.

C. The Personal Data Protection Bill 2019

The *Personal Data Protection Bill 2019* was introduced in Lok Sabha by the Minister of Electronics and Information Technology, Mr Ravi Shankar Prasad, on December 11, 2019.[43] The Bill seeks to provide for protection of personal data of individuals and establishes a Data Protection Authority to that end. The Bill governs the processing of personal data by: (i) government, (ii) companies incorporated in India, and (iii) foreign companies dealing with personal data of individuals in India.[44]

Following the recommendations of the report of the Committee, the Bill establishes a central role for the consent of the 'data principal'; which is similar to the concept of the 'data subject' in the *GDPR*. Under section 11, personal data 'shall not be processed, except on the consent given by the data principal at the commencement of its processing'. However, sections 12, 13 and 14 provide other legal bases for processing. These include, under section 12, public functions authorised by law, and to respond to medical emergency or threat to public health. Section 13 provides for processing necessary in an employment context. Section 14 permits processing without consent if necessary, for 'reasonable purposes' as may be specified by the Regulations, taking into account respective private and public interests, whether it is reasonable to expect consent to be obtained, and the reasonable expectations of the data principal in the context.

Where consent is the lawful basis for processing, section 11(2) of the Bill states the consent of the data principal shall not be valid, unless such consent is—

(a) free, having regard to whether it complies with the standard specified under section 14 of the Indian Contract Act, 1872;

(b) informed, having regard to whether the data principal has been provided with the information required under section 7;

(c) specific, having regard to whether the data principal can determine the scope of consent in respect of the purpose of processing;

---

[43] On the scope of the bill see further: Deva Prasad M and Suchithra Menon C, 'The Personal Data Protection Bill, 2018: India's Regulatory Journey Towards a Comprehensive Data Protection Law' (2020) 28(1) International Journal of Law and Information Technology 1; Determann and Gupta (n 25); Ashit Kumar Srivastava, 'Data Protection Law in India: The Search for Goldilocks Effect' (2019) 5(3) European Data Protection Law Review 408.

[44] For suggested improvements to strengthen privacy protection see Graham Greenleaf AM, 'India's Personal Data Protection Bill, 2019 Needs Closer Adherence to Global Standards' (Submission to Joint Committee, Parliament of India, 12 February 2020).

(d) clear, having regard to whether it is indicated through an affirmative action that is meaningful in a given context; and

(e) capable of being withdrawn, having regard to whether the ease of such.[45]

This approach follows the recommendation of the Committee that the statutory requirements for valid consent should be a 'significant step towards ensuring the consent is informed and meaningful'.[46] The burden of proof that consent has been given is on the party who will be in control of the data, termed the 'data fiduciary',[47] but all legal consequences of a valid withdrawal of consent must be borne by the data principal.[48] It is not permissible to make provision of any good or service, performance of any contract, of enjoyment of any right or claim, conditional upon consent to the processing of personal data except where necessary for that purpose.[49]

In addition to establishing a higher threshold for a valid consent, again following the recommendations of the Committee, the Bill proposes a considerable role for the 'data fiduciary'. A data fiduciary is 'any person … who alone or in conjunction with others determines the purpose and means of processing of personal data.[50] Substantially the same definition is used for a 'data controller' under the *GDPR*.[51] The data fiduciary under the Bill is also under a responsibility to process personal data 'in a fair and reasonable manner and ensure the privacy of the data principal'.[52] The data fiduciary is also under an obligation to ensure that data is processed

for the purpose consented to by the data principal or which is incidental to or connected with such purpose, and which the data principal would reasonably expect that such personal data shall be used for, having regard to the purpose, and in the context and circumstances in which the personal data was collected.[53]

---

[45] Additional conditions attach to consent to the processing of sensitive personal data: see Personal Data Protection Bill 2019 (India) s 11(3).

[46] *Protecting Privacy, Empowering Indians* (n 10) 38–46; Annexure B; 185.

[47] Personal Data Protection Bill 2019 (India) s 11(5).

[48] ibid s 11(6).

[49] ibid s 11(4).

[50] ibid s 3. There is a further category of 'significant data fiduciary'. The Personal Data Protection Bill 2019 (India) s 26 establishes the conditions under which a data fiduciary may be defined as a significant data fiduciary, and thus subject to additional responsibilities.

[51] *GDPR* (n 14) art 4(7): 'controller' means 'the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data'.

[52] Personal Data Protection Bill 2019 (India) s 5(a).

[53] ibid s 5(b).

i. Consent and Data Fiduciaries under the Indian Bill

As has been seen, one of the distinctive features of the Indian *Personal Data Protection Bill 2019* is its reliance on the concept of a data fiduciary. The use of the term 'fiduciary' to describe the obligations of the data controller is deliberate in order to invoke the equitable concept of a fiduciary. The classic description of a fiduciary in equity is a person who undertakes to act 'for or on behalf of or in the interests of another'.[54] Examples include doctors, lawyers and accountants. In adopting this approach, the Committee was influenced by the work of Professor Jack M Balkin.[55] Balkin observed that individuals are also dependent on, and vulnerable to the actions of, digital platforms such as Facebook, Amazon, Twitter and Uber. Because they hold special power to affect the well-being of others, Balkin argued that these digital platforms, and any business that collect, analyse, sell, use, and distribute data, should 'have special duties to act in ways that do not harm the interests' of the data principal.[56] Balkin accordingly proposed the concept of an information fiduciary applying to business and people in a digital age who 'collect, analyse, use, sell, and distribute personal information'.[57] Balkin's aim in developing this approach was to broaden the debate around protecting privacy from focusing on the kinds of data being held by an entity to the kinds of relationships between data subjects and data controllers that might justify regulation.[58] Balkin argued that if entities hold themselves out as trustworthy in holding personal information, they should be held to these assertions.[59] The framework has been criticised by other scholars, prominently by Khan and Pozen.[60] They argue that the technique of using fiduciary law to address concerns about how data is handled by companies fails to address the systematic issues of 'structural power' around digital platforms and the need for 'more robust public regulation'.[61] Khan and Pozen also question the fit between the fiduciary concept, even in the modified form

---

[54] *Hospital Products* (n 40) 96–7 (Mason J). In US jurisprudence, see *Kurtz v Solomon* 656 NE 2d 184, 190 (III App Ct, 1995); Tamar Frankel, *Fiduciary Law* (Oxford University Press, 2011) 42–5; Deborah A DeMott, 'Beyond Metaphor: An Analysis of Fiduciary Obligation' [1988] (5) Duke Law Journal 879, 882.

[55] Balkin (n 38). See also Lina M Khan and David E Pozen, 'A Skeptical View of Information Fiduciaries' (2019) 133(2) *Harvard Law Review* 497.

[56] Balkin (n 38) 1186.

[57] ibid.

[58] ibid 1187.

[59] ibid 1224.

[60] Khan and Pozen (n 55).

[61] ibid 502.

proposed by Balkin, and the business models of digital platforms who would be the prime exemplars of the new data fiduciary designation,[62]

In the Indian *Personal Data Protection Bill 2019*, the concept of the data fiduciary has been extended more generally to address fundamental concerns about the ability of data subjects to adequately protect their own interests purely through mechanisms based on consent and contract. The Committee of Experts, whose recommendations shaped the Bill, explained that the use of the term fiduciary in the data protection context was a recognition not only that the relationship between contracting parties may be unequal, but of 'one party's dependence on another for performance of a service or achievement of an objective'.[63] This imbalance in bargaining power and consequent dependence on the decisions of the data controller characterises many online transactions where a consumer may not have any alternative other than to agree to provided terms and conditions, if they wish to receive a service or achieve another objective.

In equity fiduciaries are subject to a rigorous set of protective obligations. The Committee of Experts observed that fiduciaries must uphold 'trust and loyalty placed in them by the data principal'.[64] This takes the form of a duty to act 'in the best interest of the principal'.[65] In general fiduciary relationships this requires the fiduciary to avoid conflicts of interest [66]and taking unauthorised profits from their position as fiduciary.[67] It does not appear that the data fiduciary under the Indian *Personal Data Protection Bill 2019* is intended to hold the same set of stringent expectations around loyalty, and indeed Balkin's model of an information fiduciary a more limited set of expectations than might apply to traditional kinds of fiduciary.[68] As Khan and Pozen have pointed out, avoiding conflicts would be practically impossible for many key players in the digital economy.[69] The committee of experts described the responsibilities of the data fiduciary as requiring it not to

---

[62] ibid 507. See also 511 discussing the tension between fiduciary duties of loyalty and targeted advertising.

[63] *Protecting Privacy, Empowering Indians* (n 10) 51.

[64] ibid.

[65] ibid. See, eg, *Breen v Williams* (1996) 186 CLR 71, 135 (Gummow J); *Pilmer v Duke Group Ltd* (2001) 207 CLR 165, 199 [78] (McHugh, Gummow, Hayne and Callinan JJ) ('*Pilmer*'). See also Deborah A DeMott, 'Breach of Fiduciary Duty: On Justifiable Expectations of Loyalty and Their Consequences (2006) 48(4) *Arizona Law Review* 925.

[66] *Pilmer* (n 65) 199 [78] (McHugh, Gummow, Hayne and Callinan JJ); *Hospital Products* (n 40) 103 (Mason J); *Boardman v Phipps* [1967] 2 AC 46: [1966] 3 WLR 1009, 127 (Lord Upjohn).

[67] For the interaction between these two 'overlapping but distinct' themes, see *Chan v Zacharia* (1984) 154 CLR 178, 198–9 (Deane J).

[68] Balkin (n 38) 1225.

[69] Khan and Pozen (n 55) 504.

process data in a way that goes beyond the reasonable expectations of the data principle or in a way that was not in the data principal's best interests.[70] The *Personal Data Protection Bill 2019* sets out a more narrowly focused set of duties, focused on protecting the privacy interests of the data subject, rather than avoiding conflicts of interest. In particular, as noted above, the data fiduciary's obligations are to process personal data 'in a fair and reasonable manner and ensure the privacy of the data principal'.[71] The scope of protection is determined by reference to the purposes that the data principal would reasonably expect, having regard to 'the purpose, context and circumstances of the collection'.[72]

Whether this formulation of the data fiduciaries' duties leaves any real resonance with the general law concept of a fiduciary is not, for our purposes, a necessary debate. It may be that different language would be preferable to avoid confusion around the equitable and statutory concepts.[73] We also do not here engage with the broader issue of whether the structural imbalances in power that characterise a modern information economy should be addressed in more direct ways, including an entire restructuring of the market. Khan and Pozen are certainly concerned that Balkin's concept of a data fiduciary may prove an unhelpful distraction from the broader reforms required.[74] We wish to focus solely on the decision in the legislature to impose subjective restrictions on data processing that apply regardless of the existence of consent, or for that matter, contract, of the data subject. In this context, we observe that the label 'data fiduciary' seems to be to have an iterative function in emphasising that the data controllers' duties go beyond acting in its own commercial self-interest. A move to make clear that protecting the reasonable expectations of the data subject to data privacy is the responsibility of the data controller/data fiduciary. Placing the defined positive obligations on the entity that determines the purpose and means of processing of personal data extends responsibility beyond technical compliance with a duty to ensure a legal basis for processing.

> Placing such an obligation is recognition of the fact that given the unequal nature of the relationship and its inherent opacity, what is legal may not ipso facto be fair or reasonable.[75]

---

[70] *Protecting Privacy, Empowering Indians* (n 10) 52.
[71] Personal Data Protection Bill 2019 (India) s 5(a).
[72] ibid s 5(b).
[73] Cf Jeannie Marie Paterson and Elise Bant, 'Mortgage Broking, Regulatory Failure and Statutory Design' (2020) 31(1) Journal of Banking and Finance Law and Practice 7.
[74] Khan and Pozen (n 55) 502.
[75] *Protecting Privacy, Empowering Indians* (n 10) 52.

The effect of this strategy is that the fiduciary has obligations to assess the consequences of data use and cannot rely on consent as permission for a specified use. A consumer's consent to processing is not sufficient guarantee that the processing is either in their best interests or fair and reasonable. Consumers cannot be presumed to be capable of protecting their own interests when it comes to privacy and the common law concept of 'reasonable expectations' remains critical in defining the acceptable limits of data processing. As noted by the Committee:

> Further it is testament to the fact that consent which may be valid for creating legal relationships may not be sufficient to fully disclaim liability.[76]

The Committee does not suggest that the standard of fair and reasonable will unpack in the same way in all circumstances:

> Needless to say, the extent of the obligations of a data processor may differ, depending on the exact nature of processing in question and the requisite duty of care may be duly reflected in the contract between the data fiduciary and itself.[77]

They saw the flexibility within the standard, and the discretion it afforded the regulator and courts to do justice in the instant case, to be a strength:

> This is precisely why laying down such a general principle of fair and reasonable processing will allow it to be developed by the DPA and courts of law, taking into account technological developments over time and differential obligations of different entities.[78]

There is little doubt that this move leaves many questions unanswered. Should the obligations of online sellers be the same as those of social media platforms or online banking service providers?[79] What happens if the data fiduciary is a public rather than a private body? How do these circumstances affect what constitute 'reasonable expectations'? These are important questions to be resolved. Without answering them ourselves, we can note the value of prospective regulatory guidance. Our point is only that the opportunity to promote a contextual understanding of what constitutes a valid consent in different circumstances is valuable. This is something that seems

---

[76] ibid.
[77] ibid.
[78] ibid.
[79] We note that the Bill itself proposes some answers to such questions by elevating the obligations of a 'significant data fiduciary' and including 'social media intermediary' within the latter class: seen n 58. This does not, however, preclude further debate on how obligations should be distributed across different kinds of data controller.

to be becoming less, rather than more, nuanced under European data protection legislation.

III. A European Perspective

We can see within European data protection law similar signs of ambivalence with regards to the function of consent as we have previously noted. It is a central data protection safeguard. But it remains unresolved whether informational self-determination is valued for its own sake or as a means to prevent misuse of personal data: with 'misuse' defined relative to a conception of reasonable expectation that is at least partially independent of the data subject.[80] The proper function of consent in European law is further complicated by the fact that European data protection law has moved to disconnect a right to data protection from the right to privacy[81]. This also opens many questions we do not seek here to pursue. We wish only to note that — irrespective of any underlying normative or conceptual coherence — this move has been accompanied by a strengthening of the requirements for a valid consent beyond that anticipated by the Indian *Personal Data Protection Bill 2019* and a trend toward recommending reliance upon legal basis *other than* consent to legitimise processing. We offer UK data protection law as an example of a regime that has raised the bar for individual consent, recommended that alternatives be relied upon when available, and not applied the test of *unfair* processing in a way that demonstrates it to have the substantive content proposed by the Expert Committee in India. The result, we suggest, is a missed opportunity to progress either a welfarist or individualist agenda: individuals are not effectively empowered in practice, nor are agreements regulated to protect the best interests of either individuals or society more generally.

---

[80] We do not have the space here to fully unpack a conception of 'reasonable expectation' but we note that the classic US formulation of 'reasonable expectation,' dating back to *Charles Katz v United States* 1967 SCC OnLine US SC 248: 19 L Ed 2d 576 : 389 US 347 (1967), has both a subjective and an objective element. We would connect an understanding of 'fair processing' to the objective element. One of us has written more on the concept of a reasonable expectation in the context of the English law of confidence. Mark J Taylor and James Wilson, 'Reasonable Expectations of Privacy and Disclosure of Health Data' (2019) 27(3) *Medical Law Review* 432. The systematic consideration of the conceptual relationship between the term as used in different contexts, and the notion of 'fair' in data protection law, must wait for future research.

[81] See further Bart van der Sloot 'Legal Fundamentalism: Is Data Protection Really a Fundamental Right?' in Ronald Leenes et al (eds), *Data Protection and Privacy: (In)visibilities and Infrastructures* (Springer, 2017) 3 exploring the question of what it means for EU law to have separated data protection from the right to privacy and instead to have elevated data protection to the level of a fundamental right.

The EU *General Data Protection Regulation* ('*GDPR*') (2016/679) repealed and replaced the *European Data Protection Directive* (95/46/EU). It came into force on 25 May 2018 and was intended to not only update European data protection law but also, as a regulation (rather than a directive), to achieve higher levels of harmonisation across Europe. In the UK, any processing[82] of personal data carried out in the context of an establishment of a controller or processor in the UK,[83] must comply with data protection legislation,[84] including the *Data Protection Act 2018* and the *GDPR* as applied in the UK context.

The term 'personal data' is defined very broadly by data protection legislation to include *any* information relating to an identified or identifiable person.[85] Those subject to the requirements of data protection legislation must process personal data in compliance with a set of data protection principles which relate to 'lawfulness, fairness, and transparency', 'purpose limitation', 'data minimisation', 'accuracy', 'storage limitation', 'integrity and confidentiality', and 'accountability'. The lawfulness of processing is determined, in part, by Article 6 of the *GDPR*.

It is necessary (but not sufficient) for lawful processing to meet one of the conditions set out in Article 6(1) of the *GDPR*. The conditions most likely to be appropriate to processing for research purposes are (i) processing is with the data subject's consent (Article 6(1)(a)), (ii) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (Article 6(1)(e)), or (iii) processing is necessary for the purposes of a data controller's legitimate interests (Article 6(1)(f)). Only one condition needs to be satisfied. A data subject's consent is not required if an alternative ground is available. Controllers should select the most appropriate ground available for the processing intended.

---

[82] Broadly defined by *GDPR* (n 14) art 4(2) to include any operation or set of operations performed on personal data or on sets of personal data whether or not by automated means.

[83] Data Protection Act 2018 (UK) s 207(2). In fact, the territorial application of the 2018 extends beyond this. This is a point we pick up later as it has some significance for researchers in member states targeting research participants in the UK in case of Brexit.

[84] ibid s 3(9) provides a definition of data protection legislation. To be amended, in case of Brexit by Sch 21, Pt 2, Para 2(1) of the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019.

[85] *GDPR* (n 14) art 4(1) defines 'personal data' as 'any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person'.

Special categories of data qualify for additional protections under data protection law, through Article 9 of the *GDPR*. Processing of special category data is prohibited unless one of a number of exceptions apply. The first alternative exception under Article 9 is that 'the data subject has given explicit consent to the processing' (Article 9(2)(a)).

'Consent' is thus both an available lawful basis for processing (under Article 6) *and* 'explicit consent'(an available exception to the prohibition on processing special category data (under Article 9)). Consent is defined by the *GDPR* to mean

> any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.[86]

The *GDPR* is understood to have raised the threshold for a valid consent under EU data protection law and represents

> an important reframing of the consent standard in terms of greater specificity of requirements and more stringent protection of participants. The consent framework is expanded upon in several of its Recitals (particularly 32, 33, 40, 42, 43, 157 and 171), as well as in Articles 7 (on the conditions for consent), 8 (on a child's consent relating to information society services) and 17 (on the right to erasure).[87]

This has led to a move away from a reliance upon consent.[88] The data protection authority in the UK, the Information Commissioner's Office ('ICO'), advises that:

> The GDPR sets a high standard for consent. But you often won't need consent. If consent is difficult, look for a different lawful basis.[89]

---

[86] *GDPR* (n 14) art 4(11).

[87] Megan Prictor et al, 'Consent for Data Processing Under the General Data Protection Regulation: Could 'Dynamic Consent' be a Useful Tool for Researchers?' (2019) 3(1) *Journal of Data Protection and Privacy* 93, 96.

[88] Olly Jackson, 'Businesses Retreating from Consent Under GDPR', *International Financial Law Review* (online, 3 April 2018) <https://www.iflr.com/Article/3798060/Businesses-retreating-from-consent-under-GDPR.html>.

[89] Information Commissioner's Office (Guide), 'Guide to the GDPR: Lawful Basis for Processing: Consent' <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/>.

The *GDPR* itself discourages reliance upon consent where the controller is a public body or where there might otherwise be a clear imbalance of power between the parties:

> In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation.[90]

This threshold for a 'free' consent thus appears higher than that under the Indian *Personal Data Protection Bill 2019*, where it is sufficient to comply with the standard specified under section 14 of the Indian *Contract Act 1872*: namely that it is not caused by coercion, undue influence, fraud, misrepresentation or mistake.[91] It is questionable, however, whether raising the bar in this way — and discouraging consent in any case of clear imbalance of power, irrespective of whether that imbalance is abused — is empowering if it encourages organisations to rely upon alternative legal bases.

