PROTECTING CITIZENS FROM THE STATE POST *PUTTASWAMY*: ANALYSING THE PRIVACY IMPLICATIONS OF THE JUSTICE SRIKRISHNA COMMITTEE REPORT AND THE DATA PROTECTION BILL, 2018

—Vrinda Bhandari and Renuka Sane[*]

In this paper we seek to conceptualise the right to privacy and its implications from the State and private actors, post the Puttaswamy judgment. We then examine the draft Personal Data Protection Bill, 2018 submitted by the Justice Srikrishna Committe and evaluate how it has fared in regulating the actions of the State relative to the private sector, with a broad focus on consent, surveillance, and the interaction between the State and private sector including the ability of the latter to deny data requests of the former. Finally, we emphasize the implementation challenges of a legislation given the weak state capacity in India, focusing on regulation making and enforcement, and highlight that both give substantial power to the State (as regulator) over its regulated entities. We argue that considering the privacy concerns against State action, the challenge to implementation in the area of personal data may only get exacerbated.

Introduction 144
Understanding the nature of the right to privacy 146
Privacy against the State and private actors . 148
Privacy from the State 149
Privacy from non-State actors 152
Why the "I have nothing to hide" argument is misconceived 154

[*] Vrinda Bhandari is an Advocate in the Delhi High Court and Renuka Sane is an Associate Professor at the National Institute of Public Finance and Policy. This paper has been adapted from a previous 2016 paper, *Towards a privacy framework for India in the age of the internet*" that was presented at the 1st Law and Economics Policy Conference, New Delhi in 2016. We thank Sunil Abraham for his comments at the conference and Shubho Roy, Smriti Parsheera, Faiza Rehman, Amba Kak, and Risabh Bailey for useful discussions.

Need for a privacy law 155
Analysing the Personal Data Protection Bill 2018 and its treatment of the State and the private sector 157
Consent 158
Surveillance 159
Interaction between the State and non-State actors 162
Moving from law to implementation 163
Regulation making 164
Enforcement 166
Conclusion 168

I. INTRODUCTION

In recent times, privacy considerations arising out of the Cambridge Analytica scandal, the WhatsApp-Facebook privacy sharing arrangement, the Apple-FBI dispute, the Snowden leaks, and the Aadhaar Act have dominated headlines. The rise of data analytics and the increasing availability, storage, and ease of mining of personal information online has created a public policy conundrum over balancing the benefits of big data with the threat to the right to privacy.[1]

Countries across the world have responded to some of these concerns by revisiting their privacy legislation and imposing additional safeguards. The EU General Data Protection Regulation, 2016/679 ('GDPR') came into force in 2018, replacing the EU Data Protection Directive of 1996, in a bid to adapt the EU data protection framework to address modern technology-privacy conundrums. In 2016, the U.S. and the EU also entered a new data transfer framework agreement - the 'Privacy Shield' - intended to protect the privacy of data of European users stored in the U.S.[2] The Obama White House commissioned various reports on big data and privacy[3] and various consumer privacy Bills have been introduced in the U.S.[4]

Meanwhile in India, two years after the reference in 2015, a nine judge bench of the Supreme Court unanimously ruled in *K.S. Puttaswamy* v. *Union of India* ('Puttaswamy')[5] that the right to privacy is protected as an intrinsic part of the

---

1 *See* generally, Omer Tene and Jules Polonetsky, *Privacy in the Age of Big Data: A Time for Big Decision*s, 64 STAN. L. REV. ONLINE 63-69 (2012); President's Council of Advisors on Science and Technology (PCAST), *Big Data and Privacy: A Technological Perspective*, Executive Office of the President, White House (2014).

2 This agreement replaced the 16 year old Safe Harbour Agreement, which was declared invalid by the European Court of Justice in *Maximillian Schrems* v. *Data Protection Commr.*, Case C-362/14 (2015) in October 2015 in the wake of Snowden's revelations about the NSA's surveillance activities.

3 *See* generally, PCAST, *supra* note 1; John Podesta et al, *Big Data: Seizing Opportunities, Preserving Values*, Executive Office of the President, White House (2014); Richard Clarke et al, *Liberty and Security in a Changing World*, Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies (2013).