If consent is not the legal basis, then there is some protection for individual or collective interests built into the alternatives but not necessarily in consistent measure. If processing is by a public body, then processing shall be lawful to the extent it is 'necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller' (Article 6(e)). This clearly restricts the freedom of public bodies to act in pursuit of a self-interested agenda without adequate account taken of the public interest evidenced either in the specific task or in the original allocation of official authority. Private bodies may rely upon 'legitimate interests' (Article 6(1)(f)) or on the requirement that processing is necessary for the performance of a contract to which the data subject is party (Article 6(1)(b)). If reliant on the former, then they must consider whether their interests in processing are overridden by the individual's interests or fundamental rights and freedoms. A controller can rely upon processing being necessary

> for the purposes of the legitimate interests pursued by the controller or by a third party, *except where such interests are overridden by*

---

[90] *GDPR* (n 14) Recital 43.

[91] 'Consent is said to be free when it is not caused by (1) coercion, as defined in Section 15, or (2) undue influence, as defined in Section 16, or (3) fraud, as defined in section 17, or (4) misrepresentation, as defined in Section 18, or (5) mistake, subject to the provisions of Sections 20, 21 and 22. Consent is said to be so caused when it would not have been given but for the existence of such coercion, undue influence, fraud, misrepresentation or mistake'.

> *the interests or fundamental rights and freedoms of the data subject* which require protection of personal data, in particular where the data subject is a child.[92]

While this puts no obligation on a data controller to act in the interests of a data subject, nor consider collective concerns, it does constrain the ability of the data controller to pursue their own interests in a way that disproportionately impacts upon an individual. If reliant on the fact that processing is necessary for the performance of a contact to which the data subject is party, then the interests of an individual are narrowly protected by a requirement that the processing be necessary given the contractual purpose. The Article 29 Working Party opined that this legal basis applies to prevent unilateral imposition on a data subject through a contract:

> For example, Article 7(b) is not a suitable legal ground for building a profile of the user's tastes and lifestyle choices based on his click-stream on a website and the items purchased. This is because the data controller has not been contracted to carry out profiling, but rather to deliver particular goods and services, for example. Even if these processing activities are specifically mentioned in the small print of the contract, this fact alone does not make them 'necessary' for the performance of the contract.[93]

Of course, this does not preclude a data subject from contracting for services, such as profiling, in circumstances where others might question whether the service is in the individual's best interests.[94] Where processing *is* on the basis of an individual's consent, then even these uneven levels of protection for individual and collective interests do not apply. When consent is the lawful basis, then the expectation is that the data subject is best placed to protect his or her best interests. As the Article 29 Working Party put it:

> In the first case, under Article 7(a), it is the data subjects themselves who authorise the processing of their personal data. It is up to them to decide whether to allow their data to be processed …. As the processing of the user's data is ultimately at his/her discretion, the emphasis is on the validity and the scope of the data subject's consent. In other words, the first ground, Article 7(a), focuses on the self-determination of the data subject as a ground for legitimacy. All other grounds, in contrast, allow processing — subject to safeguards and measures

---

92 *GDPR* (n 14) art 6(1)(f) (emphasis added).

93 European Commission, 'Opinion 06/2014 on the Notion of legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC', 844/14/EN WP 217, 17.

94 The interests of the data subject are, however, not here to be protected via data protection law, but rather through consumer protection measures in commercial and contract law.

> — in situations where, irrespective of consent, it is appropriate and necessary to process the data within a certain context in pursuit of a specific legitimate interest.

There are other specific examples where it is left to an individual, through the consent mechanism, to protect their own interests. We briefly mention just two. The first relates to automated processing, and here there is a clear intent to ensure some level of protection does persist. The second relates to transfer of data outside of the European Union and the protective regime of the *GDPR*. Here, however, it is much clearer that a data subject is entitled to agree to an arrangement that leaves them with materially less protection without proportionate benefit.

First, the *GDPR* states that individuals should have the right not to be subject to a decision based solely on automated processing.[95] However, decision-making based on such processing should be allowed 'when the data subject has given his or her explicit consent'.[96] In this case, the data controller is required to suitably safeguard the data subjects' rights, freedoms and legitimate interests and the data subject has 'at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision'.[97] There is thus a continued requirement to safeguard the individual's interests, but the level of protection is not the same. There is a level of risk that a data subject is entitled to take on by waiving the right not to be subject to decisions based solely on automated processing, and there seems no requirement that it be in his or her best interests to do so.

Chapter V of the *GDPR* (especially Articles 44 to 48) establishes the rules for transfer to a 'third country' and makes clear the underlying principle that such transfer ought not to undermine the level of protection guaranteed by the Regulation. However, Article 49 does allow for derogations for specific situations. One of these is that:

> The data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject.

If a data subject *has* been informed of the risks, and he or she provides a valid consent, then he or she is entitled to assume the risks of the transfer. This is the case even though a data controller is likely to have involved a third country for their own reasons and to their own advantage. For example, a

---

[95] *GDPR* (n 16) art 22(1).
[96] *GDPR* (n 16) recital 71; art 22(2)(c).
[97] ibid art 22(3).

data subject might be asked to accept risks which are associated with cheaper processing operations for the data controller. There is no requirement that the transfer to a third country be in the best interests of the data subject. There is only the underlying assumption that if the processing operation overall was not in his or her interests, they would not agree to it.

A. Fair Processing

Of course, any processing operation must not only be 'lawful' but must also satisfy other data protection requirements. Additional requirements may remedy any lack of protection associated with processing on the basis of a data subject's consent. Perhaps the most pertinent is that processing must be 'fair', as well as lawful.

Article 8 of the *Charter of Fundamental Rights of the European Union* requires that personal data must be processed 'fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law'.[98] The first data protection principle set out by the *GDPR* is that data shall be 'processed lawfully, *fairly* and in a transparent manner' (emphasis added).[99] When identifying the appropriate legal basis, data controllers must 'take into account the impact on data subjects' rights … in order to respect the principle of fairness'.[100]

In online guidance, the UK data protection regulator, the Information Commissioner's Office ('ICO') answers the question 'What is fairness?' in the following way:

> In general, fairness means that you should only handle personal data in ways that people would reasonably expect and not use it in ways that have unjustified adverse effects on them. You need to stop and think not just about how you can use personal data, but also about whether you should.
>
> […]
>
> In order to assess whether or not you are processing personal data fairly, you must consider more generally how it affects the interests of the people concerned – as a group and individually. If you have obtained and used the information fairly in relation to most of the

[98] Charter of the Fundamental Rights of the European Union [2012] OJ C 326/391, art 8(2).
[99] *GDPR* (n 16) art 5(1)(a).
[100] European Data Protection Board, 'Guidelines 2/2019 on the Processing of Personal Data under Article 6(1)(b) GDPR in the Context of the Provision of Online Services to Data Subjects' (Guide, 16 October 2019) 4.

> people it relates to but unfairly in relation to one individual, there will still be a breach of this principle.[101]

This guidance suggests that the requirement that data is processed fairly may operate to constrain adverse effects on people, both as individuals and as members of groups. Superficially, there appear many parallels with the requirement for fair and reasonable processing proposed in the Indian *Personal Data Protection Bill 2019*. However, there is no parallel notion of a data fiduciary and there is some indication that this requirement has functioned to protect an idea of 'fair' that is tied closely to a procedural rather than substantive conception of fairness: requiring transparency and action consistent with declared intention, avoiding duplicity or misleading practice.[102] This does not, however, include the requirement that fair processing necessarily must also be in the interests of the data subject.

The Hellenic Data Protection Authority, in response to a complaint against PricewaterhouseCoopers ('PwC'), found that PwC had failed to process personal data relating to employees fairly. PwC required employees to provide consent to the processing of their personal data. This was considered an inappropriate legal basis in the circumstances. The Authority concluded that PwC

> [p]rocessed the personal data of its employees in an unfair and non-transparent manner … given them the false impression that it was processing their data under the legal basis of consent … while in reality it was processing their data under a different legal basis about which the employees had never been informed.[103]

One of the concerns with the fact that employees had been misled as to the legal basis upon what data was being processed was that this created a false impression of the control they might exercise over that processing: 'the choice of each legal basis has a legal effect on the application of the rights of data subjects'. There was no suggestion that PwC could not process the personal data for the purposes they had been processing it or that employees

---

[101] Information Commissioner's Office (Guide), 'Guide to the GDPR: Principles: Lawfulness, Fairness and Transparency' <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/lawfulness-fairness-and-transparency/>.

[102] Damian Clifford and Jef Ausloos have suggested that two key elements may be distilled from the fairness principle in European data protection law: fair balancing (proportionality and necessity) and procedural fairness. See Damian Clifford and Jef Ausloos 'Data Protection and the Role of Fairness' [2018] *Yearbook of European Law* 1.

[103] 'Price Waterhouse Coopers Business Solutions: Summary of Hellenic DPA's Decision' (Decision Summary No 26/2019, 2019) <https://edpb.europa.eu/sites/edpb/files/files/news/summary_of_decision_26_2019_en_2.pdf>.

must have more control than they did; the problem was that they had misled employees and sought to transfer compliance obligations to them by relying upon consent rather than a more appropriate legal basis.

The UK Data Protection Authority found that the processing by Royal Free NHS Foundation Trust ('Royal Free') did not fully comply with the requirements of the *Data Protection Act 1998*. Royal Free provided a third party, DeepMind, with approximately 1.6 million patient records under agreement for the purposes of carrying out clinical safety testing as part of the development of a new clinical detection, diagnosis and prevention application for the Trust in relation to Acute Kidney Injury. The Authority found that:

> The processing of patient records by DeepMind significantly differs from what data subjects might reasonably have expected to happen to their data when presenting at the Royal Free for treatment.[…] The mechanisms to inform those patients that their data would be used in the clinical safety testing of the Streams application were inadequate. In short, the evidence presented to date leads me to conclude that data subjects were not adequately informed that the processing was taking place and that as result, the processing was neither fair nor transparent.[104]

If the mechanisms to inform patients that data would be used in this way *had* been adequate, then the implication is that the processing would not have been unfair. No substantive judgement was made about the fairness of Royal Free patient data being processed by DeepMind. There was no substantive consideration given to whether the processing was in the interests of the patients whose data was transferred; only whether patients might reasonably expect it in the circumstances.

IV. Reflection and Recommendations: The Function and Limits of Consent

The Indian *Personal Data Protection Bill 2019* raises the threshold for valid consent, allows processing without consent in a limited range of circumstances, but places an obligation on data fiduciary to process 'fairly and reasonably' irrespective of consent to the processing. This is in recognition of the unequal bargaining positions of data principal and data controller. It is

[104] Information Commissioner's Office, 'DeepMind: Undertaking Cover Letter' (Notice of Investigation and Findings, 3 July 2017) <https://ico.org.uk/media/action-weve-taken/undertakings/2014353/undertaking-cover-letter-revised-04072017-to-first-person.pdf>.

intended to carry substantive content, and the use of the term 'data fiduciary' reinforces this position.

This approach may provide more significant protection than under European data protection law for which we have taken UK law as an example. This is even though a number of the provisions in the Indian *Personal Data Protection Bill 2019* appear analogues of those in European data protection law, and also despite the fact that the threshold requirements for consent may even be higher under UK law than under the Indian *Personal Data Protection Bill 2019*. In fact, raising the level of valid consent may be counterproductive.

The goal, if relying on consent to provide the legal basis for processing, presumably lies in the judgment that this mechanism will produce beneficial outcomes for individuals and for the market. In principle, individuals consent to processing only where they consider it to represent a fair bargain: consent itself is a sign of perceived mutual benefit. The stance taken in data protection regimes of imposing high threshold requirements for valid consent may be steps toward empowering consumers to strike bargains only when it is perceived to be in their best interests to do so. If it is a win-win scenario, then the consumer's interests may be sufficiently protected. A similar principle informs the law of contract and is expressed in the idea of 'freedom of contract'.

However, consent is a fragile means of protecting individual rights. As the Indian Expert Committee noted, one commonly expressed view is that consent in online contexts is 'broken'.[105] Consent in the context of online transactions or standard form contracts is not an adequate, or even accurate, indicator of the preferences of the individuals that give it, nor guaranteed to lead to welfare enhancing outcomes. Statutory mechanisms may seek to protect individuals against so called 'forced' consent by requirements — such as found in both the Indian *Personal Data Protection Bill* and the *GDPR* — for consent to be free, informed, specific, clear and capable of being withdrawn. These protections will be buttressed by prohibitions on misleading conduct and coercion provided under contract law[106] and consumer protection legislation.[107] However, they do little to get to the heart of the limitations on consent as an autonomy enhancing measure, which lies in the bounded rationality of human decisionmakers.

---

[105] *Protecting Privacy, Empowering Indians* (n 10) 32.
[106] See, eg, the Indian Contract Act 1872, s 15 (coercion) and s 18 (misrepresentation).
[107] See further the Consumer Protection Act 2019 (India).

Studies suggest that there are cognitive limitations on the ability of individuals to assess the risk allocations embedded in particular terms.[108] Individuals tend to estimate the probability of risk by reference to their experience or knowledge of the risk. Thus, individuals 'judg[e] risk to be high when the type of harm is familiar or easily imagined and low when it is not'.[109] They tend to be overly optimistic about their abilities to avoid risk. Moreover, hyperbolic discounting means that 'individuals systematically overvalue immediate benefits and costs and undervalue delayed benefits and costs'.[110] For these kinds of reasons, consumer protection law now commonly contains principles that can also impose substantive protections about the kinds of things that can be consented to including through scrutiny of unfair contract terms.[111] The proposed Indian *Personal Data Protection Bill 2019 i*s notable in that substantive protections are, as we have already noted, included as a counter balance to the notion of consent. The requirement for consent, or available exception, is supplemented by a requirement that personal data only be processed in a way that is 'fair and reasonable'. This obligation is given to the data controller or fiduciary. In so doing the Bill emphasises, in our view, that the requirement of fair and reasonable processing is not a mere procedural requirement but a substantive obligation. It requires, in our view, the data fiduciary to have regard to the interests of the data subject and at least ensure their interests are not undermined in a manner that is disproportionate to the goals to be achieved. It may also allow the data fiduciary to consider the interests of the data principal by reference to social values and expectations. Just how this balance is struck depends on the view taken of the interests that can justifiably be set against the privacy rights of the individual, leading to questions about the appropriate priorities as between public/private, present/future and individual/group interests should be set. Our point in this paper is that such limits should be seen as central part of a functioning data protection system.

---

[108] See, eg, Russel Korobkin, 'Bounded Rationality, Standard Form Contracts, and Unconscionability' (2003) 70(4) University of Chicago Law Review 1203; Robert A Hillman and Jeffrey J Rachlinski, 'Standard Form Contracting in the Electronic Age' (2002) 77(2) New York University Law Review 429; Melvin Aron Eisenberg, 'The Limits of Cognition and the Limits of Contract' (1995) 47(2) Stanford Law Review 211; Genevieve Helleringer and Anne-Lise Sibony, 'European Consumer Protection Through the Behavioral Lense' (2017) 23(3) Columbia Journal of European Law 607.

[109] Korobkin (n 108) 1233.

[110] Jason J Kilborn, 'Behavioral Economics, Overindebtedness and Comparative Consumer Bankruptcy: Searching for Causes and Evaluating Solutions' (2005) 22(1) *Emory Bankruptcy Developments Journal* 13, 21. See also Jon D Hanson and Douglas A Kysar, 'Taking Behavioralism Seriously: The Problem of Market Manipulation' (1999) 74(3) *New York University Law Review* 630, 678–680; Cass R Sunstein, 'Behavioral Analysis of Law' (1997) 64(4) *University of Chicago Law Review* 1175, 1193–4.

[111] Consumer Protection Act 2019 (India).

V. Conclusion

The proposed Indian *Personal Data Protection Bill 2019* takes steps to ensure that consent to personal data processing in India is informed and meaningful. It does not, however, stop there. The Bill seeks also to recognise more broadly the conditions necessary for trust in a modern information economy; placing responsibilities on organisations to not abuse the inevitable inequities in relative bargaining positions. The Srikrishna Committee, commenting on the proposed Bill, recognised the importance of consent as a safeguard but emphasised also that a privacy and data protection framework must serve 'the common good'.

We have not sought to answer the perennial question, 'What constitutes the common good?'. We have, however, suggested that whether one's sympathies lie toward a 'market individualist' or 'consumer welfarist' ideal of society, there are merits in a substantive test for 'fair processing'. Whether the intent is only to safeguard the ability of the individual to take decisions, or to protect interests and values beyond individual autonomy and information self-determination, it is necessary to go beyond consent. The role of a data fiduciary, as currently conceived under the Indian *Personal Data Protection Bill 2019*, gives more substance to the idea of what it means for a data controller to act fairly in relation to a data subject than has hitherto been applied by data protection authorities in Europe. It goes beyond the idea that organisations should be transparent and avoid misleading or deceptive practices. It places a responsibility upon the organisation to act in a way that is both 'fair and reasonable'.

Interpretation and application of 'fair and reasonable' under Indian law will be shaped by the case of *Justice KS Puttaswamy* v. *Union of India* (2017). In this case the Indian Supreme Court established the right to privacy is a fundamental right under Article 21 of the Indian Constitution. The Supreme Court indicated data protection and informational privacy is encompassed by the right to privacy. One can expect there to be normative implications associated with this pedigree; divorcing the right to data protection from a right to privacy in European data protection law may lead to different expectations being considered to be reasonable. The opacity of key concepts and their interconnectedness, concepts such as autonomy, liberty and human dignity, leaves a lot of scope for judicial interpretation of a 'reasonable expectation' in both jurisdictions. Different explanations for right to privacy, and its relationship with data protection, have different implications for scope and content of a right to fair processing, and the relationship to, and function of, individual consent as a safeguard. While the proper function of consent

may remain obscure while the philosophical underpinnings are moot, there is little doubt that it is no longer sufficient a device to progress even an individualist agenda.

A thin notion of consent that is not buttressed by other kinds of protection, both procedural and substantive, does not guarantee either autonomy or privacy. This is not to undermine the significance of consent. On the contrary, our argument is that if properly supported by a substantive test of fairness, there is less need to operate with the high threshold for valid consent that may discourage reliance upon consent as the legal basis for processing. The proper response to a recognition that consent is currently 'broken' in many online contexts is neither to abandon it, nor to try to fix it by ever higher thresholds for valid consent. The proper response is to complement it with other safeguards that protect the underlying values and interests at stake. Whether these are articulated in ways that display individualist or welfarist tendencies, there is an important role to be played by a test for 'fair and reasonable' processing: guaranteeing that data will not be processed for ends that may be harmful to data principals or which go beyond their reasonable expectations.

Although the judgment in *Puttaswamy* shows the ambivalence we have noted, the point is that whichever conception of privacy is preferred, and whatever that means for the role of consent within privacy and data protection law, there has been a recognition in India that it is necessary to move beyond consent to a more substantive test of 'fair and reasonable'. Consent and substantive fairness protections should not be seen as diametrically opposed requirements, one presenting respect for individual's right themselves to make the decisions that affect their lives and the other a paternalistic intrusion by the state to promote collectivist goals. Rather, once it is recognised that there are limits to the work that can be done by consent in protecting individuals' reasonable expectations of privacy, then substantive safeguards may be seen as both autonomy enhancing, by allowing individuals scope to live their lives to the fullest without being responsible for endless decisions affecting their future selves, as well as promoting more collectivist goals. Indeed, those goals of substantive fairness may be seen as an expression of community expectations that the state will indeed take actions to protect the interests of its citizens in order to preserve fundamental values that benefit them individually and as members of a community, both presently and into the future.[112]

[112] Cartwright (n 1) 37. See also Mindy Chen-Wishart, 'Controlling Unfair Terms: Protecting the Institution of Contract' in Louise Gullifer and Stefan Vogenauer (eds), *English and*

VI. Acknowledgements

We would like to sincerely thank Radhika Sarda and Devansh Kaushik, LLB (Hons) candidates at the National Law School of India University for their assistance with the preliminary research for this article and for the very helpful and constructive comments of the anonymous reviewer. We would also like to sincerely thank Yi Tung, JD Candidate at the University of Melbourne for assistance with referencing, formatting and copy-editing the final work. We are very grateful for the valuable help provided. This would not have been written without you.

European Perspectives on Contract and Commercial Law: Essays in Honour of Hugh Beale (Hart Publishing, 2017) 105.