4 Consumer Privacy Protection Act of 2017 was introduced as H.R. 4081 in the U.S. Congress. In 2015, the Obama Administration introduced the Consumer Privacy Bill of Rights Act as a draft Bill.

5 (2017) 10 SCC 1.

right to life and personal liberty under Article 21 and other freedoms guaranteed by Part III of the Constitution. Although the court was unanimous in recognizing privacy as a fundamental right, the nine judges, in six separate opinions, differed in their articulation of the right to privacy and the tests applicable in case of a violation of the right.[6] During the course of the hearing in *Puttaswamy,* the government constituted a committee of experts chaired by Justice B.N. Srikrishna ('Justice Srikrishna Committee') to, *inter alia,* review data protection norms in India and make recommendations. The Committee released a White Paper on Data Protection in 2017 ('White Paper'),[7] and a submitted its final report titled, 'A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians' ('the Report') along with a draft law, 'The Personal Data Protection Bill, 2018' ('the Bill') in July 2018.[8] This has led to a healthy public debate on the way forward. The discourse today rests on a growing body of work that has examined the jurisprudential development and state of law of privacy in India[9] and the various model privacy laws that have been drafted over the years.[10] In the early years, privacy concerns were mostly related to the State. The advent of big data and the internet of things moved the discussion to privacy infringements by the private sector. The lines between the two are now indistinct, especially because the State is increasingly able to use the private sector to improve surveillance often for reasons of efficiency in service delivery or concerns about national security, bringing us back to the threats imposed by the State.

---

6 The judgment consisted of six separate opinions, with the plurality (and longest) opinion being authored by Justice Chandrachud on behalf of three other judges - Chief Justice Khehar, Justice Nazeer, and Justice Agrawal. However, given that only four judges signed this opinion, it does not constitute the majority opinion, and surprisingly does not refer to any of the concurring opinions of the other judges. Five other concurring opinions have been pronounced by Justice Chelameswar, Justice Bobde, Justice Nariman, Justice Sapre, and Justice Kaul.

7 Ministry of Electronics and Information Technology, *White Paper of the Committee of Experts on a Data Protection Framework for India* (2017), http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf ('White Paper').

8 *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians*, Committee of Experts under the Chairmanship of Justice B.N. Srikrishna (July 2018), http://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report-comp.pdf ('Report'). The draft 'Personal Data Protection Bill, 2018' is available at http://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill%2C2018_0.pdf.

9 Vrinda Bhandari and Renuka Sane, *Towards a Privacy Framework for India in the Age of the Internet*, Working Paper No. 179, NIPFP Working Paper Series (Oct. 2016); Planning Commission, Government of India, *Report of the Group of Experts on Privacy* chaired by Justice (Retd.) A.P. Shah, (2012) ('Justice Shah Report'); Centre for Internet & Society, *Privacy in India: Country Report* (2011); CRID-University of Namur, *First Analysis of the Personal Data Protection Law in India* (2006), http://www.crid.be/pdf/public/5946.pdf; Abhayraj Naik, *Privacy at the Stake in the Supreme Court*, Socio-Legal Rev. Forum (Aug. 23, 2017), http://www.sociolegalreview.com/privacy-at-the-stake-in-the-indian-supreme-court/.

10 Centre for Internet & Society, *Privacy (Protection) Bill 2013*, https://cis-india.org/internet-governance/blog/privacy-protection-bill-2013-updated-third-draft; *The Indian Privacy Code 2018*, https://saveourprivacy.in/bill; *The Data (Privacy and Protection) Bill, 2017*, introduced as a Private Member Bill No. 100 of 2017 in the Lok Sabha by Sh. Baijayant Panda, MP, http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/889LS%20AS.pdf. The government had introduced two draft Privacy Bills in 2011 and 2014, but they are not available publicly.