Drug Clinical Trials Legislation In The European Union

*Paola Sangiovanni, Flavio Monfrini and Marco Bertucci**

I. Introduction

The purpose of this article is to illustrate the basic tenets of European Union law on clinical trials. Such body of law has been progressively harmonized in the European Union over the years with the aim of subjecting interventional clinical trials conducted in any of the 27 European Union Member States to identical rules.

The article initially describes the reasons why clinical trials are important to measure the safety, efficacy and cost-effectiveness of innovative medical treatment. It then continues by illustrating the scope and basic principles of the current EU Regulation, as well as its main changes over the previous legislation. Further, the article explains the requirements of the scientific and the ethical approvals of a clinical trial application. Lastly, the authors focus on the patients' consent to the enrolment in a clinical trial, as well as to the patients' separate consent to the processing of their personal data.

* The authors are Partners, Gitti and Partners, with an expertise in commercial and corporate law and regulatory matters. They would like to thank Karthik Rai and Vasu Agarwal, students at the National Law School of India University, for their invaluable research assistance in coming up with this paper.

The European Union harmonized body of law is not only relevant within the EU borders: European Union rules also play a significant role for contract research organizations and research institutions operating outside the European Union because – as the article points out - clinical trials conducted outside the European Union, but referred to in a clinical trial application within the European Union, must comply with regulatory requirements that are at least equivalent to those applicable in the European Union.

II. Drug Clinical Trials: Why, Who and What

2.1 Drug Clinical Trials: Why They Matter. Recently, the Covid-19 pandemic crisis has shown that innovation is key to resolving this momentous health issue: "*In these extraordinary circumstances, we need to unleash the full power of science, to deliver innovations that are scalable, usable, and benefit everyone, everywhere, at the same time*".[1] However, some[2] argue that "[…] *the continued expansion of health care costs is largely the result of innovation that tends to have low productivity*". As States, as well as private citizens, invest tremendous resources in healthcare,[3] it is important to identify medicinal products and med-tech solutions that are safe, efficacious and cost-effective.

Clinical trials are a key tool through which new drugs are ultimately measured. "*Clinical trials can show researchers what does and doesn't work in humans that cannot be learned in the laboratory or in animals*".[4] The healthcare industry, as well as physicians,[5] rely on research that tests medicinal products throughout various phases of scientific trials, as "*External clinical evidence both invalidates previously accepted diagnostic tests and treatments and replaces them with new ones that are more powerful, more*

---

1 WHO Director-General's opening remarks at the media briefing on COVID-19 – 15 May 2020.

2 Eli M. Cahan, Robert Kocher Roger Bohn 'Why Isn't Innovation Helping Reduce Health Care Costs?' *Health Affairs Blog* of June 4, 2020.

3 Erixon, Fredrik, and Erik Van der Marel, 'What is Driving the Rise in Health Care Expenditures?: An Inquiry into the Nature and Causes of the Cost Disease.' *European Centre for International Political Economy*, 2011.

4 Robert L. Ferris, MD, PhD, in LifelineLetter, March/April 2017.

5 Evidence based medicine relies on the best available external clinical evidence. "*By best available external clinical evidence we mean clinically relevant research, often from the basic science of medicine, but especially from patient centred clinical research into the accuracy and precision of diagnostic tests (including the clinical examination), the power of prognostic markers, and the efficacy and safety of therapeutic, rehabilitative, and preventive regimens*." *Sackett, David L., et al* 'Evidence Based Medicine: What it is and What it isn't: It's About Integrating Individual Clinical Expertise and the Best External Evidence,' *BMJ: British Medical Journal*, vol 312, Nos 7023, 1996, pp 71–72.

accurate, more efficacious, and safer."[6] In conclusion, "*Randomized controlled trials are the gold standard tool for evaluating interventions*".[7]

2.2 The Actors on the Stage of Clinical Trials. Clinical trials always require at least three different subjects working together:

(a) a sponsor of the trial, i.e., an individual, company, institution or organization which takes responsibility for the initiation, management and financing of the clinical trial;

(b) an investigator, who is an individual responsible for the conduct of a clinical trial at a clinical trial site;

(c) a clinical trial site where the trial is conducted; and

(d) patients who participate in a clinical trial either as recipients of an investigational medicinal product or as part of a control group.

The "script" of the clinical trial is set out in the protocol of the clinical trial, which is defined as "*a document that describes the objectives, design, methodology, statistical considerations and organization of a clinical trial.*"[8]

It is of paramount importance that all the above subjects have specifically regulated roles and responsibilities, so they may work in-sync in order to obtain reliable data that can be the basis of clinical findings. As it has been stated,[9] "*It is only with open dialogue that sponsors, health care providers, government regulators and – most importantly – trial participants and the public will become comfortable that clinical trials are not exploitative but fair, necessary and often beneficial. Transparency in that debate and dialogue is critical.*"

III. Clinical Trials in the European Union

3.1 Clinical Studies vs. Clinical Trials. According to the current definition given by the European Union Regulation number 536/2014 (hereinafter the "***Regulation***"), a clinical study is a simpler investigation compared to a clinical trial. In fact, while a clinical study intends to discover the effects of a

---

[6] Again, Sackett, David L., et al 'Evidence Based Medicine: What it is and What it isn't: It's About Integrating Individual Clinical Expertise and the Best External Evidence,' BMJ: British Medical Journal, vol 312, Nos 7023, 1996, pp 71–72.

[7] Ioannidis, John P.A. 'Clinical Trials: What a Waste,' BMJ: British Medical Journal, vols 349, 2014.

[8] The definition of "protocol" is provided by art 2.2(22) of the Regulation.

[9] Li, Rebecca, et al 'Global Clinical Trials: Ethics, Harmonization and Commitments to Transparency,' Harvard Public Health Review, vol 6, 2015, pp. 1–7.

medicinal product, identify adverse reactions and study its functioning in the human body,[10] a clinical study "upgrades" to a clinical trial, or interventional trial, when the investigation does not fall within normal clinical practice.[11]

In other words, a clinic trial entails, by its nature, a deviation from standard clinical practice and, as such, is subject to additional legal requirements, given that the clinical trial may pose new risks to the safety of the study subject arising "*from two sources: the investigational medicinal product and the intervention*".[12]

The Regulation applies only to drug clinical trials (and not to clinical studies in general, or non-interventional studies). In fact, the deviation from the normal clinical practice – which defines, instead, clinical trials - represents the key factor reflecting additional risks and justifying a more rigorous approach.The distinction between interventional and non-interventional studies is of the utmost importance, as the inclusion of a certain clinical study in one category or the other could lead to greater freedom for Member States, who are not bound by the provisions of the Regulation with regard to non-interventional studies.

Regulators will also need to be careful that studies, which are interventional in nature, are not mislabelled as non-interventional. In such case, a trial posing higher risks to patients would be concealed as posing no risks for patients and the stricter regime set out in the Regulation would be circumvented.

---

[10] The following definition of clinical study is provided by Article 2.2(1) of the Regulation: "[...] *an investigation relating to humans intended (a) to discover or verify the clinical, pharmacological or other pharmacodynamic effects of one or more medicinal Products; (b) to identify any adverse reactions to one or more medicinal products; or (c) to study the absorption, distribution, metabolism and excretion of one or more medicinal products; with the objective of ascertaining the safety and/or efficacy of those medicinal products.*"

[11] The following definition of clinical trial is provided by Article 2.2(2) of the Regulation: "[...] *the assignment of the subject to a particular therapeutic strategy is decided in advance and does not fall within normal clinical practice of the Member State concerned; the decision to prescribe the investigational medicine product is taken together with the decision to include the subject in the clinical study; or diagnostic or monitoring procedures in addition to normal clinical practice are applied to the subjects".*

[12] Preamble No 11 of the Regulation.

IV. European Union Legislation on Clinical Trials on Drugs: Main Principles and how it Evolved

4.1 EU Directive 2001/20/CE. The European Union has recognized the importance of the issue of clinical trials and attempted to provide harmonized regulatory solutions for the past 20 years. The initial effort to harmonize regulations of various Members States occurred through a directive. According to European Union law, a directive is only binding as to its goals, while Member States are free to enact different provisions in order to reach such goals.

Directive number 2001/20/CE (hereinafter the "***Directive***") was enacted in 2001 in order to provide certain basic rules mandatory for Member States in relation to drug interventional trials (non-interventional or observational trials are not covered by the Directive and are mostly regulated by national legislation of Member States). The main goal of the Directive was to ensure the application of good clinical practice in the conduct of clinical trials.[13]

The Directive concerns clinical trials of medicinal products and does not apply to non-interventional clinical trials. The principal aim of the Directive is the protection of clinical trial subjects.[14] Further protection measures are constituted by the role of a qualified physician acting as investigator in the trial and the requirement that the trial must be conducted in compliance with good clinical practice.

Further, the Directive provides that a clinical trial, prior to it being conducted, has to be authorized by at least two distinct bodies: (1) a national competent authority, which assesses compliance with the Directive's requirements, and (2) an ethical committee, that each Member State is free to regulate.[15] The clinical trial is thus separately assessed both from a scientific and an ethical point of view.

The ethical point of view has always been an important pillar of European Union clinical trial regulations, and remains so on the basis of the idea that

---

[13] In Italy such Directive has been implemented by means of Legislative Decree No 211/2003, while other European members had issued their own national laws.

[14] "*[…] a clinical trial may only be undertaken if the risks to the subject are not disproportionate to the potential benefits of the medical research. On the other hand, the right of the subject to physical and mental integrity must be respected, as well as the right to privacy.*" From the summary of the Directive provided on the EUR LEX website:<https://eur-lex.europa.eu/legal-content/EN/LSU/?uri=CELEX:32001L0020>.

[15] According to the definition of 'Ethics committee' provided by the Regulation, such committee should take into account the views of laypersons, in particular patients or patients' organisations.

human beings' needs and dignity should never be neglected. It is in fact possible to imagine a potential conflict between scientific research, aiming at discovery and innovation, and the safety, wellbeing and dignity of human beings. Clinical research should never go "too far" and thwart the rights of individuals, which must always be protected, and such protection cannot be limited to requesting consent of the study subject.

4.2 Goals of Simplification and Harmonization Fail under the Directive. It is widely accepted that the Directive did not achieve its intended goals of harmonization (i.e., making uniform the various national rules of single Member States)[16] and of simplification (allowing an expedite assessment of the trial application).[17] In fact, the Directive has been heavily criticized by researchers,[18] as well as by sponsors and patients' associations. As admitted also by the European Union legislator, "*[…] the Clinical Trials Directive is arguably the most heavily criticised piece of EU-legislation in the area of pharmaceuticals. This criticism is voiced by all stakeholders - patients, industry, and academic research*"[19] and "*[…] experience shows that a harmonised approach to the regulation of clinical trials has only been partly achieved. This makes it in particular difficult to perform a given clinical trial in several Member States.*"[20]

The system set up by the Directive in fact prolonged the average waiting time to commence clinical trials, increased the costs of conduct of the trial (both the trial costs and the insurance costs), and significantly decreased the number of trials conducted under the Directive. In 2009/2010 the European Commission arranged for a public consultation on the Directive, which

---

[16] Hartmann, M. 'Impact Assessment of the European Clinical Trials Directive: A Longitudinal, Prospective, Observational Study Analyzing Patterns and Trends in Clinical Drug Trial Applications Submitted Since 2001 to Regulatory Agencies in Six EU Countries', Trials 13, 53 (2012).

[17] Giannuzzi V., Altavilla A., Ruggieri L., Ceci A. 'Clinical trial application in Europe: what will change with the new regulation?' Sci Eng Ethics. 2016; 22: 451-466.

[18] "*According to the Council of the European Union, between 2007 and 2011 the number of applications for clinical trials decreased by 25% in the EU. This is partially attributed to the Clinical Trials Directive of 2001, which ensured a high level of patient safety, but an unfavorable regulatory framework not only for pharmaceutical companies, but also for academic research in general. The Directive caused, for example, increases in staff requirements for sponsors, insurance fees, and administrative costs. As a result, many pharmaceutical companies and academic researchers felt discouraged to submit new applications within the EU.*" Yves Geysels, Christopher A. Bamford, Richard H. Corr 'The New European Union Regulation for Clinical Trials', Clinical Researcher, The Association of Clinical Research Professionals, February 1, 2017.

[19] Paragraph 1 of the Proposal of the Regulation proposal: <https://ec.europa.eu/health//sites/health/files/files/clinicaltrials/2012_07/proposal/2012_07_proposal_en.pdf>.

[20] Preamble 4 of the Regulation.

exposed its weaknesses.[21] In short, the European Union had become a much less attractive region for conducting multi-centre clinical trials.

The Goals of the 2014 Regulation. The Regulation was born to address the Directive's shortcomings, and particularly to target the goals of harmonization and simplification in this field, also with a view of making Europe a competitive region in the global clinical trials market.

4.3.1 Harmonization. With regard to harmonization, the Regulation is a different legislative instrument compared to a directive: while a directive is only binding on Member States with regard to its goals, a regulation applies in the exact identical way in all Member States. Given that the letter of clinical trial rules will be identical rules in all 27 Member States, it would appear that the goal of harmonization is within easy reach. However, in practice, certain areas of the Regulation are still left to Member States' legislation. In particular, as it will be better illustrated in paragraph 5 below, the ethical revision of trials continues to be up to ethical committees, which Member States may regulate autonomously ("*The ethical review shall be performed by an ethics committee in accordance with the law of the Member State concerned*"[22]).

4.3.2 Simplification. A second important achievement of the Regulation is the unification of the process of authorization of the trial, which will be coordinated among national competent authorities. The earlier de-centralized system will be replaced by a centralized system, whereby a single application dossier will be submitted to all the Member States concerned through a single submission portal (hereinafter the "***EU Portal***"). The process of authorization entails the cooperation of various national competent authorities involved in the authorization of the trial, which will however lead to a single decision. The same EU Portal will be used to notify the sponsor of such decision, setting forth "*as to whether the clinical trial is authorised, whether it is authorised subject to conditions, or whether authorisation is refused*".[23] Such EU Portal will also be used as a single database for any safety communication relating to the safety of the study drug and of the trial. It is expected that the cooperation of Member States through this digital platform will also lead to easier authorization and conduct of multi-centred European Union clinical trials.

---

[21] The responses of the consultation can be found here: <https://ec.europa.eu/health/sites/health/files/files/clinicaltrials/2010_03_30_summary_responses.pdf>.

[22] Art 4 para 2 of the Regulation.

[23] Art 8 of the Regulation.

4.4 Open Results of the Trial. Irrespective of the outcome of a clinical trial, within one year from the end of a clinical trial in all Member States concerned, the sponsor must submit to the European Union database a summary of the results of the clinical trial, accompanied by a summary written in a manner that is understandable to laypersons.[24] The ability to have open and shared sets of clinical data will enable researches to have access to grounds for further research.[25]

4.5 Novelties and Other Aspects of the Regulation. It is clear that most innovations will be a consequence of the implementation of the EU Portal. This feature of the Regulation is quite meaningful as it has been noted that "*Perhaps the most significant novel aspect of the Clinical Trial Regulation is the establishment of the EU Portal, a "one-stop shop" through which sponsors can apply for an authorization to conduct a clinical trial in any number of Member States.*"[26]

Great benefits in terms of harmonisation will also derive from the uniform set of documents, listed in Annex I of the Regulation, which will be required for the application. Such documents will be the same across the European Union and will include a cover letter, the complete European Union application form, the protocol, the investigator's brochure, the documentation relating to the compliance to good clinical practices and the investigational medicinal product dossier. Such uniform set of documents, once the EU Portal will be available, will surely simplify the submission of the applications, regardless of the Member States involved in the process.

The Regulation also introduced the Clinical Trials Coordination and Advisory Group ("**CTAG**")[27]. The new body will serve as a forum for exchanging best practices between Member States, in accordance with the harmonisation goal pursued by the Regulation. In particular, CTAG will: (i) support the exchange of information between the Member States and the Commission on the experience acquired with regard to the implementation

---

[24] Art 37 para 4 of the Regulation.

[25] "*With each of these advances we get closer to having all trials registered and all results reported. The next challenges are how to normalise and standardise the release of anonimysed individual patient data from trials and how to restore hidden data from old trials. But let's pause briefly to appreciate how far we have already come.* Europe's drug regulators and legislators, and everyone who has campaigned for and supported transparency, deserve much credit for holding their nerve and doing the right thing for public health." Groves, Trish. 'Big Strides in Europe towards Clinical Trial Transparency' BMJ: British Medical Journal, vol 349, 2014.

[26] Pavlou, Anna, and Emmanuel Saurat. 'Clinical Trials Regulation: A Further Step towards Increased Medical Innovation in the EU,' European Journal of Risk Regulation, vol 6, No 4, 2015, pp 646–648.

[27] Art 85 of the Regulation.

of the Regulation; (ii) assist the Commission in providing the support for the cooperation of Member States; and (iii) draft recommendations on criteria regarding the selection of a reporting Member State.

4.6 The Entry into Force of the Regulation. The EU Portal, as well as the European Union database where all information submitted through the EU Portal will be stored, supposedly one of the highpoints of the Regulation, is probably its worst enemy so far. In fact, the entry into force of the Regulation shall occur six months after the publication of a notice whereby the European Commission confirms that the EU Portal and the EU database have achieved full functionality and the systems meet the required functional specifications. This has not happened yet, although the Commission has continued to state that this is imminent.[28] Therefore, so far, the Directive continues to apply, while some argue that the Regulation – that appeared cutting edge in 2014 – already shows the signs of age.

V. Ethical Review of Clinical Trials

5.1 The *Rationale* behind the Ethical Review. The previous section of this article focused on the required authorization by regulatory authorities of a clinical trial from a scientific standpoint. We now turn to consider the other fundamental requirement for clinical trials: ethical approval of trials. In fact, the Regulation provides for an additional and separate assessment of a proposed clinical trial: an ethical review of the trial at a national level. This further assessment allows the process to develop also outside the scientific arena and to involve patients and citizens, who obviously need to trust the sponsors and investigators, but have the statutory right to be directly involved.

Although the Regulation does not expressly state the *rationale* behind the need for an ethical review, the importance of such ethical assessment can be inferred by certain indications given by the Regulation in its introductory preambles. For example, Preamble 18 of the Regulation sets forth that ethical reviews are required in order to ensure the involvement of laypersons, in particular patients or patients' organisations, in the process.

---

[28] "*Due to technical difficulties with the development of the IT systems, the portal's go-live date had to be postponed and therefore the EU Clinical Trial Regulation will come into application during 2020 instead of October 2018, as previously scheduled.*" (European Union Commission website). "*The product owners will work with EMA and the IT supplier to analyze and design these items in the first few months of 2020, in a way that ensures efficient delivery.*" (EMA website).

Further, the same Preamble also provides that ethics committees are meant to involve all the expertise necessary to look at the study from various points of view. In accordance with international guidelines, the ethical assessment should be carried out jointly by a reasonable number of persons who collectively have all the necessary qualifications and experience, without limitation to a single field. Such requirement can be set forth in different ways by Member States, but international guidelines, such as the World Health Organization's Standards and Operational Guidance for Ethics Review of Health-Related Research with Human Participants, suggest including at least individuals with expertise in behavioral or social sciences, health care providers, experts in legal matters and/or ethics, and lay people, whose primary role is to share their insights about the communities from which participants are likely to be drawn.[29]

Ethics committees must be independent from the sponsor, the clinical trial site and the investigators involved, as well as free from any other undue influence. Such a principle is also mentioned in Preamble 18, but Member States are free to determine their implementing measures to guarantee independence. Again, international standards provide some guidance.[30] To ensure that the ethics committees cannot be pressured to approve or reject particular protocols, the ethics committee's membership should include at least one person with no connection to the organization that sponsors or conducts the trial. Moreover, researchers, sponsors and funders may attend the ethics committees' meetings only to answer questions about their research protocols and associated documents, but their participation shall not be allowed when the committee reaches decisions about the proposed research. Measures should also be taken to ensure that committees' members are protected from retaliation based on positions taken with respect to the review of research projects.

5.2 Discretion of Member States in the Field of Ethical Review. While the scientific assessment of clinical trials is subject to a detailed harmonised procedure by the Regulation,[31] the Regulation approach is completely different in relation to the ethical review of clinical trials. In fact, the Regulation

---

[29] Standard 2 (Composition of research ethics committees) of WHO's Standards and Operational Guidance for Ethics Review of Health-Related Research with Human Participants, <*https://apps.who.int/iris/bitstream/handle/10665/44783/9789241502948_eng.pdf;jsessionid=15A876B1B012E6A09A206E10E26F7155?sequence=1*>.

[30] Standard 4 (Independence of research ethics committees) of WHO's Standards and Operational Guidance for Ethics Review of Health-Related Research with Human Participants, <*https://apps.who.int/iris/bitstream/handle/10665/44783/9789241502948_eng.pdf;jsessionid=15A876B1B012E6A09A206E10E26F7155?sequence=1*>.

[31] Arts 6 and 7 of the Regulation.

merely requires that the ethical review is performed by an ethics committee in accordance with the law of the Member State concerned.[32]

While such ethical review may encompass aspects listed in the Regulation, each Member State is granted with a fairly high degree of discretion to such regard: in fact, the mandatory provisions of the Regulation only require Member States to ensure that the timelines and procedures for the review by the ethics committees are compatible with the timelines and procedures set out in the Regulation for the scientific assessment of the application. In other words, the Regulation appears to be more concerned about the timing of the ethical review than the substance of it.

Such difference may allow Member States within the European Union to opt for different solutions with regard to the regulation of ethical reviews of clinical trials, thus impairing the goal of harmonization. Some States may even be ready to exploit this level of discretion and design their regulatory environment to be more attractive for the industry. Others may adopt or maintain a more restrictive ethical review framework. The Regulation thus allows for different ethical standards to coexist, if not to compete against each other.

Some have argued that the ethical committee's review under the Regulation is limited to the grounds set out in Articles 6 and 7 of the Regulation and thus is too restricted. "*In essence, this unreasonably limits the ethics committee to consideration of consent issues, confidentiality issues and suitability and recruitment of participants. This amounts to a drastic curtailment of the issues that ethics committees normally, and indeed must, consider.*"[33]

The timing of the ethical and the scientific reviews must be linked: Member States must complete the ethical review within completion of the scientific review process. With specific regard to timing of the scientific assessment, the Regulation grants to the reporting Member State a 10-day term from the submission of the dossier through the EU Portal to validate the application, taking into account the considerations expressed by the other Member States concerned, if any. Member States concerned can communicate any considerations relevant to the validation of the application within seven days from the submission of the application dossier.[34] From the validation of the dossier, the reporting Member State and each Member State concerned shall

---

[32] Art 4 of the Regulation.

[33] Shaw, David, and David Townend "*Division and Discord in the Clinical Trials Regulation.*" *Journal of Medical Ethics*, vol 42, No 11, 2016, pp 729–732.

[34] Art 5 of the Regulation.

complete their assessment within 45 days.[35] Certain Member States have attempted to rationalize the previously existing network of ethical committees in order to render the ethical review of clinical trials more efficient and faster.[36]

VI. A Patient Perspective: Consent to Participation in The Study and Processing of Personal Data

6.1 Consent by the Study Subjects to Participate in the Clinical Trial. Our analysis of the Regulation would not be complete without focussing on a key requirement of a clinical trial: patients' consent. From the perspective of a patient, it is important to underline that no clinical trial can occur without the study subject expressly consenting to participate in it. In fact, long-standing ethical standards in the clinical research field require two basic components: informed consent and independent ethical oversight.[37] These components ensure that the participation of any individual in a clinical research is not only informed and free, but also complies with high ethical standards and respects human dignity.

The subject's consent under the Regulation aims at ensuring that ethical standards are met and the freedom of the patient is safeguarded.[38] Such consent is an essential requirement for the participation of the subject in a clinical trial. The Regulation sets forth such requirement in Article 29, which describes in detail all the information that must be provided to the patient in a prior interview with a member of the investigating team, in order to allow the patient to take an informed decision concerning the participation in the trial.[39] The information to be given to the patient includes, by way of

---

[35] Art 7 of the Regulation.

[36] Italy, for example, had an impressive number of ethical committees, almost one for each hospital. Italian law n 3 of 2018 on clinical trials provides for a reduction and simplification of ethics committees, but delegates to further governmental decrees, not yet enacted, the promising results anticipated by the law. Therefore, Italy, which currently has a 20% share of the European Union's clinical trials, is attempting to set up a regulatory framework that will continue to render it an attractive destination for clinical trials, as evidenced by the eighteenth national report of the Italian Medicines Agency "AIFA" for year 2019, available here <*https://www.aifa.gov.it/documents/20142/241052/18-Rapporto-OsSC_03.10.2019.pdf/4694ddbe-8f65-68b4-ac3a-cd0e883fd982*>.

[37] European Data Protection Supervisor, "*A Preliminary Opinion on Data Protection and Scientific Research*", January 6, 2020.

[38] European Commission, "Questions and Answers on the interplay between the Clinical Trial Regulation and the General Data Protection Regulation".

[39] Art 29, para 2, of the Regulation provides that: "*Information given to the subject or, where the subject is not able to give informed consent, his or her legally designated representative for the purposes of obtaining his or her informed consent shall: (a) enable the subject or his or her legally designated representative to understand: (i) the nature, objectives,*

example, risks and inconveniences of the clinical trial and the patient's rights and guarantees (including the right to refuse to participate and the right to withdraw from the clinical trial at any time without any resulting detriment and without having to provide any justification). Furthermore, the information given to the patient must be comprehensive, concise, clear, relevant and understandable to a layperson.[40]

Once the patient is provided with all required information under the Regulation, the informed consent must be formalized in writing, must be dated and signed by both the patient and the member of the investigating team performing the interview with the patient. The Regulation also sets forth specific provisions applicable to particular categories of study subjects, in order to safeguard their rights and integrity, such as minors, incapacitated persons, pregnant or breastfeeding women.[41]

6.2 Consent to Allow Processing of Data within a Clinical Trial. The study subject must also expressly and separately allow for the processing of her/his personal data within the context of a clinical trial. Such consent cannot be implied by the consent to participate in the clinical trial.

The informed consent under the Regulation and the consent to the processing of personal data under the General Data Protection Regulation (EU)

---

benefits, implications, risks and inconveniences of the clinical trial; (ii) the subject's rights and guarantees regarding his or her protection, in particular his or her right to refuse to participate and the right to withdraw from the clinical trial at any time without any resulting detriment and without having to provide any justification; (iii) the conditions under which the clinical trial is to be conducted, including the expected duration of the subject's participation in the clinical trial; and (iv) the possible treatment alternatives, including the follow-up measures if the participation of the subject in the clinical trial is discontinued; (b) be kept comprehensive, concise, clear, relevant, and understandable to a layperson; (c) be provided in a prior interview with a member of the investigating team who is appropriately qualified according to the law of the Member State concerned; (d) include information about the applicable damage compensation system referred to in Article 76(1); and (e) include the EU trial number and information about the availability of the clinical trial results in accordance with paragraph 6."

[40] The risks of information overload have been often underlined: "*Adequately informing patients, as explained above, is key, but is a delicate and sensitive process that needs to be adapted to each patient's health literacy. The regulator, on the other hand, sees the need to inform patients from a more legalistic perspective. Different regulations accumulate what patients need to be informed about; consent via separate documents may sometimes be asked for (e.g. separate data protection or genetic testing documents), bringing the amount of information patients have to digest up to several dozens of pages. This approach does not help them to make an informed decision, as it may dilute the key questions patients need to focus on by the amount of administrative and legalistic details mandatory by law.*" Negrouk, Anastassia, et al "Clinical Trials, Data Protection and Patient Empowerment in the Era of the New EU Regulations" *Public Health Genomics*, vol 18, No 6, 2015, pp 386–395.

[41] Arts 31 to 35 of the Regulation.

2016/679 ("***GDPR***") are two distinct consents and serve different purposes. The consent under the Regulation aims at ensuring that ethical standards are met and the freedom of the patient is safeguarded.[42] Such consent is a procedural condition for the participation of the subject in a clinical trial. On the other hand, consent to the processing of personal data in the framework of a clinical trial allows the lawful processing of such data.

The entry into force of the GDPR brought novelties also with regard to the legal grounds for the processing of personal data in the conduct of clinical research. Consent to the processing of personal data in the framework of a clinical trial is one of the legal grounds allowing the lawful processing of personal data. Public interest and legitimate interest are also grounds for processing, which may be validly be used under certain circumstances.

With regard to the legal grounds of the processing, Member States appear to have taken different, often opposing, approaches. In certain instances, the consent of the patient to the processing of his/her personal data is viewed as essential for the conduct of the research. In other cases, the legitimate interest of the sponsor is considered to be the main ground for processing. While the debate is still open, the current interpretations and positions adopted by different Member States may end up undercutting one of the main goals of the GDPR, which was to ensure a uniform legal framework throughout the 27 Member States.

It should also be pointed out that, whenever consent is chosen as the legal ground for the processing of personal data in the framework a clinical study, such consent may always be withdrawn by the study subject pursuant to the provisions of the GDPR. If the subject withdraws his/her consent under the Regulation, such withdrawal does not necessarily affect the processing of data gathered in the trial. In fact, if the patient withdraws his/her consent under the GDPR, all data processing operations that were based on such consent remain lawful, but no further processing may occur and – if there is no other legal ground under the GDPR, such as legal obligations of the sponsor for purposes of ensuring safety – the data should be deleted.[43]

6.3 Interactions between the Regulation and Data Protection Legislation. The Regulation, which was devised in 2014 in order to overhaul the governance of clinical trials in the European Union, will become applicable in a legislative framework deeply changed by the subsequent entry into force

[42] European Commission, 'Questions and Answers on the Interplay between the Clinical Trial Regulation and the General Data Protection Regulation', April 10, 2019.

[43] European Commission, *Questions and Answers on the Interplay between the Clinical Trial Regulation and the General Data Protection Regulation*.

of the GDPR. The interconnection between the Regulation and the GDPR has been the subject of several studies by scholars and regulators. It has been recognized that the GDPR assigns to scientific research a more favourable regime,[44] but as of today there have been few comprehensive studies on the application of data protection rules to research.[45] As a consequence, several matters, questions and issues concerning the protection of personal data in the framework of clinical studies remain open for debate and interpretation, both at the European level and at Member States' level.

The outbreak of the COVID-19 pandemic prompted additional guidelines from European Union regulators and new guidelines were issued on April 21, 2020 by the European Data Protection Board.[46] Such guidelines clearly confirmed that consent is only one of the available legal bases for the processing of personal data under the GDPR and there is no ranking or preference among them. Furthermore, the guidelines reiterate that consent may not be a valid legal basis for data processing under certain circumstances, for instance if there is a clear imbalance between the study subject and the data controller (i.e., the research site or investigator). In this latter case, other legal bases, such as public interest, maybe more suitable to protect the rights of the patient to have his/her personal data processed according to the Regulation.

6.4 GDPR Only Partially Achieves Uniformity. One of the main goals pursued by the GDPR was to ensure a more uniform approach to data protection legislation across the European Union. In the past, the previous directive governing data protection in the European Union allowed Member States broad discretion in its implementation. This caused significant differences in legislation among the Member States and *de facto* hindered the conduct of

[44] The importance of scientific research for the ultimate benefit of individuals and society is enshrined in the GDPR itself (Recital 157 of the GDPR), which states that "*by coupling information from registries, researchers can obtain new knowledge of great value with regard to widespread medical conditions such as cardiovascular disease, cancer and depression. On the basis of registries, research results can be enhanced, as they draw on a larger population. Within social science, research on the basis of registries enables researchers to obtain essential knowledge about the long-term correlation of a number of social conditions such as unemployment and education with other life conditions. Research results obtained through registries provide solid, high-quality knowledge which can provide the basis for the formulation and implementation of knowledge-based policy, improve the quality of life for a number of people and improve the efficiency of social services. In order to facilitate scientific research, personal data can be processed for scientific research purposes, subject to appropriate conditions and safeguards set out in Union or Member State law*".

[45] European Data Protection Supervisor, "A Preliminary Opinion on Data Protection and Scientific Research", January 6, 2020.

[46] European Data Protection Board, *Guidelines 03/2020 on the Processing of Data Concerning Health for the Purpose of Scientific Research in the Context of the COVID-19 Outbreak*, April 21, 2020.

multinational/multi-centric clinical trials and studies in the European Union. The GDPR, being a regulation and not a directive, partially addressed such need for a more uniform legal framework.

However, the GDPR itself allows derogations by Member States on several matters, and national data protection authorities are still mainly responsible in their respective jurisdictions for the enforcement of the GDRP. Furthermore, on certain matters Member States appear headed towards different interpretations of the GDPR: for instance, certain Member States favour consent as the legal basis of choice for the processing of personal data within a clinical trial, whereas others are more inclined to favour public interest or legitimate interest as appropriate legal bases. Therefore, even if the GDPR enhanced uniformity throughout the EU, local data protection assessments of multinational research projects cannot be avoided entirely.

VII. Application of the Regulation Beyond EU Borders

7.1 Clinical Trials Conducted Outside the EU, but Referred to in an Application within the EU. The EU Regulation may also affect clinical trials conducted outside the European Union. In fact, according to Article 25 paragraph 5[47] of the Regulation, clinical trials conducted outside the European Union, but referred to in a clinical trial application within the European Union, must comply with regulatory requirements that are at least equivalent to those applicable in the European Union as regards the rights and safety of the subjects and reliability and robustness of the data generated in the clinical trial. Therefore, even when trials are conducted outside of the EU (for example, in India), it is essential to ensure that the principles of the Regulation are duly taken into consideration, if the data generated in such trials will be referred to in an EU application dossier.

Furthermore, European Union controls in Member States and third countries are mandatory under Article 79 of the Regulation. They will be carried out by the European Commission to ensure that clinical trials rules are being properly applied, even when trials are conducted outside the European Union.

---

[47] "*Where the clinical trial referred to in paragraph 4 has been conducted outside the Union, it shall have been conducted in accordance with principles equivalent to those of this Regulation as regards the rights and safety of the subject and the reliability and robustness of the data generated in the clinical trial*".

7.2 The 2015 Ban by the EU of Medicinal Products Tested in India and Developments in Indian Clinical Trial Legislation. The above discussed EU Regulation requirement echoes the 2015 suspension by the European Medicines Agency of about 700 medicinal products that were clinically tested by GVK Biosciences based in Hyderabad, India. The ban was recommended following an inspection at GVK Biosciences site at Hyderabad by the French medicines agency raising concerns over the conduct of clinical trials. It appeared that the studies conducted by GVK were flawed by systematic data manipulations that occurred over at least 5 years. The clinical studies results were therefore unreliable and thus it was recommended that, where no supporting data from other studies were available, the medicinal products were suspended. The European Medicines Agency reiterated a basic requirement: "*studies underpinning marketing authorisations in the EU are carried out to the highest standards and that the companies involved comply fully with all aspects of Good Clinical Practice (GCP)*".[48]

The European decision sparked intense political reactions on the part of the Indian government. In response, free trade talks with the European Union were cancelled by the Indian government. The then trade secretary Ms. Rita Teaotia said it was an "*expression of concern*" on India's part of an "*extremely disproportionate reaction to the perceived infringement*".[49] The Indian government, through the Central Drugs Standard Control Organization ("***CDSCO***"), probed the GVK Biosciences issue and found no manipulation of data. A further panel of experts engaged by the Indian government in October 2014 also found no manipulation of data after its investigation. The Indian government handled the GVK issue as a political and commercial problem: the Commerce Ministry said in a press release that it was "*disappointed by and concerned*" at the ban on "*one of the flagship sectors of India*".[50] The CDSCO never acted against Hyderabad's GVK Biosciences and no judicial cases about the GVK scandal ensued.

Nonetheless, the Indian government later strengthened its drug regulatory system. In particular, with regard to clinical trials regulations, the New Drugs and Clinical Trials Rules were enacted in 2019 (hereinafter the "***Rules***"). The Rules include several basic principles that appear to be aligned

---

[48] See the May 21, 2015 opinion by the European Medicines Agency on case EMEA/H/A-31/1408.

[49] Asit Ranjan Mishra, 'India hardens stance on special safeguard mechanism at WTO' (*livemint*, 11 December 2015) <https://www.livemint.com/Politics/kk9eHd7iEqIM1GjpJgw1FN/India-hardens-stand-on-special-safeguard-mechanism-at-WTO.html>.

[50] 'India-The European Union (EU) FTA: The Intellectual Property Conflict' (*Coventus Law*, 14 August 2015) <http://www.conventuslaw.com/report/india-the-european-union-eu-fta-the-intellectual/>.

with those of the European Union Regulation on drug clinical trials, e.g., (i) Consent: trial subjects will be enlisted for trials only with prior informed consent; (ii) Ethical review: an ethics committee will monitor the trials; and (iii) Compensation in case of adverse events: in case of adverse events, trial subjects will be entitled to compensation for damages suffered.[51] The aim of the new Rules is to ensure that clinical trials in India are subject to predictable, transparent and effective regulations for such trials, also to the end of ensuring easier access to new drugs by the Indian population. Under the Rules, clinical trials must be approved by the Drugs Controller General of India following a specific application. Approval or rejection times vary depending on where the drug is developed: for drugs developed outside India further information may be sought within 90 days, while in case of an application for conducting clinical trial of a new drug or investigational new drug as part of discovery, research and manufacture in India, the application is to be decided within 30 days. In case of no communication from DCGI, the application will be deemed to have been approved.

As some scholars[52] have concluded about the developments of clinical trials in India, "*many of the well-meaning requirements imposed on researchers and sponsors beginning in 2013 chilled the clinical trial environment, yet the requirements also brought appropriate attention to complex ethical issues*."

VIII. Conclusions

The above overview of the European Union regulatory framework for clinical trials on drugs illustrates the core principles of the harmonized regimen in the EU. Such regimen is important beyond EU borders due to Article 25 paragraph 5 of the Regulation, mandating that clinical trials conducted outside the European Union, but referred to in a clinical trial application within the European Union, must comply with regulatory requirements that are at least equivalent to those applicable in the European Union.

---

[51] In relation to adverse events, Drugs Controller General of India ("DCGI") S. Eswara Reddy said: "*In case of injury to clinical trial subject, medical management will be provided as long as required as per the opinion of the investigator or till such time it is established that the injury is not related to the clinical trial. Also, compensation in cases of death and permanent disability or other injury to a trial subject will be decided by the DCGI*," Reddy said.

[52] Barnes, Mark, et al, 'The Evolving Regulatory Landscape for Clinical Trials in India' *Food and Drug Law Journal*, vol 73, No 4, 2018, pp. 601–623.

Since the clinical trials industry is globally interconnected (as evidenced by the numerous trials that European pharmaceutical companies are conducting in Asia, especially in India[53]), the principles of European Union law may be a relevant benchmark for other jurisdictions, too. Furthermore, it is possible that principles of clinical trial legislations of various countries around the world (and not just Member States of the European Union) will converge in the future.[54]

[53] With regard to the percentage of clinical trials worldwide conducted in India, see Sandhiya Selvarajan, Melvin George, Suresh S. Kumar, and Steven Aibor Dkhar, 'Clinical Trials in India: Where do we Stand Globally', Perspective in Clinical Research, 2013 July-September; 4(3): 160–164.

[54] Discussions by US, EU and Japan regulators on certain issues point towards a greater coordination in various fields, including clinical trials. See, for example, the November 6, 2019 tripartite meeting's press release: <https://www.ema.europa.eu/en/documents/agenda/meeting-summary-ema-food-drug-administration-fda-pharmaceuticals-medical-devices-agency-pmda_en.pdf>.

Rising Internet Shutdowns in India: A Legal Analysis

*Shrutanjaya Bhardwaj, Nakul Nayak, Raja Venkata Krishna Dandamudi, Sarvjeet Singh and Veda Handa**

* Shrutanjaya Bhardwaj is a lawyer in Delhi and a Fellow at the Centre for Communication Governance at National Law University Delhi (CCG); Nakul Nayak was a Project Officer at CCG. He is currently a Lecturer at Jindal Global Law School; Sarvjeet Singh is a Doctoral Candidate at National Law University Delhi, Raja Venkata Krishna Dandamudi was a Research Associate at CCG, and Veda Handa is technology policy lawyer in Delhi and was a Research Assistant with CCG.

We are grateful to Rahul Narayan, Ujwala Uppaluri, and Geetha Hariharan for their inputs and review of earlier drafts of this paper, and the John D. and Catherine T. MacArthur Foundation and Access Now Grants for supporting CCG's academic work around internet shutdown from 2016-18.

I. Introduction

The central theme of this paper is to critically study the interplay of internet shutdowns with the right to freedom of speech and expression.[1] We use the phrase "internet shutdown" broadly to mean any intentional act on part of the State to disrupt – totally or partially – access to the Internet for people in a particular area.[2] In a *total* shutdown, the State completely cuts off all internet access in the area. In a *partial* shutdown, the State may adopt one (or a combination of) the following options: (i) blocking specific websites and content, (ii) disrupting internet access through specific mediums, such as mobile networks, while leaving other mediums such as wired broadband free to access the internet, and (iii) lowering the network speed, e.g. from 4G to 2G.