Against this background, our contribution to this debate is three-fold - first, we seek to conceptualise the right to privacy, post *Puttaswamy*, in the age of the internet and big data, and its implications for the State and private actors. We explain why privacy matters, both in the context of the State and private entities, and the blurring distinction between them. We also argue that the "I have nothing to hide" argument is misconceived, particularly given the significant consequences of inadequate privacy protection, ranging from 'chilling effect' on speech, to increased profiling and discrimination.

Second, we examine those aspects of the draft Bill that touch upon the public-private distinction. We evaluate how it has fared in regulating the actions of the State and private sector, with a broad focus on consent, surveillance, and the interaction between the State and private sector (including the (in)ability of the latter to deny data requests of the former).

Third, we emphasize the implementation challenges of a legislation given the weak state capacity in India. We focus on two aspects of implementation, namely regulation making and enforcement, and highlight that both give substantial power to the State (as regulator) over its regulated entities. We argue that considering the privacy concerns against State action, the challenge to implementation in the area of personal data may only get exacerbated.

II. UNDERSTANDING THE NATURE OF THE RIGHT TO PRIVACY

As *Puttaswamy* illustrates, there are various accounts and definitions of privacy. A 'descriptive' account of privacy views it as a condition or state of being.[11] At the lowest common denominator, it is seen as the right to be left alone,[12] or being able to be free from certain kinds of intrusions.[13] Parent describes privacy as the condition of not having undocumented personal knowledge about one possessed by others.[14] In a descriptive account, thus, the right to privacy would include a bundle of rights such as the right to privacy of beliefs, thoughts, personal information, home, and property. This view is reflected in international texts such as Article 8 of the European Convention on Human Rights and Article 17 of the International Covenant on Civil and Political Rights, as the right to respect for private and family life, home and correspondence. In the United States, it is reflected in the idea that a person's "home is their castle", which is a zone of privacy that is secure from the prying eyes of the State.[15]

---

[11] Adam Moore, *Defining Privacy*, 39(2) J. OF SOC. PHILOSOPHY 411, 412 (2008).

[12] Samuel Warren and Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890).

[13] Thomas Scanlon, *Thomson on Privacy*, 4(4) PHIL. AND PUB. AFFAIRS 315 (1975).

[14] William Parent, *Privacy, Morality and the Law*, 12(4) PHIL. AND PUB. AFFAIRS 269 (1983).

[15] Thomas Cooley, A Treatise on the Constitutional Limitations Which Rest Upon the Legislative Power of the States of the American Union (Little, Brown and Co, 1871); Jonathan Hafetz, *"A*

A descriptive account stands in contrast with the 'normative' account of privacy, which views privacy as a *moral* claim against third parties to desist from certain actions.[16] It answers the question of why we value privacy and places privacy at the heart of our identity, dignity, sense of self, and ability to have intimacy and meaningful inter-personal relations. It is also seen as the claim of individuals to "*determine for themselves when, how, and to what extent information about them is communicated to others*".[17] Privacy, thus, determines our interaction with our peers, the society and the State. Such a normative account was given judicial recognition by the Inter-American Court of Human Rights in the *In Vitro Fertilization* case,[18] which grounded the understanding of privacy in dignity and autonomy. The nine judges in *Puttaswamy* too, were unanimous in their view of privacy forming the constitutional core of human dignity and autonomy.

In fact, in *Puttaswamy,* both Justice Chandrachud (writing the plurality opinion on behalf of himself and three other judges) and Justice Bobde (in his concurrence) expressly recognized the descriptive and normative aspects of privacy.[19]

There are other accounts and definitions of privacy as well. Privacy has also been studied as a relational concept, based on the nature of inter-personal interaction;[20] as an account of control and access;[21] and as a cultural concept.[22] It can also be understood in respect of the answer to the question, privacy *from whom*, whether the State or private actors.

These views were echoed by different judges in their concurring opinions in *Puttaswamy.* Thus, for Justice Bobde, privacy is a relational, context-dependent right that allows an individual to *choose* to perform a certain activity and *specify* who to include while performing it. This right is not lost when an individual

---

Man's Home is His Castle?": Reflections on the Home, the Family, and Privacy During the Late Nineteenth and Early Twentieth Centuries, 8(2) WILLIAM & MARY J. OF WOMEN & L. 175 (2002).