A study of this nature is necessitated by India's abysmal record with internet shutdowns. Indeed, recourse to shutdowns has become quite routine in the country.[3] India has had at least 397 instances of internet shutdowns since 2010.[4] In 2019 alone there were at least 106 instances of which 55 were imposed in the erstwhile[5] State of Jammu & Kashmir.[6] Between 2012-17,

---

1 The discussion in this paper is not to preclude the application of other rights. In addition to communication, a shutdown also directly impacts non-communicative online activities that are increasingly becoming essential to our everyday lives. For instance, a shutdown would prevent the reservation of train tickets out of a town in turmoil or booking a cab from the airport to a hotel. Some of these online activities are not only harmless but also potentially lifesaving in areas facing unrest. Indeed, during an epidemic and a nationwide lockdown, shutdowns could well mean a denial of education and health services. *See* Memorandum of Writ Petition, *Foundation for Media Professionals v UT of J&K*, (2020) 5 SCC 746, available at <https://drive.google.com/file/d/1u8T6zldNXlabjA0igdXObA55fyX2_4Bz/view>, at pp. 33, 37. Further, in *Faheema Shirin R.K. v State of Kerala* 2019 SCC OnLine Ker 2976 [15], the Kerala High Court held that the right to access the internet forms part of the rights to education and privacy under Article 21 of the Constitution.

2 A working group of participants at RightsCon, a popular event on the Internet and human rights organized by civil society, devised a crowd-sourced, working definition of an Internet shutdown as "*an intentional disruption of Internet or electronic communications, rendering them inaccessible or effectively unusable, for a specific population or within a location, often to exert control over the flow of information*." *See*, 'No more Internet shutdowns! Let's #KeepItOn' (*Access Now*, 30 March 2016) <https://www.accessnow.org/no-internet-shutdowns-lets-keepiton/> accessed February 1, 2017.

3 *See*, e.g., Anuj Srivas, 'Jammu & Kashmir has Lost 18 Days of Mobile Internet Access over Last Four Years' *The Wire* (15 April 2016) <http://thewire.in/2016/04/15/jammu-kashmir-has-lost-18-days-of-mobile-internet-access-over-last-four-years-29857/> accessed 1 February 2017.

4 Sarvjeet, Singh, "Incidents of Internet Shutdowns in India (2010 onwards)", Centre for Communication Governance at National Law University, Delhi, <https://drive.google.com/file/d/0BycAZd9M5_7NOExCRnQ3Q1pqcm8/view>; Software Freedom Law Centre, 'Internet Shutdown Tracker', <https://internetshutdowns.in/>.

5 With effect from 7.8.2019, the State stands bifurcated into two Union Territories.

6 Software Freedom Law Centre, 'Internet Shutdown Tracker' <https://internetshutdowns.in/> accessed 3 May 2020). *See also* 'Launching STOP: the #KeepItOn Internet

Internet shutdowns cost the economy at least $3.04 billion.[7] India's positions at the international stage with respect to Internet shutdowns inspire no hope. In 2016, the United Nations Human Rights Committee passed a resolution calling states to desist and refrain from "measures to intentionally prevent or disrupt access to or dissemination of information online" including measures to shut down the Internet or part of the Internet at any time, particularly at times where access to information is critical, such as during an election, or in the aftermath of a terrorist attack.[8] The Committee further urged for the adoption of a "human rights-based approach" to provide and expand access to the Internet, with particular regard to addressing the gender digital divide, and to promote Internet access for persons with disabilities.[9]Perhaps unsurprisingly, India favored an amendment to the Resolution seeking removal of the clause containing a call for "a human rights based approach" to the internet.[10]

We must hence begin examining Internet shutdowns seriously within the Indian constitutional framework. This paper begins that project with an analysis centered on the freedom of expression under Article 19(1)(a). For two reasons, internet shutdowns whether total or partial always implicate the freedom of expression. *First*, the internet is a vital medium for speech and expression in this age, and a restriction on the medium necessarily implies a restriction on the right itself.[11] *Second*, the freedom of speech and expression has been consistently interpreted by the Supreme Court as including the right

---

Shutdown Tracker' (*Access Now*, 16 November 2017) <https://www.accessnow.org/keepiton-shutdown-tracker/> accessed 1 June 2019. The country was also the most hurt economically, losing US$3.04 billion for the 16315 hours of internet shutdowns during the period 2012-2017. *See* Indian Council for Research on International Economic Relations, 'The Anatomy of Internet Blackout: Measuring the Economic Impact of Internet Shutdowns in India' (April 2018), <https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=2ahUKEwjorrC7_oXhAhUJ7XMBHV3qCOYQFjAAegQICRAC&url=http%3A%2F%2Ficrier.org%2Fpdf%2FAnatomy_of_an_Internet_Blackout_ppt.pdf&usg=AOvVaw3pgnNST2CKlyJwCChRI0cg> accessed 10 March 2019.

7 *See*, Indian Council for Research on International Economic Relations, 'The Anatomy of Internet Blackout: Measuring the Economic Impact of Internet Shutdowns in India' (April 2018), <https://icrier.org/pdf/Anatomy_of_an_Internet_Blackout.pdf>.

8 United Nations Human Rights Council, 'Resolution on the Promotion and Protection of All Human Rights, Civil, Political, Economic, Social and Cultural Rights, Including the Right to Development' (A/HRC/32/L.20) June 27, 2016, <https://www.article19.org/data/files/Internet_Statement_Adopted.pdf.>.

9 ibid.

10 Article 19, 'Significant Resolution Reaffirming Human Rights Online Adopted' (1 July 2016) <https://www.article19.org/resources.php/resource/38429/en/unhrc:-significant-resolution-reaffirming-human-rights-online-adopted>. The resolutions of the HRC are not binding and is opinio juris.

11 *Anuradha Bhasin v Union of India* (2020) 3 SCC 637 : 2020 SCC OnLine SC 25 [29].

to receive information;[12] given that the internet is the chief source of all kinds of information today, this informational right is directly affected by internet shutdowns. In the recent judgment of *Anuradha Bhasin*,[13] the Supreme Court has accepted that Article 19(1)(a) protects the right to disseminate and receive information through the internet.[14]

Therefore, the constitutional validity of every internet shutdown would have to be tested (at least) against the standards ordinarily applied to test restrictions on the freedom of speech. These standards are exhaustively[15] contained in Article 19(2) of the Constitution and can be stated in the form of a three-part test as follows:[16]

i The restriction should be imposed by "law".

ii It should be in pursuance of one of the nine standards listed in Article 19(2).

iii It should be "reasonable".

Accordingly, this paper sequentially analyzes internet shutdowns against these three requirements. Part I of this paper addresses the lawfulness prong by studying the statutory regime that is used by the executive to impose internet shutdowns. The Telegraph Act, 1885 (and the rules framed thereunder), the Code of Criminal Procedure, 1973, and the Information Technology (Amendment) Act, 2008 (and the rules framed thereunder) are studied and compared. The requirement of publication of shutdown orders – another component of lawfulness – is also discussed. Part II explores the meaning of public order, which is the most relevant[17] ground from the list given in Article 19(2) in the context of internet shutdowns. The principles governing the permissible invocation of this ground are also discussed. Part III explains the concept of reasonableness, which is the final requirement of Article 19(2), and lays out the factors that must be examined to determine whether an internet shutdown is reasonable. Part IV examines judgments in which the Indian Supreme Court and various High Courts have considered the validity

---

[12] *Ministry of Information & Broadcasting v Cricket Assn. of Bengal* (1995) 2 SCC 161 [36]; *Union of India v Assn. for Democratic Reforms* (2002) 5 SCC 294 [38]; *Namit Sharma v Union of India* (2013) 1 SCC 745 [2].

[13] *Anuradha Bhasin* (n 11).

[14] ibid [31].

[15] *Sakal Papers (P) Ltd. v Union of India* AIR 1962 SC 305 : (1962) 3 SCR 842 [34]; *State of Karnataka v Associated Management of English Medium Primary and Secondary Schools* (2014) 9 SCC 485 [41].

[16] Constitution of India, art 19(2).

[17] We say "relevant" not because other grounds can never be invoked, but because in practice the State mostly invokes this ground rather than the others.

of internet shutdowns and applied (or failed to apply) the relevant constitutional principles. To conclude, we outline questions that should be considered in future research on this subject in order to mitigate the ill-effects of shutdown orders.

II. The First Prong: Lawfulness

The first requirement of Article 19(2) is that a restriction on the freedom of speech must be provided by a "law".[18] This requirement of lawfulness further entails at least two broad principles. First, there should be a statute i.e., a primary legislation, to which the restriction is traceable. Second, the executive order which imposes the restriction should be published. This part of the paper first sets out, with a critical eye, the laws which the executive relies on to impose internet shutdowns. It then discusses the requirement of transparency that is critical to the substantive validity of executive orders.

A. Statutory Basis

The word "law" in Article 19(2) implies that any restriction on speech should be traceable to a statute.[19] In other words, a mere departmental instruction which is not traceable to any law would not furnish an adequate legal basis for the imposition of the restriction on free speech.[20] Broadly speaking, three statutory provisions are used by governments to impose internet shutdowns:[21](i) Section 144 of the Code of Criminal Procedure, 1973 ("**CrPC**"); (ii) Section 69A of the Information Technology (Amendment) Act, 2008 ("**IT Act**") read with the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 ("**Blocking Rules**"); and (iii) Section 5(2) of the Telegraph Act, 1885 read with the Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules, 2017 ("**Suspension Rules**").

---

[18] Constitution of India 1950, art 19(2).

[19] *Kharak Singh v State of U.P.* AIR 1963 SC 1295 : (1964) 1 SCR 332 [5]; *Bijoe Emmanuel v State of Kerala* (1986) 3 SCC 615 [16].

[20] ibid.

[21] For a brief overview of the available legal bases and their applicability, *see* Siddharth Narrain, 'Internet Shutdowns: Background and Use of Section 144, Code of Criminal Procedure, 1973' (*Socio-Legal Review*, 11 March 2018) <https://www.sociolegalreview.com/post/internet-shutdowns-background-and-use-of-section-144-code-of-criminal-procedure-1973> accessed 31 May 2020; and Siddharth Narrain, 'Internet Shutdowns: Amendment to the Telegraph Act and Mobile Company Licenses' (*Socio-Legal Review*, 28 March 2018) <https://www.sociolegalreview.com/post/internet-shutdowns-amendment-to-the-telegraph-act-and-mobile-company-licenses> accessed 31 May 2020.

In the first three sections below, we sequentially analyze the framework under the CrPC, the IT Act & the Blocking Rules, and the Telegraph Act & the Suspension Rules. The fourth section compares the three regimes and suggests that internet shutdowns cannot be imposed under the CrPC at all.

i. The CrPC

Section 144 of the CrPC empowers the District Magistrate to "direct any person to abstain from a certain act or to take certain order with respect to certain property in his possession or under his management".[22] This broadly worded power is circumscribed by two key safeguards contained in the text of the provision itself.

First, the power may be exercised only in cases of urgency i.e. when "immediate prevention or speedy remedy is desirable".[23] Section 144 occurs in a Chapter titled "Urgent Cases of Nuisance or Apprehended Danger",[24]and its marginal note describes it as a "[p]ower to issue order in urgent cases of nuisance or apprehended danger".[25] These requirements must be read with the specific aims stated in Section 144 in furtherance of which the District Magistrate may issue directions under that provision:

i "obstruction, annoyance or injury to any person lawfully employed",[26]

ii "danger to human life, health or safety",[27] or

iii "a disturbance of the public tranquillity, or a riot, or an affray".[28]

This narrow reading of Section 144 is supported by the Supreme Court's judgment in *Madhu Limaye*.[29] While upholding the *vires* of Section 144 against Article 19(1)(a), the Court held that the provision can be invoked only when there is an emergency *and* the consequences of the speech involved are sufficiently grave.[30]The "annoyance" contemplated in Section 144 "must assume sufficiently grave proportions to bring the matters within interests of public order" for the power to be held to have been validly exercised.[31]

---

22 CrPC, s 144(1). The *vires* of Section 144 was unsuccessfully challenged in *Babulal Parate v State of Maharashtra* AIR 1961 SC 884 and *Madhu Limaye v Sub-Divisional Magistrate, Monghyr* (1970) 3 SCC 746.

23 CrPC, s 144(1).

24 CrPC, ch X-C.

25 CrPC, s 144 Marginal Note.

26 ibid.

27 ibid.

28 ibid.

29 *Madhu Limaye v Sub-Divisional Magistrate, Monghyr* (1970) 3 SCC 746.

30 ibid [24].

31 ibid [24].

This reading of Section 144 – which ties the validity of exercise of power to an "emergency" – was recently approved by the Supreme Court in the context of the restrictions placed upon the movement of persons in Jammu & Kashmir.[32]

Second, Section 144 requires the Magistrate to pass "a written order stating the material facts of the case".[33] Written orders act as the first check for the existence of a good cause for exercising extraordinary powers;[34] stating the material facts enables judicial scrutiny of the order.[35] Further, the material facts stated in the order must be such that they indicate proper application of mind on part of the Magistrate:

> *"Proper reasoning links the application of mind of the officer concerned, to the controversy involved and the conclusion reached. Orders passed mechanically or in a cryptic manner cannot be said to be orders passed in accordance with law."*[36]

Besides these textual safeguards, two other important safeguards have been read into Section 144 by the Supreme Court. *First*, a repeated issuance of Section 144 orders would amount to an abuse of the provision.[37] *Second*, any orders under Section 144 must be published to enable affected persons to challenge them.[38] The safeguards are often breached – e.g., in some states including Rajasthan,[39] Gujarat[40] and Arunachal Pradesh,[41] internet services have been suspended to prevent malpractices and ensure fair conduct of

---

[32] *Anuradha Bhasin* (n 11) [128].

[33] *See*, s 144(1) of the CrPC.

[34] *See P.T. Chandra v Crown* 1942 SCC OnLine Lah 23 : AIR 1942 Lah 171 [5].

[35] *Anuradha Bhasin* (n 11) [142].

[36] ibid [144].

[37] ibid [124] (citing *Acharya Jagdishwaranand Avadhuta v Commr. of Police* (1983) 4 SCC 522, [16]).

[38] ibid [163(a)].

[39] 'Rajasthan to Suspend Internet during Constable Recruitment Examinations on 14th and 15th July' (*MediaNama*, 13 July 2018) <https://www.medianama.com/2018/07/223-rajasthan-to-suspend-internet-during-constable-recruitment-examinations-on-14-15-july/>; *See also*: 'Rajasthan to Suspend Mobile Internet Services Tomorrow from 9 am to 1 pm' (*The Financial Express*, 4 August 2018) <https://www.financialexpress.com/india-news/rajasthan-to-suspend-mobile-internet-services-tomorrow-from-9-am-to-1-pm/1269716/>.

[40] '4-Hour Ban on Mobile Internet in State Today' (*The Times of India*, 28 February 2016) <http://timesofindia.indiatimes.com/tech/mobiles/4-hour-ban-on-mobile-internet-in-state-today/articleshow/51175590.cms>; 'To Beat Exam Cheats, Gujarat to Block Mobile Internet Today' (*The Times of India*, 28 February 2016) <http://timesofindia.indiatimes.com/india/to-beat-exam-cheats-gujarat-to-block-mobile-internet-today/articleshow/51173461.cms?from=mdr.>.

[41] 'Arunachal Govt Orders Suspension of Internet across State for APPSC Exam' (19th July 2018) <https://thenewsmill.com/arunachal-govt-orders-suspension-of-internet-across-state-for-appsc-exam/>.

competitive examinations, which corresponds neither to the kind of urgency that Section 144 contemplates nor to the aims it lists. Likewise, the requirement of stating material facts has also been breached.[42] Nonetheless, the presence of these safeguards within the text of the CrPC and in case law ought to be valued.

ii. The IT Act and Blocking Rules

Section 69A of the IT Act empowers the Central Government to "direct any agency of the Government or intermediary to block for access by the public or cause to be blocked for access by the public any information generated, transmitted, received, stored or hosted in any computer resource".[43] Two important safeguards are embedded in this provision: (i) the Government must record its reasons in writing;[44] and (ii) the exercise of this power is "subject to"[45] any other procedure and safeguards that may be prescribed through rules.[46]

The Blocking Rules were framed by the Government under Section 69A. The Rules specify a Designated Officer (a high-level officer in the Central Government) responsible for ordering the blocking of information,[47] provide a detailed procedure to be adopted before the order can be made (involving written communication at each step),[48] mandate a periodic review (at least once in two months) of the orders passed under these rules,[49] and require the designated authority to maintain written records of those orders.[50]

An important safeguard in the Rules is the multi-layered scrutiny that every blocking request must go through. Individual persons can send requests for blocking websites to the Nodal Officer of the relevant government department (central or state).[51] If the department finds the request to be meritorious, its Nodal Officer must forward it to the Designated Officer,[52] who then forwards it to a Committee headed by herself along with "… representative

---

[42] *See*, e.g., Order of the District Magistrate, Jammu (5 June 2015) <http://sikhsiyasat.net/2015/06/05/information-blackout-govt-orders-ban-on-internet-services-in-jammu-district-situation-tense-after-sikh-youths-killed-in-police-firing/>.
[43] IT Act, s 69A(1).
[44] ibid.
[45] ibid.
[46] ibid s 69A(2).
[47] Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules 2009, r 3.
[48] ibid rr 6, 7, 8 and 9. *See also* ibid Form-A.
[49] ibid r 14.
[50] ibid r 15.
[51] ibid r 6(1).
[52] ibid r 6(2).

not below the rank of Joint Secretary in Ministries of Law and Justice, Home Affairs, Information and Broadcasting and the Indian Computer Emergency Response Team…"[53] After hearing representations from the intermediaries[54] (or not, in case of an emergency),[55] the Committee submits its recommendations to the Secretary in the Department of Information Technology under the Ministry of Communications and Information Technology.[56] Finally, the Secretary of the Department of Information Technology must give her approval to the request.[57] There is a review mechanism under the Rules that operates after the shutdown order has been issued. A Review Committee constituted under the Indian Telegraph Rules, 1951[58] is to meet at least once every two months to verify the various blocking directions issued in the said duration.[59]

There is some doubt with respect to the scope of the powers under Section 69A. In *Anuradha Bhasin*,[60] the Supreme Court observed that this provision cannot be invoked to "restrict the internet generally", for the aim of this section is to "block access to particular websites on the internet".[61] This view is not baseless. The design of the Blocking Rules – which require the government to specify the websites to be blocked and hear the affected intermediaries – does suggest that the rules are intended for a narrower purpose than a full shutdown. Yet, the Supreme Court's view is not an *obvious* one. Section 69A empowers the Central Government, *inter alia*, to direct "any… intermediary" to block or cause to be blocked "any information… in any computer resource".[62] The word "intermediary" is defined under Section 2(w) of the IT Act as including telecom service providers,[63] who can effect a total internet shutdown. It would be plausible to argue that the word "any", especially in light of its repeated use in the provision, must be read as including "all" or "every" because of the broad wording of the statute.[64]

---

[53] ibid r 7.
[54] ibid r 8(1).
[55] In cases of emergency, the Designated Officer is permitted to bypass the requirements to place the request before a Committee and to give a hearing to the affected parties. *See* ibid r 9.
[56] ibid r 8(5).
[57] ibid r 8(6).
[58] The Indian Telegraph Rules 1951, r 419A.
[59] Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules 2009, r 14.
[60] *Anuradha Bhasin* (n 11).
[61] ibid [88].
[62] IT Act, s 69A.
[63] IT Act, s 2(w).
[64] The Supreme Court has held that the meaning of the word "any" would depend on the context in which it occurs. Depending on the context, it could either mean "all"/"every"

One could argue that the presence of other laws on the same subject – such as the Telegraph Act and the Suspension Rules– would have the effect of narrowing the scope of Section 69A. But such a claim would be defeated by Section 81of the IT Act which says:

> *"The provisions of this Act shall have effect notwithstanding anything inconsistent therewith contained in any other law for the time being in force."*

Given the wide amplitude of Section 69A read with Section 81, a compelling argument would be required to hold that the scope of the Blocking Rules, which are framed under Section 69A, is significantly narrower than that of the parent statute and extends only to the selective blocking of a few websites. Equally, the Blocking Rules do not place a cap on the number of websites that may be blocked at once. Hence, while the Supreme Court's position is not implausible, it is far from obvious. The Court ought to have engaged more with the issue in holding what it did.

iii. The Telegraph Act and Suspension Rules

Section 5(2) of the Telegraph Act, 1885 permits the issuance of an order directing, *inter alia*, that "any message or class of messages to or from any person or class of persons… brought for transmission by or transmitted or received by any telegraph… shall not be transmitted".[65] The words "telegraph" and "message" are given wide definitions under the Telegraph Act which makes Section 5(2) a source of power for imposing Internet shutdowns. While "telegraph" means "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",[66] the word "message" implies "any communication sent by telegraph, or given to a telegraph officer to be sent by telegraph or to be delivered".[67] Viewing Section 5(2) in this light, insofar as contents on the internet are "communication"[68] sent using instruments capable of signal

---

or "either". *Shri Balaganesan Metals v M.N. Shanmugham Chetty* (1987) 2 SCC 707 [18] (citing *Black's Law Dictionary*, 5th edn).

[65] Telegraph Act 1885, s 5(2). Readers will note that like Section 69A of the IT Act, the language of Section 5(2) of the Telegraph Act language is also expansive, the word "any" having been used repeatedly.

[66] ibid s 3(1AA).

[67] ibid s 3(3).

[68] The word "communication" is generally understood broadly to include any exchange of information. E.g., the *Black's Law Dictionary* defines it as: "1. The expression or exchange of information by speech, writing, gestures, or conduct; the process of bringing an idea

transmission and reception, they are covered within the ambit of Section 5(2). Because the definition of "telegraph" under the Act is wide enough to encompass web servers as well as the technical apparatuses of telecom service providers,[69] internet shutdown orders issued to such service providers fall within Section 5(2).

A suspension order under Section 5(2) may be issued only by the Central Government, the State Government or any officer specifically authorized in this behalf by either government, for reasons recorded in writing.[70] It may only be issued "[o]n the occurrence of any public emergency" or "in the interest of the public safety" and if the issuing authority is satisfied that the order is required "the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of an offence".[71]

Section 7 of the Telegraph Act confers power on the Central Government to make rules.[72] The Suspension Rules[73] were enacted in exercise of this power.[74] They provide that directions to suspend telecom services may be issued only through a reasoned order[75] and only[76] by the Union Home Secretary (for the Central Government) or the State Home Secretary (for a State Government).[77] By the next working day, the order must be placed before a three-member Review Committee which must decide, within five days, whether the order is in consonance with Section 5(2) of the Telegraph Act.[78] In *Anuradha Bhasin*,[79] the Supreme Court read into the Rules a further requirement of periodic review every seven days from the date of the

---

to another's perception. 2. The information so expressed or exchanged." *Black's Law Dictionary* (9th edn, 2009) 316.

69 ibid s 3(1AA).

70 ibid s 5(2).

71 ibid.

72 ibid s 7(1).

73 Department of Telecommunications, Ministry of Communications, Government of India, Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules, 2017, G.S.R. 998(E) dated 7th August 2017.

74 ibid Preamble.

75 ibid r 2(2).

76 ibid r 2(1). Readers will note that this Rule may be contrary to Section 5(2) of the Telegraph Act insofar as it takes away the State Government's power to authorize any officer for the purposes of suspension of services.

77 ibid. In unavoidable circumstances where prior directions cannot be obtained from the said competent authority, suspension orders can be passed by officers holding the post of Joint Secretary or above in the Central Government who have been empowered to do so by the relevant Home Secretary. Such orders must then be confirmed by the relevant Home Secretary within 24 hours.

78 ibid r 2(6).

79 *Anuradha Bhasin* (n 11).

previous review.[80] We submit, however, that the Suspension Rules are defective for four reasons.

First, the Review Committee is empowered under the Suspension Rules only to "record its findings" but not set aside an illegal suspension order.[81] This makes it a toothless committee. *Second*, as has been argued elsewhere, allowing a five-day period for the review is not reasonable.[82] Since most internet shutdowns run for less than five days continuously,[83] the review exercise – otherwise an important procedural check – is reduced to a purely academic and unactionable *post-mortem*. *Third*, the Rules do not provide for publication of either the suspension orders or the Review Committee's findings. They set up an opaque procedure capable of cloaking the executive's misuses of its sweeping power to blackout a vital medium of communication, while affording Indian citizens no right to remedy. Avoiding public notification of the suspension causes more harm than it prevents, considering that the public would be left in a state of surprise and under-preparedness to tackle with a lack of much-needed network facilities.[84] As Apar Gupta puts it, "[*f*] *rom the creation of the rules to their implementation, there is secrecy. And secrecy is the hallmark of an autocracy, not a democracy*".[85] (It was only in January 2020 that the Supreme Court held that the requirement of publication is inherent in any piece of legislation, and hence also in the Suspension Rules.[86])

iv. Choosing among the three laws

Internet shutdowns have continued to be imposed under the CrPC despite enactment of the Blocking Rules in 2009 and Suspension Rules in 2017.[87] The reasons could be speculated. The fact that Section 144 can be exercised by states without any advertence to the Central Government makes it – from the states' perspective – pragmatically superior to the IT Act under which the Designated Officer, who is the sole authority authorized to issue

---

[80] ibid [109].

[81] ibid. r 2(6).

[82] Nakul Nayak, 'The Legal Disconnect: An Analysis of India's Internet Shutdown Laws' (2018) Working Paper No. 1 , Internet Freedom Foundation, 13.

[83] ibid.

[84] ibid.

[85] 'IEThinc: Is Internet Shutdown the New Order for Law and Order?' (*The Indian Express*, 7th September 2018) <https://indianexpress.com/article/business/market/iethinc-is-internet-shutdown-the-new-order-for-law-and-order-5344069/>.

[86] *Anuradha Bhasin* (n 11) [19].

[87] Arunabh Saikia, 'India's Internet Shutdown: Most States Block Services without Following Centre's New Rules' (*Scroll.in*, 7th April 2018) <https://scroll.in/article/874565/internet-shutdown-most-states-continue-to-block-services-without-adhering-to-the-centres-new-rules>.

shutdown orders, is a Central Government officer and must seek the Union IT Ministry's approval before issuing any shutdown orders. Section 144 holds a clear preference over the Telegraph Act & Rules as well, because it does not even remotely contain the kind of procedural safeguards that the said Act and Rules provide for – decisions under Section 144 are taken at the District Magistrate level rather than the Home Secretary level, no review committee is required to examine the validity of the order in a time-bound manner, and no periodic review is provided for. The same comparison holds true between the CrPC and the IT Act and Rules as well.

This raises an important question: is it legally permissible for governments to resort to Section 144 of the CrPC – a general law providing for maintenance of public order – despite the availability of legal regimes which specifically deal with internet shutdowns? In February 2016, the Chief Justice of India reportedly labelled the powers conferred by the CrPC and the IT Act as "*concurrent*".[88] Some government officials[89] and writers[90] also hold this view. We disagree.

According to the well-known legal maxim *generalia specialibus non derogant*, "if a special provision has been made on a certain matter, that matter is excluded from the general provisions".[91] The Supreme Court has applied this principle to exclude general statutes from fields covered by special statutes. For example, the Bihar Finance Act, 1981 which provided for the levying of "all commercial taxes generally" stood ousted by the Bihar Sugarcane Act, 1981 which provided specifically for the levy only of purchase tax on sugarcane.[92] Likewise, the summoning powers of a trial judge under the CrPC stood excluded by the more specific provisions of the Prevention of Corruption Act, 1988.[93] The test in applying this maxim is whether the legislative intent in enacting the special law was to provide "special treatment" to the subject regulated.[94] Applying this test would reveal that the provisions of both the IT Act & Rules as well as the Telegraph Act & Rules are special

---

88 'Mobile Internet can be Banned under S. 144 CrPC, Says Supreme Court' (*Bar and Bench*, 11th February 2016) <http://barandbench.com/mobile-Internet-can-be-banned-under-s-144-crpc-for-law-and-order-says-supreme-court/>.

89 Arunabh Saikia (n 87).

90 Shikhar Goel, 'Internet Shutdowns: Strategy to Maintain Law and Order or Muzzle Dissent?' (2018) vol 53(42) *Economic and Political Weekly*.

91 *Dilawar Singh v Parvinder Singh* (2005) 12 SCC 709 [8].

92 *Gobind Sugar Mills Ltd. v State of Bihar* (1999) 7 SCC 76 [10].

93 *Dilawar Singh v Parvinder Singh* (2005) 12 SCC 709 [8].

94 *Gobind Sugar Mills Ltd* (n 92) [10].

vis-à-vis the CrPC.[95] The sequitur is that internet shutdowns cannot permissibly be imposed under Section 144 of the CrPC.[96]

But what about choosing between the Telegraph Act & Suspension Rules on the one hand and the IT Act & Blocking Rules on the other? Notably, Section 81 of the IT Act which provides that the provisions of that Act shall have effect notwithstanding anything contained in any other law in force.[97] Even if the Telegraph Act & Rules were imagined as a "special" regime, therefore, the IT Act & Rules would continue to operate. On the other hand, if the IT Act & Rules are special (in terms of blocking individual websites, say) vis-à-vis the Telegraph Act and the Suspension Rules, the former would oust the application of the latter. But since both regimes specifically contemplate the imposition of internet shutdowns,[98] and both provide for blocking of access to particular pieces of information – "messages" in case of the Telegraph Act and "information" in case of the IT Act,[99] it is not possible to say that either regime is more special than the other. Hence both regimes will continue to operate in their own stead.

B. Publication and Transparency

A publication requirement is stated neither in the IT Act & Blocking Rules nor the Telegraph Act & Suspension Rules. In fact, the Blocking Rules actively mandate strict confidentiality of all complaints that seek shutdowns, and also of the actions taken on those complaints.[100] Yet, the Supreme Court has treated publication of orders as an imperative requirement for any piece of legislation, whether primary or secondary, to have substantive validity.[101] Indeed, publication is a requirement of natural justice:

---

[95] See e.g. Long Title of the IT Act ("An Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication …"); Short Title of the Blocking Rules ("…Procedure and Safeguards for Blocking of Access of Information by Public"); Preamble to the Telegraph Act ("[w]hereas it is expedient to amend the law relating to telegraphs in India…"); and Preamble to the Suspension Rules ("…[T]he Central Government hereby makes the following rules to regulate the temporary suspension of telecom services due to public emergency or public safety…").

[96] A similar argument has been made earlier. *See* Geetha Hariharan and Padmini Baruah, 'The Legal Validity of Internet Bans: Part II' (*Centre for Internet and Society*, October 8 2015) <http://cis-india.org/Internet-governance/blog/the-legal-validity-of-internet-bans-part-ii.------>.

[97] IT Act, s 81.

[98] Why the power under the IT Act contemplates a total internet shutdown is discussed in Section (ii) above.

[99] Contrast Telegraph Act, s 5(2) with IT Act s 69A(1).

[100] Information Technology (Procedure and Safeguards for Blocking Access of Information by Public) Rules 2009, r 16.

[101] *B.K. Srinivasan v State of Karnataka* (1987) 1 SCC 658; *Gulf Goans Hotels Co Ltd v Union of India* (2014) 10 SCC 673.

> *"Natural justice requires that before a law can become operative it must be promulgated or published…. The thought that a decision reached in the secret recesses of a chamber to which the public have no access and to which even their accredited representatives have no access and of which they can normally know nothing, can nevertheless affect their lives, liberty and property by the mere passing of a resolution without anything more, is abhorrent to civilised man."*[102]

The Court reiterated this in the specific context of internet shutdowns in *Anuradha Bhasin*:[103]

> *"It must be noted that although the Suspension Rules does [sic.] not provide for publication or notification of the orders, a settled principle of law, and of natural justice, is that an order, particularly one that affects lives, liberty and property of people, must be made available. Any law which demands compliance of the people requires to be notified directly and reliably."*[104]

Hence, it is now well-settled that internet shutdown orders cannot satisfy the 'lawfulness' requirement of Article 19(2) unless they are duly promulgated and brought to the notice of citizens. This is an inherent requirement of the rule of law and need not be expressly stated in the legislation under question.

Yet, there has been a trend of internet shutdown orders not being published online. Information about shutdowns is available, if it is available at all, only *ex post facto* through secondary sources like newspapers. This information asymmetry is borne out by the facts and arguments narrated in some judgments. E.g., in a 2016 PIL in the Gujarat High Court, the State argued that the Court had not been presented with accurate information about the shutdown as the Petitioner would not have this information available.[105] More recently in *Anuradha Bhasin*,[106] the Court noted that the Petitioners had challenged the internet shutdown orders without annexing them because they did not have access to them.[107] In a brazen statement, even the Government refused to produce the orders before the Court, citing a vague "difficulty".[108] Given such attitude on part of the government,

---

[102] *Harla v State of Rajasthan* AIR 1951 SC 467 : 1952 SCR 110.
[103] *Anuradha Bhasin* (n 11).
[104] ibid [96].
[105] *See Gaurav Sureshbhai Vyas v State of Gujarat* 2015 SCC OnLine Guj 6491 [4].
[106] *Anuradha Bhasin* (n 11).
[107] ibid [14].
[108] ibid [15].

examining the scope, duration, and stated reason of each shutdown is often difficult.

III. The Second Prong: "Legitimacy" and "Public Order"

To recap, restrictions may be placed on the freedom of speech and expression only for one of the nine reasons stated in Article 19(2).[109] Governments usually claim that internet shutdowns are being imposed in the interests of public order. Therefore, this part of the paper presents an analysis of "public order" under Article 19(2) and its application to internet shutdowns. Specifically, it addresses two facets of the public order clause on which the Supreme Court has commented repeatedly: (i) the meaning of "public order" and (ii) the degree of proximity or closeness that the restriction in question must have with public order so that it can be said to fall within Article 19(2).

A. Defining "Public Order"

In *Lohia-I*,[110] the *vires* of Section 3 of the Uttar Pradesh Special Powers Act, 1932, which penalized the instigation of people to not pay taxes, was challenged. Attempting to define public order, the Court held that "*[i]t implies the orderly state of society or community in which citizens can peacefully pursue their normal activities of life.*"[111] The Court also held that "*public order is synonymous with public peace, safety and tranquility.*"[112] In other words, public order "*is the absence of disorder involving breaches of local significance in contradistinction to national upheavals, such as revolution, civil strife, war, affecting the security of the State.*"[113] In *Lohia-II*,[114] the Court speaking through Hidayatullah, J. famously conceptualized national security, public order, and law and order as part of a scheme of concentric circles:

> *"One has to imagine three concentric circles. Law and order represents the largest circle within which is the next circle representing public order and the smallest circle represents security of State. It is then easy to see that an act may affect law and order but not public*

[109] *See Romesh Thappar v State of Madras* AIR 1950 SC 124 : 1950 SCR 594 [10].
[110] *Supt., Central Prison v Ram Manohar Lohia* AIR 1960 SC 633.
[111] ibid.
[112] ibid [11].
[113] ibid [18].
[114] *Ram Manohar Lohia v State of Bihar* AIR 1966 SC 740 : (1966) 1 SCR 709.

> *order just as an act may affect public order but not security of the State.*"[115]

Later, in *Madhu Limaye*,[116] a seven-judge bench of the Court held that *Lohia-II*'s conception of the three concentric circles was rendered in the context of preventive detention and it "*need not always apply*".[117] In contexts other than preventive detention, public order would carry a broader meaning – it would refer to "*a state of law abidingness vis-à-vis the safety of others*", such that even "*small local disturbances of the even tempo of life*" and "*certain acts which disturb public tranquility or are breaches of the peace*" would implicate public order.[118] More recently, in *Anuradha Bhasin*,[119] the Court explained the distinction between "public order" and "law and order" in the following words:

> *"If two families quarrel over irrigation water, it might breach law and order, but in a situation where two communities fight over the same, the situation might transcend into a public order situation.*"[120]

Thus, what appears consistently in the Court's decisions is a focus on violence in understanding public disorder. It would be fair to say that public order has broadly been understood as a violence-centric notion which does not cover every minor infraction of the law.[121] Accordingly, any internet shutdowns that purport to be issued for the preservation of public order must be linked to this understanding of public order. Yet, states have not abided by these principles in imposing shutdowns. For instance, on two occasions

---

[115] ibid [55].
[116] *Madhu Limaye v Sub-Divisional Magistrate, Monghyr* (1970) 3 SCC 746.
[117] ibid [20].
[118] ibid.
[119] *Anuradha Bhasin* (n 11).
[120] ibid [123].
[121] *Jaya Mala v Govt. of J&K*, (1982) 2 SCC 538 [7]; *Ramlila Maidan Incident*, *In re*, (2012) 5 SCC 1 [238]. However, one aberration is worth noting from the Supreme Court's case law. In *Devendrappa*, the Appellant was dismissed from service in a public corporation after publicly pointing out maladministration in the affairs of the corporation. He was dismissed under a rule that prohibited employees from undertaking actions detrimental to the "interests or prestige of the corporation." The Court upheld the rule, noting that "[a]ny action detrimental to the interests of prestige of the employer clearly undermines discipline within the organisation and also the efficient functioning of that organisation. Such a rule could be construed as falling under 'public order'". *M.H. Devendrappa v Karnataka State Small Industries Development Corp* (1998) 3 SCC 732 [14]. We submit that this judgment ignores previous binding precedent and consequently misunderstands "public order" under Article 19(2).

in Rajasthan,[122] and on one occasion each in Gujarat[123] and Arunachal Pradesh,[124] internet services were suspended in parts of these states in order to prevent malpractices and ensure fair conduct of public competitive and entrance examinations. These measures corresponded neither to "public order" nor to any other ground in Article 19(2).

B. Nexus between the Restriction and "Public Order"

Article 19(2) requires that the restriction be "in the interests of" public order. In the earlier years, the Supreme Court interpreted the words "in the interests of" expansively and held that they make the ambit of public order "very wide", such that a law "may not be designed to directly maintain public order and yet it may have been enacted in the interests of public order."[125] Through subsequent judgments, however, the nexus requirement of Article 19(2) was interpreted more tightly.

Lohia-I[126] laid down the principles that would authoritatively guide the interpretation of Article 19(2) in the years to come.[127] The Court held that "any remote or fanciful connection" between the restriction and public order is not sufficient for the purposes of Article 19(2).[128] Rather, the restriction "should be one which has a proximate connection or nexus with public order...."[129] This understanding was carried forward in *Rangarajan*,[130] where the Court held:

---

[122] Rana, 'Rajasthan to Suspend Internet during Constable Recruitment Examinations on 14th and 15th July' (*MediaNama*, 13th July 2018) <https://www.medianama.com/2018/07/223-rajasthan-to-suspend-internet-during-constable-recruitment-examinations-on-14-15-july/)>----; *See also*: PTI, 'Rajasthan to Suspend Mobile Internet Services Tomorrow from 9 am to 1 pm' (*The Financial Express*, 4th August 2018) <https://www.financialexpress.com/india-news/rajasthan-to-suspend-mobile-internet-services-tomorrow-from-9-am-to-1-pm/1269716/> ------.

[123] TNN, '4-Hour Ban on Mobile Internet in State Today' (*The Times of India*, 28 February 2016) <http://timesofindia.indiatimes.com/tech/mobiles/4-hour-ban-on-mobile-internet-in-state-today/articleshow/51175590.cms> -----.

[124] TNM NewsDesk, 'Arunachal Govt Orders Suspension of Internet across State for APPSC Exam' (*NewsMill*, 19th July 2018) <https://thenewsmill.com/arunachal-govt-orders-suspension-of-internet-across-state-for-appsc-exam/>

[125] *Ramji Lal Modi v State of U.P.*, AIR 1957 SC 620 : 1957 SCR 860 [7].

[126] *Supt., Central Prison* (n 110).

[127] An aberration may be noted at this juncture. In *Dalbir*, a provision penalizing spreading disaffection towards the Government among police forces was challenged. The Court held that "[a]ny breach in the discipline by its [police force] members must necessarily reflect in a threat to public order and tranquillity. If the police force itself were undisciplined they could hardly serve as instruments for the maintenance of public order." *Dalbir Singh v State of Punjab* AIR 1962 SC 1106 : 1962 Supp (3) SCR 25 [9].

[128] ibid [12].

[129] ibid [13].

[130] *S. Rangarajan v P. Jagjivan Ram* (1989) 2 SCC 574.

> "In other words, the expression should be inseparably locked up with the action contemplated like the equivalent of a "spark in a powder keg"."[131]
>
> (emphasis supplied)

These principles would equally apply in the context of internet shutdowns. Therefore, a shutdown may be imposed only when the government apprehendsan *imminent* threat of violence and breach of public peace, as opposed to situations where the apprehended danger is either remote in time or simply farfetched and conjectural. For example, in a 2019 order, the Gauhati High Court refused to accept the government's contention that there was a threat to public order in the State of Assam on account of anticipated protests in respect of the Citizenship Amendment Act, and that such a threat justified the shutting down of mobile internet services. The Court demanded that the State produce concrete material to make good its claim of apprehension of violence, and when the State failed to do so, the Court ordered the restoration of mobile internet services.[132]

IV. The Third Prong: "Reasonableness"

Besides being lawful and legitimate, restrictions must also be "reasonable".[133] Reasonableness under Article 19 is a rigorous and contextual standard of review. A determination of reasonableness must take into account "[t]he nature of the right alleged to have been infringed, the underlying purpose of the restriction imposed, the extent and urgency of the evil sought to be remedied thereby, the disproportion of the imposition, [and] the prevailing conditions at the time…."[134] Reasonableness, therefore, refers to the necessity and proportionality of the measure in light of the nature of the right and the purpose sought to be achieved by the State.[135]

One key aspect of the proportionality inquiry – overbreadth –is worth noting because of its relevance to internet shutdowns. This implies that

---

[131] ibid [45].

[132] *Banashree Gogoi v Union of India* 2019 SCC OnLine Gau 5584 [7]. The judgment is discussed in greater detail in Section IV(C) below.

[133] The "reasonableness" criterion was inserted into Article 19(2) *vide* the First Amendment to the Constitution. *See*, The Constitution (First Amendment) Act 1951, s 3(1)(a).

[134] *State of Madras v V.G. Row* AIR 1952 SC 196 [16].

[135] The ideas of "reasonableness" and "proportionality" are overlapping but not necessarily interchangeable. For a recent analysis of this intersection, see Aparna Chandra, 'Proportionality in India: A Bridge to Nowhere?' (2020) vol 3(2) University of Oxford Human Rights Journal 55, 55-86.

restrictions should be "narrowly tailored"[136] to the aim sought to be achieved by the State; their ambit must be limited to what is necessary to achieve the aim and must go no further. In *Kameshwar Prasad*,[137] the Court struck down a blanket rule prohibiting government servants from taking part in demonstrations, and held:

> *"The vice of the rule, in our opinion, consists in this- that it lays a ban on every type of demonstration — be the same however innocent and however incapable of causing a breach of public tranquility and does not confine itself to those forms of demonstrations which might lead to that result".*[138]

Of course, the rule against overbreadth does not demand the State to do the impossible. In *Babulal Parate*,[139] the Court rejected the argument that the impugned Section 144 order was unconstitutional for the reason that it was directed against the entire public:

> *"it would be extremely difficult for those who are in charge of law and order to differentiate between members of the public and members of the two textile unions [i.e. the alleged perpetrators of public disorder] and, therefore, the only practical way in which the particular activities referred to in the order could be restrained or restricted would be by making those restrictions applicable to the public generally."*[140]

Both *Babulal Parate* and *Kameshwar Prasad* are judgments rendered by five-judge benches of the Supreme Court. While the two judgments seem to conflict at first blush, reading them harmoniously yields the principle that the overbreadth of a rule is a ground to strike down the given speech restriction as unreasonable unless there is no other practical way to formulate the rule effectively.

The Court has stated the same requirement differently in subsequent cases. Under one such reformulation, the State has an obligation to apply its mind to "less restrictive but equally effective alternatives"[141]– measures that would achieve the desired aim without restricting the freedom of speech as much – before imposing the restriction. Recently, in *Anuradha Bhasin*,[142] the

---

[136] *Shreya Singhal v Union of India* (2015) 5 SCC 1 [17].
[137] *Kameshwar Prasad v State of Bihar* AIR 1962 SC 1166.
[138] ibid [16].
[139] *Babulal Parate v State of Maharashtra* AIR 1961 SC 884 : (1961) 3 SCR 423.
[140] ibid [29].
[141] *K.S. Puttaswamy v Union of India* (2019) 1 SCC 1 [157-58] (Sikri, J).
[142] *Anuradha Bhasin* (n 11).

Court affirmed this principle in context of internet shutdowns by holding that "only the least restrictive measure" can be adopted by the State.[143]

To comply with constitutional norms, therefore, shutdowns must not go beyond what is necessary to maintain public order. A shutdown that covers within its fold *every* type of speech and action, irrespective of its connection with a breach of public order, is overbroad and unconstitutional. An analogy can be drawn with *Kameshwar Prasad*, where the Court had held that it is unconstitutional to place a ban on "every type of demonstration… however innocent and however incapable of causing a breach of public tranquility".[144] Keeping these principles in mind, we can draw an indicative list of factors which should be considered in deciding the proportionality of internet shutdowns:[145]

i. Extent: Is the shutdown total or partial? Three aspects may be considered:

   a. Has access been blocked to all websites or only to select websites that are most closely linked to the public order apprehension? While *some* Internet websites and applications are indeed used to spread hatred[146] and coordinate attacks[147] during times of strife, not all websites are capable of being such platforms. In *Anuradha Bhasin*,[148] in the context of the internet shutdowns imposed in Jammu & Kashmir, the Court specifically noted that the State is obligated to "attempt to determine the feasibility" of blocking access to only social media services which pose a threat, before imposing cutting off access to the entire internet.[149]

---

143 ibid [77].

144 *Kameshwar Prasad v State of Bihar* AIR 1962 SC 1166 [16].

145 Some of these can be found mentioned in *Anuradha Bhasin v Union of India* (2020) 3 SCC 637 : 2020 SCC OnLine SC 25 [79].

146 *See*, *for instance*, Smita Nair, 'In Nagaland Lynch Mob: Airline Staffer, Ex-Sepoy, Auto Driver and Teachers' (*The Indian Express*, 12 March 2015) <http://indianexpress.com/article/india/india-others/in-lynch-mob-airline-staffer-ex-sepoy-auto-driver-and-teachers/#sthash.e0Db0VYz.7E6blKuj.dpuf.> ----. For a more gripping account, *see* Durga M. Sengupta, 'Supporters of Dadri "Beef" Murder Use Social Media to Wield Their Weapons', (*Catch News*, 1 October 2015), <http://www.catchnews.com/national-news/supporters-of-dadri-beef-murder-use-social-media-to-wield-their-weapons-1443717569.html> -----.

147 *See*, *for example*, Josh Halliday, 'London Riots: How BlackBerry Messenger Played a Key Role', *The Guardian*, 8 August 2011), <http://www.theguardian.com/media/2011/aug/08/london-riots-facebook-twitter-blackberry>. ----.

148 *Anuradha Bhasin* (n 11).

149 ibid [111].

b. Has internet access been blocked across all platforms or only some platforms (such as mobile phones)? If access is suspended only on one platform, that may point towards greater acceptability of the restriction.[150] However, it is simultaneously important to be cognizant of the disproportionate impact that mobile internet shutdowns have on the economically poor. As per a report by Kantar IMRB, as of December 2018, 97% of India's internet users (total 566 million) are mobile internet users.[151] As per estimates of the Internet and Mobile Association of India, 99% of India's total 451 million internet users use mobile internet.[152] The latter report also suggests that this high percentage is the result the cheap and affordable access offered by mobile platforms.[153] Broadband internet is indeed a luxury, and these compelling numbers prove that disruption of Internet access through shutdowns most affects people who arguably need it the most. Indeed,[154] it may be that an otherwise *partial* ban that only disrupts mobile internet services might effectively be a *total* ban in respect of the economically poor.

c. Does the shutdown involve a complete disruption of internet access or a mere reduction in network bandwidth (from 4G to 2G, e.g.)?

ii. Area: In determining the proportionality of a shutdown, it may be relevant to look at the geographical area over which the shutdown has been imposed vis-à-vis the area where the risk to public order is reasonably apprehended. This "territorial" aspect of proportionality was highlighted in *Anuradha Bhasin*.[155]

iii. Gravity: Proportionality must be judged considering the gravity of the apprehended danger. If great danger to lives is anticipated, such as in a terrorism-prone region, severer restrictions may be placed.[156]

iv. Duration: Finally, the duration of the shutdown vis-à-vis the duration of the apprehended danger is a crucial consideration in determining

---

[150] *Foundation for Media Professionals v UT of J&K*, (2020) 5 SCC 746 [20].

[151] Nandita Mathur, 'India's Internet Base Crosses 500 Million Mark, Driven by Rural India' (*LiveMint*, 11 March, 2019) <https://www.livemint.com/industry/telecom/internet-users-exceed-500-million-rural-india-driving-growth-report-1552300847307.html> -------.

[152] Nielsen, Internet and Mobile Association of India (2019) 10.

[153] ibid.

[154] We are grateful to an anonymous reviewer for this insightful formulation.

[155] *Anuradha Bhasin* (n 11) [78].

[156] *Foundation for Media Professionals v UT of J&K*, (2020) 5 SCC 746 [19].

> the reasonableness of an internet shutdown. This "temporal" aspect of proportionality was also highlighted in *Anuradha Bhasin*.[157]

Every instance of an internet shutdown will therefore have to be analyzed on its own facts and circumstances to determine its constitutional validity. Having outlined the basic constitutional principles, let us now look at how Indian constitutional courts have applied them while adjudicating challenges to the constitutionality of shutdowns.

V. Judicial Approach to Internet Shutdowns

Of the five challenges we chronologically outline below, three were decided by the High Courts of Gujarat, Manipur and Assam respectively, and the other two – both pertaining to internet shutdowns imposed in Jammu & Kashmir – were decided by the Supreme Court.

A. Gaurav Vyas v. State of Gujarat (Gujarat High Court)

In 2015, Gujarat witnessed mass agitations by the Patidar community demanding reservations in public sector jobs and education.[158] When the state government started to lose grip over the law and order situation, it decided to impose a mobile phone internet shutdown in some parts of the state.[159] This lasted for about a week or so, with access being restored in different parts of the state at different times.[160] In this backdrop, law student Gaurav Vyas filed a public interest litigation in the Gujarat High Court arguing that the shutdowns were unconstitutional.[161] He contended that:[162]

---

[157] *Anuradha Bhasin* (n 11) [78].

[158] Nidhi Sinha, 'Patel Agitation Turns Gujarat into a Battlefield' (*LiveMint*, August 27 2015), <http://www.livemint.com/Politics/bYe8fFBsGvJNJXpUmo9M3L/Patel-agitation-turns-Gujarat-into-a-battlefield.html> -------.

[159] Mugdha Variyar, 'Gujarat Bandh: WhatsApp and Mobile Internet Suspended as Hardik Patel Rally Turns Violent' (*International Business Times*, 26 August 2015) <http://www.ibtimes.co.in/gujarat-bandh-whatsapp-mobile-internet-suspended-hardik-patel-rally-turns-violent-644221> accessed ------.

[160] *See,* Express News Service, 'Mobile Internet Ban Ends; Ahmedabad, Surat Last Out' (*The Indian Express*, 2 September 2015) <http://indianexpress.com/article/india/india-others/mobile-internet-ban-ends-ahmedabad-surat-last-out> ------.

[161] *Gaurav Sureshbhai Vyas v State of Gujarat*, 2015 SCC OnLine Guj 6491.

[162] It is important to note that the structure of the petitioner's arguments precluded the High Court from assessing any other potential applicable law governing Internet bans, like the Unified Access License between the State and the telecom companies or Section 5(2) of the Telegraph Act. *See* Nakul Nayak, 'The Anatomy of Internet Shutdowns – I (Of Kill Switches and Legal Vacuums)', (*Centre for Communication Governance Blog*, 29 August 2015) <https://ccgnludelhi.wordpress.com/2015/08/29/the-anatomy-of-Internet-shutdowns-i-of-kill-switches-and-legal-vacuums/>.

i. The applicable law for an internet shutdown is Section 69A of the Information Technology Act, 2000 ("IT Act") and not Section 144 of the CrPC which had been resorted to by the state government.

ii. A total mobile phone internet ban is not narrowly tailored, as blocking only social media websites could have achieved the needed outcome.

The High Court's judgment[163] was disappointing in its lack of reasoning and callous approach towards respecting fundamental rights. In response to the first argument, the Court held that the fields of operation of the two provisions were different. According to the Court, "*Section 69A may in a given case also be exercised for blocking certain websites, whereas under Section 144 of the Code, directions may be issued to certain persons who may be the source for extending the facility of Internet access.*"[164] The Court seemed to suggest that while Section 69A grants powers to the State to block access either to particular websites or the web as a whole, the powers under Section 144 only allow the Executive Magistrate to block access to the web entirely. But the Court does not explain why a reading of the broadly-worded Section 144 does not include disabling access to specific websites. As we have suggested earlier in this paper, both Section 69A of the IT Act and Section 144 of the CrPC empower the respective authorities to suspend access to the entire internet *or* to selectively block access to certain websites; and hence, Section 69A being a special law would totally exclude the applicability of S.144.

Further, the High Court's response to the second argument pertaining to overbreadth reflects its conservative approach towards the right to free speech. The Court rejected the argument for two (shaky)reasons:

> *"…one is that normally, it should be left to the authority to find out its own mechanism for controlling the situation and the second is that* there are number of social media sites which may not be required to be blocked independently or completely. *But if Internet access through mobiles is blocked by issuing directions to the mobile companies, such* may possibly *be more effective approach found by the competent authority.*"[165] *(emphasis supplied)*

The Court's first reason is no reason at all. It is axiomatic that the District Magistrate has a wide discretion in choosing her course of action. But that is neither here nor there, for equally axiomatic is the rule that her decision

---

[163] ibid.
[164] *Gaurav Sureshbhai Vyas v State of Gujarat*, 2015 SCC OnLine Guj 6491 [9].
[165] *Gaurav Sureshbhai Vyas v State of Gujarat*, 2015 SCC OnLine Guj 6491 [11].

must not be unconstitutional. The Court's second argument is essentially a strawman; it was nobody's case that instead of a total mobile internet shutdown, all social media websites should have been banned across mobile phone platforms as well as broadband connections. Indeed, the petitioner's argument had nothing to do with broadband connections. The limited contention was that even as far as mobile phone internet was concerned, there was no need to suspend all websites and only those websites could be suspended which posed a risk to public order. The Court does not consider whether it was warranted to ban non-communication websites such as news sites or e-commerce sites, disabling access to vital information and damaging business interests.[166]

The Court goes on to characterize the shutdown as "minimal" in nature by pointing out that "*access to Internet through broadband and wi-fi facility was permitted or rather was not blocked*."[167] This betrays the Court's conservative attitude towards the freedom of speech and expression. Instead of finding the ban on mobile Internet as a complete prohibition of access to all smart phone users, the Court assures itself of narrowly tailored restrictions by highlighting the continued provision of broadband and Wi-Fi Internet access. In doing so, the Court settles for a comparatively speech-restrictive standard, almost treating the right to Internet access through mobile phones as a privilege. The corollary to the High Court's "minimal damage" reasoning, of course, is that if access to both mobile *and* broadband/Wi-Fi Internet is blocked, there may be grounds for unconstitutionality. The Court says so expressly.[168] However, this allowance had little concrete meaning in that case, and in any event overlooked the fact that mobile internet suspension disproportionately and adversely affects the poor.

In February 2016, Gaurav Vyas filed a special leave petition ("**SLP**") in the Supreme Court against the High Court's judgment.[169] However, a two-judge bench of the Supreme Court dismissed the SLP at the admission stage itself, thereby conferring finality on the High Court judgment.[170]

---

[166] *See generally,* SFLC, Legality of Internet Shutdowns under Section 144 CrPC, (*Software Freedom Law Centre*, 10 February 2016), <http://sflc.in/legality-of-Internet-shutdowns-under-section-144-crpc/>. ----; Also *see* 'Gujarat Mobile Internet Ban: Business Takes a Hit' (*The Indian Express*, August 29 2015) <http://indianexpress.com/article/cities/ahmedabad/mobile-Internet-ban-business-takes-a-hit-2/> ----.

[167] *Gaurav Sureshbhai Vyas v State of Gujarat*, 2015 SCC OnLine Guj 6491 [11].

[168] ibid.

[169] *Gaurav Sureshbhai Vyas v State of Gujarat*, 2016 SCC OnLine SC 1866.

[170] 'Mobile Internet can be Banned under S. 144 CrPC, Says Supreme Court' (*Bar and Bench*, 11 February 2016) <http://barandbench.com/mobile-Internet-can-be-banned-under-s-144-crpc-for-law-and-order-says-supreme-court/>-----.

B. Paojel Chaoba v. State of Manipur (Manipur High Court)

In 2018, widespread protests took place in Manipur seeking the suspension of the then Vice Chancellor of Manipur University on allegations of financial irregularities.[171] Several organizations mobilized support for the protests and agitations.[172] In light of the same, internet services were suspended across the State of Manipur for five days.[173] Within a month of resumption of internet services, they were again suspended for six days by a second order.[174] Paojel Chaoba, a journalist, challenged both suspension orders in the Manipur High Court.

When the second shutdown was in effect, the High Court passed the first preliminary order in the case, ordering the government to restore broadband and Wi-Fi internet facility services for the reminder of the shutdown.[175] Before passing a substantive order, the Court heard all parties andalso took the expert guidance of a system analyst and a computer programmer who found it "technically feasible" to selectively block only certain internet applications "without disturbing the entire mobile internet as a whole".[176] Accordingly, rejecting the state's contention that mobile internet services were suspended in order to prevent misuse of social media networks such as Facebook, WhatsApp etc. on mobile phones, the Court observed that "*other applications of day to day use, such as Paytm etc., are also used widely by the citizens of this country*",[177] thus implying overbreadth in the state's measure.[178] Noting the vitality of internet services for human life, the Court also held that is an "*undeniable fact that mobile internet/data services have become a part and parcel of everyday life of the citizens of this country, irrespective of location and residence and as such, suspension of mobile*

[171] Prasanta Mazumdar, 'Manipur University Vice Chancellor Placed under Suspension by President' (*The New Indian Express* 18 September 2018) <http://www.newindianexpress.com/nation/2018/sep/18/manipur-university-vice-chancellor-placed-under-suspension-by-president-1873884.html)> ----.

[172] ibid.

[173] 'Manipur Suspends Internet Services for 5 Days over MUSU Strike' (*India Today*, 21 June 2018) <https://www.indiatoday.in/india/story/manipur-suspends-internet-services-for-5-days-over-musu-strike-1292293-2018-07-21)> -----.

[174] Trisha Jalan, 'Internet Shutdown: Mobile Internet Suspended for 6 Days in Manipur' (*MediaNama*, 24th September 2018) <https://www.medianama.com/2018/09/223-internet-shutdown-6-days-manipur-university/> -----.

[175] *Aribam Dhananjoy Sharma v State of Manipur*, PIL No. 47 of 2018, decided on 17th November 2018 (available at <https://services.ecourts.gov.in/ecourtindiaHC/cases/display_pdf.php?filename=/orders/2018/203600000472018_4.pdf&caseno=PIL/47/2018&cCode=1&appFlag=)>.

[176] ibid [8].

[177] *Aribam Dhananjoy Sharma* (n 175).

[178] ibid [9].

internet even for a day causes immense inconvenience apart from causing huge dislocation to everyday transactions being carried out by the individuals and organisations across the country".[179] The Court called upon the Government of Manipur to give their opinion on blocking only such online applications like WhatsApp and Facebook and by not suspending mobile internet services in entirety.[180] Subsequently, however, since internet services were not suspended again, the petition was disposed of.[181]

C. Banashree Gogoi v. Union of India & Ors. (Gauhati High Court)

In December 2019, in response to widespread protests against the Citizenship Amendment Bill, 2019 in the State of Assam, the state government suspended – through repeated notifications issued daily – mobile internet services across the state by invoking provisions of the Suspension Rules.[182] Several public interest petitions were filed against this shutdown. On 17th December, the Gauhati High Court noted that no incidents of violence had taken place in the past few days, and passed an order directing the state government to place on record "*the entire material that weighed with the respondents in continuing suspension of internet/mobile data service*".[183] The Court also directed the government to take a considered decision regarding restoring internet services considering the "*improvement in the situation*".[184]

Vide an affidavit dated 19 December, the state government responded by citing intelligence information and submitting that it had taken a considered decision to continue the shutdown.[185] A message from the Director of the Intelligence Bureau was also placed before the Court for its perusal. This message, in the Court's words, was "*in the nature of an advisory to alert the officers and to marshal their resources and ensure maintenance of law and order in their areas as intensification of protests is anticipated and the scale of protest programmes may increase in the days to come.*"[186] This general advisory was the sole reason stated in the government's affidavit for the continuance of the shutdown.

---

[179] Ibid [7].
[180] ibid [110].
[181] *Aribam Dhananjoy Sharma v State of Manipur*, PIL No. 47 of 2018, decided on 17th November 2018, available at <https://services.ecourts.gov.in/ecourtindiaHC/cases/display_pdf.php?filename=rC8SUFuyEFsvB5V61cXUrJV8JyTXijQO1CjKgQ0nSuh%2F9aivpB%2FkNE921cQeXhkc&caseno=PIL/47/2018&cCode=1&appFlag=>.
[182] *Banashree Gogoi v Union of India* 2019 SCC OnLine Gau 5584 [3].
[183] ibid [4].
[184] ibid.
[185] ibid [5].
[186] ibid.

In deciding the issue whether the continuance of internet shutdowns in the state was justified, the Court acknowledged the significance of the internet in everyday life by observing that its suspension "*virtually amounts to bringing life to a grinding halt*".[187] Noting that internet shutdowns must be imposed only when necessary in the given circumstances, the Court held that the said necessity had not been shown by the State:

> *"Very importantly, no material is placed by the State to demonstrate and satisfy this Court that there exists, as on date, disruptions on the life of the citizens of the State with incidents of violence or deteriorating law and order situation which would not permit relaxation of mobile internet services."*[188]

The Court's insistence on *contemporaneous* material is a progressive step. The Court noted that there had been a return to normalcy in the lives of the residents of the State since the day the internet shutdowns were imposed. Many sit-in protests were going on in the state but there had been no reports of violent incidents. These factors together led the Court to conclude that "*the period of acute public emergency which had necessitated suspension of mobile internet services*" had now diminished.[189] Therefore, the Court ordered the state government to "*restore the mobile internet services of all Mobile Service Providers in the State of Assam, commencing 1700 Hrs (5 P.M.) today i.e. 19.12.2019*".[190]

This judgment is an example of tight and principled constitutional reasoning, one that should be emulated in the future. The Court applied the doctrine of proportionality in its truest sense by questioning the government's statements about the need to continue the shutdown. By demanding material from the government, and by declaring that the nexus between the emergency and the restriction had snapped in view of recent events, the Court responsibly exercised its powers of review without adopting an unnecessarily deferential attitude to the government's assessment of the situation.

D. Anuradha Bhasin v. Union of India (Supreme Court)

In August 2019, following the de-operationalization of Article 370 of the Indian Constitution and the consequent revocation of the special status earlier given to the State of Jammu & Kashmir, the central government suspended all modes of communication including internet, mobile and fixed

[187] ibid [8].
[188] ibid [7].
[189] ibid [8].
[190] ibid [10].

line telecommunication services throughout the state.[191] This suspension was challenged in the Supreme Court. In October, the Court was informed by the government that mobile and landline services had more or less been restored in the state, thus rendering the petition moot to that extent.[192] However, internet services remained suspended. Consequently, the judgment extensively addressed the problem of internet shutdowns and their interplay with the freedom of speech.

i. A fundamental right to internet?

The Court made it clear that it was not deciding the question as to whether there was a distinct, free-standing fundamental right to internet in Part III of the Constitution, because no such argument was made before it.[193] But it did answer a different question, i.e. whether the freedom of speech includes the freedom to communicate over the internet. "*There is no dispute*", says the Court, "*that freedom of speech and expression includes the right to disseminate information to as wide a section of the population as is possible*."[194] The Court notes the crucial role of technology and the internet in shaping everyday life in present times – both in terms of sharing information[195] and trade and commerce.[196] "*There is no gainsaying that in today's world the internet stands as the most utilized and accessible medium for exchange of information*."[197] Since the freedom of speech is protected over various media of expression,[198] and since the law must evolve with and adapt to technology,[199] the Court held that Article 19(1)(a) protects the right to speak and express through the medium of the internet.[200]

ii. Production of Suspension Orders in Court

The petitioners before the Court were unable to produce the impugned internet shutdown orders passed under the Suspension Rules since the same were "*not available*".[201] With candour, the respondent government admitted the

---

[191] *Anuradha Bhasin* (n 11), [6].
[192] ibid [10].
[193] ibid [31]. It may be noted that the Kerala High Court has already answered this question in *Faheema Shirin R.K. v State of Kerala*, 2019 SCC OnLine Ker 2976 [15], holding the right to access the internet as part of the rights to education and privacy under Article 21 of the Constitution.
[194] *Anuradha Bhasin* (n 11), [28].
[195] ibid. [25].
[196] ibid [30].
[197] ibid [25].
[198] ibid [29].
[199] ibid [27].
[200] ibid [29].
[201] ibid [14].

unavailability of the orders.[202] Yet it did not produce the orders itself, "*citing difficulty in producing the numerous orders which were being withdrawn and modified on a day-to-day basis*". Instead, the Government produced "*sample orders*" for the Court's perusal.[203]

The Court held that for many reasons the government was obliged to place all orders on record. First, as held in *Ram Jethmalani*,[204] in order for the guarantee contained in Article 32 of the Constitution to be meaningful, it is essential that the petitioners are supplied the information they need to articulate their case effectively, "*especially where such information is in the possession of the State*".[205] Second, the freedom of speech under Article 19(1)(a) also includes the right to receive information – a right crucial to a democracy that is "*sworn to transparency and accountability*" – which entitles the citizen to see the orders.[206] Third, even natural law requires that laws are not passed clandestinely.[207] Therefore, while the government could claim privilege in respect of sensitive matters in some cases, it must ordinarily take proactive steps to produce the orders which are challenged as violative of fundamental rights;[208] mere difficulty in production of orders, the Court held, is not a valid ground to refuse production.[209]

iii. The Legal Framework

The Court noted the three different legal regimes which exist under the IT Act, the CrPC and the Telegraph Act.[210] First, giving "cursory" observations on Section 69A of the IT Act (which was not directly involved in this case), the Court held that the government cannot take recourse to this provision to "*restrict the internet generally*", for the aim of this section is to "*block access to particular websites on the internet*".[211] As suggested earlier in this paper,[212] this reading is not an obvious one and the wide language of Section 69A could be plausibly understood as conferring a wide power on the Central Government to direct a total internet shutdown.

---

[202] ibid [15]
[203] ibid.
[204] *Ram Jethmalani v Union of India* (2011) 8 SCC 1.
[205] ibid [75].
[206] *Anuradha Bhasin* (n 11) [18].
[207] ibid [19].
[208] ibid [20].
[209] ibid [21].
[210] ibid [87].
[211] ibid [88].
[212] See text to note 62 onwards.

Next, noting that the position stands changed since 2017, as states now invoke the Suspension Rules to impose shutdowns,[213] the Court proceeded to discuss their width and scope. The Court read two safeguards into the provision in the process. First, interpreting the Suspension Rules in light of Section 5(2) of the Telegraph Act, the Court held that the existence of a "public emergency" is *sine qua non* for the invocation of the Rules.[214] Second, even though the Rules do not expressly mandate the publication of the orders passed thereunder, the Court read this requirement into the Rules by holding that all such orders must be "*made freely available… through some suitable mechanism*."[215]

iv. Reasonableness of the Restriction

In addition to recounting the well-settled principles against which the reasonableness, proportionality and least intrusiveness of a restriction should be measured,[216] the Court acknowledged the serious security problems that have plagued the State of Jammu & Kashmir,[217] and also the fact that the internet is a ready tool for modern terrorism.[218] The ultimate question which would hence need to be answered in determining the validity of a restriction is "*whether there exists a clear and present danger*" that justifies the restriction.[219] Certain factors are useful in conducting this inquiry: "*the territorial extent of the restriction, the stage of emergency, nature of urgency, duration of such restrictive measure and nature of such restriction*."[220] Applying these principles, the Court held that the government must analyse the precise "stage" of the public emergency before invoking the Suspension Rules. It is only in light of the stage of the emergency that the proportionality of the impugned measure can be ascertained.[221] Shutdown orders may be passed only when it is "*necessary*" and "*unavoidable*" to do so, i.e. when no "*less intrusive remedy*" exists.[222] Specifically, the State must explore the alternative of blocking access only to social media web sites rather than to the entire internet.[223]

---

213 ibid [91].
214 ibid [100].
215 ibid [104].
216 ibid [34]-[37], [77].
217 ibid [38].
218 ibid [39].
219 ibid [38].
220 ibid [79].
221 ibid [102].
222 ibid [108].
223 ibid [111].

Equally, shutdown orders under the Suspension Rules must have a specified duration. Holding that indefinite orders are simply "*impermissible*" and noting that the Suspension Rules do not specify the maximum time period for which a suspension order may be in operation, the Court recommended that the legislature fill this gap.[224] In the meanwhile, the Court laid down an important procedural safeguard: the Court directed the Review Committee constituted under the Rules to conduct a periodic review of the suspension order every seven days.[225] In conducting this review, the Committee had to not only check whether the suspension complied with the requirements contained in Section 5(2) the Telegraph Act, but also whether it was proportionate and necessary.[226]

v. Relief Granted and Implications

In line with the above principles, the Court directed the government to: (i) publish all orders presently in force passed under Section 144 of the CrPC for suspension of telecom or internet services, and (ii) forthwith review all orders suspending internet or telecom services, revoking those contrary to this judgment. It is curious that despite the non-publication and non-production of the orders, the Court did not strike them down. Nevertheless, the Court instituted a strict and meaningful review mechanism, thereby filling up the lacunae in the Suspension Rules. This development should, therefore, be welcomed.

The judgment has practically not yielded results commensurate with its potential. *Anuradha Bhasin* was decided on 10 January 2020. It was almost two months later – on 4 March 2020 – that the people of Jammu & Kashmir first regained access to 2G internet.[227] Till date,[228] 4G internet has not been restored in the region. This is despite the fact that the country is facing the pandemic of COVID-19. To add to the misery, the Supreme Court delivered a highly unfortunate judgment on 11 May 2020 (discussed below), where, despite clear violations of *Anuradha Bhasin* having been pointed out by the Petitioners in that case, the Court refused to interfere with the government's unconstitutional actions.

---

[224] ibid [108]-[109].
[225] ibid [109].
[226] ibid.
[227] 'Social Media Ban Lifted in J&K, can Access Internet on 2G', (*India Today*, 4th March 2002) <https://www.indiatoday.in/india/story/social-media-mobile-internet-access-2g-jammu-kashmir-1652376-2020-03-04>.
[228] This paper was finalized on 15 May 2020.

E. Foundation for Media Professionals v. UT of J&K (Supreme Court)

On 30 March 2020, a non-governmental organisation called Foundation for Media Professionals filed a public interest petition in the Supreme Court challenging the restriction of internet services in Jammu & Kashmir to 2G bandwidth.[229] The petition further prayed for a direction that 4G services be restored in the region with immediate effect.[230] Given the unique times in which the petition was filed, the grounds raised in the petition reflected various fundamental rights in addition to the freedom of speech, including the right to health,[231] education,[232] access to justice,[233] trade,[234] and livelihood.[235] Additionally, the petition raised the broad argument that the restriction on 4G internet is disproportionate given the special circumstances posed by COVID-19[236] and for breaching the imperative requirements of stating the material facts,[237] being the least intrusive measure[238] and being temporally limited[239] as laid down in *Anuradha Bhasin*.

i. The Government's Response

The government of Jammu & Kashmir filed its counter-affidavit on 28 April 2020. Their case, in brief, was as follows: there exists no fundamental right to the internet, and the internet can hence be restricted as a medium of communication.[240] As far as proportionality is concerned, the region is engaged in a war against terrorism which warrants restrictions to be placed on the internet,[241] as there are chance that social media will be misused by terror groups.[242] There are also chances of fake news spreading through social media.[243] Despite this, restrictions are gradually being lifted in the state step-

---

[229] Memorandum of Writ Petition, *Foundation for Media Professionals v UT of J&K*, (2020) 5 SCC 746, <https://drive.google.com/file/d/1u8T6zldNXlabjA0igdXObA55fyX2_4Bz/view>.
[230] ibid, 28, 32-33, 36, 57.
[231] ibid, 28.
[232] ibid, 37.
[233] ibid, 39.
[234] ibid, 38.
[235] ibid.
[236] ibid, 45.
[237] ibid, 52.
[238] ibid, 45-47.
[239] ibid, 49.
[240] Counter-Affidavit, *Foundation for Media Professionals v UT of J&K*, (2020) 5 SCC 746, 8 <https://images.assettype.com/barandbench/2020-04/179854fd-1307-41a9-8169-e78c-ca9e726c/J_K_Govt_Reply_2G_Restriction_compressed.pdf>.
[241] ibid, 9, 18.
[242] ibid, 11.
[243] ibid, 18.

by-step,[244] and the only present restriction on internet services is reduced speed for mobile internet[245]while fixed-line internet services remain available.[246] In addition, to avert any harm to people's health and education etc., they are being reached physically as well as through television, radio, and phone calls etc.[247]

ii. Violation of settled law

The Court observed that the suspension order "*does not provide any reasons to reflect that all the districts of the Union Territory of Jammu and Kashmir require the imposition of such restrictions*."[248] Despite this, blanket shutdown orders had been imposed throughout Jammu & Kashmir.[249] This is an implicit acknowledgement that the State did not abide by the law laid down in *Anuradha Bhasin* on two counts. *Anuradha Bhasin* had held, firstly, that internet shutdown orders passed under the Suspension Rules must contain reasons (as a legality requirement flowing from the text of Section 5 of the Telegraph Act),[250] and secondly, that in order to be narrowly tailored and least intrusive, the restrictions must be territorially limited.[251] Despite this clear acknowledgement, however, the Court did not declare the restrictions unconstitutional.

iii. The Court's Abdication

Despite noting the above violations, the Court termed these violations on the one hand and the prevalent militancy in Jammu & Kashmir on the other as "competing considerations".[252] It noted that the petitioners' contentions would merit consideration in "*normal circumstances*".[253] But cross-border terrorism in Jammu & Kashmir amounts to a "*compelling*" circumstance, according to the Court, which "*cannot be ignored*".[254] Further, the Court considered it relevant that the Government had been gradually lifting restrictions in the region and taking various steps to ensure that the rights of the people in context of COVID-19 are safeguarded.[255] For these reasons, the

---

[244] ibid,7.
[245] ibid, 9.
[246] ibid, 17.
[247] ibid, 20-24.
[248] *Foundation for Media Professionals v UT of J&K*, (2020) 5 SCC 746 [16].
[249] ibid, [18].
[250] *Anuradha Bhasin* (n 11) [102].
[251] ibid [78]-[79], [143].
[252] *Foundation for Media Professionals* (n 248) [16].
[253] ibid [19].
[254] ibid.
[255] ibid [20].

Court refused to interfere with the internet shutdown orders. However, in an apparent attempt to provide some remedy to those whose rights are continuously being affected, the Court directed a "Special Committee" comprising of the Union Home Secretary, the Union Communications Secretary, and the Chief Secretary of Jammu and Kashmir to "immediately" determine the necessity of the restrictions in place.[256] We submit that this judgment is problematic for at least four reasons.

First, the Court forgets that lawfulness and reasonableness are distinct requirements under Article 19(2), both of which must be independently satisfied by the restriction in question.[257] While the situation of militancy in Jammu & Kashmir might weigh heavily in judging the *proportionality* (reasonableness) of the internet shutdown, it has no relevance in determining the *legality* which must be judged solely with reference to the statute under which the orders have been issued. Hence, once the Court had acknowledged that the unreasoned suspension orders were illegal for being in contravention of Section 5(2) of the Telegraph Act and the corresponding legal principles laid down in *Anuradha Bhasin*, there was no question of balancing this illegality with the security risks plaguing Jammu & Kashmir, for the two are not "competing considerations".[258] The suspension orders deserved to be struck down as unlawful without further discussion.

Second, *Anuradha Bhasin* is clear on the point that the State must consider less restrictive alternatives before resorting to a total shutdown.[259] Specifically, the State must apply its mind to the possibility of disrupting access only to specific websites rather than the entire internet.[260] It was hence imperative for the Court to demand justifications from the Government as to whether it considered allowing selective 4G access to websites that did not pose any threat to public order. Yet, this aspect is not dealt with anywhere in the judgment.

Third, as has been argued,[261] the Court's approach amounts to abdication of the constitutional responsibility vested in it. Article 32 of the Constitution, under which the right to move the Supreme Court for redressal of rights

---

[256] ibid [23].

[257] Constitution of India 1950, art 19(2).

[258] See Sarvjeet Singh, 'Supreme Court's Order on Kashmir Internet Shutdown: Judicial Abdication or Judicial Restraint?' (*Times of India*, 12 May 2020) <https://timesofindia.indiatimes.com/blogs/voices/supreme-courts-order-on-kashmir-internet-shutdown-judicial-abdication-or-judicial-restraint/> accessed on 15 May 2020.

[259] *Anuradha Bhasin* (n 11) 77.

[260] ibid [111].

[261] Shrutanjaya Bhardwaj, 'Supreme Court Verdict on 4G in Jammu and Kashmir Undermines the Rule of Law' (*The Wire*, 14 May 2020) < May 2020.

violations is "guaranteed",[262] has been held as implying that the Court has the role of a "sentinel on the *qui vive*" and a "solemn duty to protect… fundamental rights zealously and vigilantly".[263] The Court does not even have the option to direct the petitioners before it to approach the relevant High Court,[264] let alone a committee comprising only of executive members.

Fourth, all three members of the Special Committee function under the control of the Central Government. Two of them (Union Home Secretary and the Chief Secretary of Jammu and Kashmir) were respondents before the Court in this very case. Directing all issues to be decided by a committee of this nature amounts to making the executive a judge in its own cause, thus breaching the principles of checks and balances as well as separation of powers that are central to the Indian Constitution.[265]

This problematic approach adopted by the Supreme Court demonstrates that rights adjudication is as much about judicial attitudes as it is about strong legal principles. The Court should have been stricter in its approach and taken the Government to task for its failure to abide by settled legal principles. Allowing the Government to get away with these violations undermines the rule of law. It sends the message that the security problems in Jammu & Kashmir are a license to overlook constitutional requirements.[266]

VI. Conclusion: The Way Ahead

This paper has attempted to sketch the legal and constitutional framework that governs internet shutdowns in India. We discussed the three-pronged test of Article 19(2) which requires that any restrictions on the freedom of speech be lawful, legitimate and reasonable. We elaborately discussed the meanings of these three concepts and how they would apply in context of internet shutdowns. We also saw examples from case law where Indian constitutional courts have applied these principles to concrete facts, some in more satisfying ways than others.

Two issues that would require further research can briefly be stated here. First, *Anuradha Bhasin* mandates periodic review of suspension orders issued under the Suspension Rules. An analysis of how this safeguard plays out in practice might be useful. Is the periodic review meaningful? Do the process

---

[262] Constitution of India 1950, art 32.
[263] *Prem Chand Garg v Excise Commr.*, AIR 1963 SC 996 : 1963 Supp (1) SCR 885 [2].
[264] See e.g. *Romesh Thappar v State of Madras*, AIR 1950 SC 124 : 1950 SCR 594 [3].
[265] Bhardwaj (n 261).
[266] ibid.

and the Committee's orders reflect due application of mind? Empirically, how often does the review committee declare the imposition or/and continuance of the shutdown illegal and unnecessary? Second, it is important to examine the options offered by technology in terms of narrowing censorship to only those websites, regions and communication platforms where it is necessary. The judgment in Anuradha Bhasin reveals that the Court had put a specific query to the Solicitor General as to the feasibility of blocking only social media websites, to which he had responded by saying that the same was not feasible.[267] On the other hand, when the Manipur High Court sought expert help in determining whether partial blocks were technologically possible, it was told that they are possible.[268] This is a technical question which concerns information technology, and is best answered through research by competent professionals from the field.

[267] *Anuradha Bhasin* (n 11) [111].

[268] *Aribam Dhananjoy Sharma v State of Manipur*, PIL No. 47 of 2018, decided on 17th November 2018 <ode=1&appFlag=>.

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 2020	Rs.
Hard Copy for 2019	Rs. 900
Hard Copy for 2018	Rs. 900
Hard Copy for 2017	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)