16 Moore, *supra* note 11, at 413.

17 Alan Westin, Privacy and Freedom, (Atheneum Publishers, 1967).

18 *Artavia Murillo (In Vitro Fertilization)* v. *Costa Rica*, 2012 SCC OnLine IACTHR 30. The IACHR, while deciding a challenge to the presumed general prohibition of in vitro fertilisation in Costa Rica ruled that the protection of private life includes a "*series of factors associated with the dignity of the individual*", including, for instance, the ability to develop one's own personality and aspirations, to determine one's own identity, and to define one's personal relationships.

19 Justice Chandrachud, at para 322 stated, "*Privacy has both a normative and descriptive function. At a normative level privacy subserves those eternal values upon which the guarantees of life, liberty and freedom are founded. At a descriptive level, privacy postulates a bundle of entitlements and interests which lie at the foundation of ordered liberty.*" See also Justice Bobde, para 407 in *Puttaswamy.*

20 Leon Green, Relational Interests, 29 ILLINOIS L.REV. 460 (1934).

21 Richard Parker, *A Definition of Privacy*, 27 RUTGERS L.R. 275 (1974).

22 For instance, Germany has one of the strongest data protection and privacy laws in the world, in part due to its history and the rise of the Third Reich. On the other hand, India, with its large joint families and way of life, has traditionally not viewed privacy as a central tenet to daily living, although this is changing. See also Irwin Altman, *Privacy Regulation: Culturally Universal or Culturally Specific?*, 33(3) J. OF SOC. ISSUES 66 (1977).

moves about in public, and in fact, serves as a 'spring-board' for the exercise of other fundamental freedoms. Justice Chandrachud noted that privacy is a concomitant of the right of the individual to exercise control over their personality. Justice Kaul, meanwhile, focused on the distinct privacy claims against the State and non-State actors, especially in a diverse social and cultural context. In respect of the State, he identified concerns of surveillance and profiling, whereas in respect of private actors, he emphasized the impact of big data and technology on pervasive data generation, collection, and use in a digital economy.

Justice Chelameswar and Justice Nariman in their separate opinions endorsed Gary Bostwick's[23] framework of privacy as 'repose' (freedom from unwarranted stimuli), 'sanctuary' (protection from intrusive observation) and 'intimate decision' (autonomy to make personal life decisions). Justice Nariman further classified privacy rights into three categories – those involving invasion by the State into a person's personal rights and body; informational privacy, relating to a person's mind; and privacy of choice. Finally, Justice Sapre focused on the importance of the Preamble to the Constitution, and its principles of liberty, dignity, and fraternity.[24]

Our view, in line with that of Solove,[25] is that a single definition of privacy is "*not possible, and perhaps not necessary*", so long as its value and meaning are understood in a comprehensive fashion. For the purpose of this paper, we view privacy primarily from a descriptive account, but try and understand why we should worry about the actions of the State and private entities from a normative perspective.

III. PRIVACY AGAINST THE STATE AND PRIVATE ACTORS

Privacy can be eroded by a single act or through multiple/period actions of information collection and profiling, both by the State and private actors - from monitoring our call records to tracking our movement and browsing history. As *The Economist* proclaimed, data is the new oil, and it has given rise to an entirely new economy.[26]

---

[23] Gary Bostwick, *A Taxonomy of Privacy: Repose, Sanctuary, and Intimate Decision*, 64 CALIFORNIA L. REV 1447 (1976).

[24] For a further discussion on *Puttaswamy*, see Vrinda Bhandari et al, *An analysis of Puttaswamy: the Supreme Court's privacy verdict*, The Leap Blog (Sept. 20, 2017), https://blog.theleapjournal.org/2017/09/an-analysis-of-puttaswamy-supreme.html; Alok Prasanna Kumar, *Supreme Court's Privacy Judgment: Contradictions and Unanswered Questions*, 52(38) ECON. & POL. WEEKLY 10 (2017).

[25] Daniel Solove, Understanding Privacy 5, 8 (Harvard University Press, 2008).

[26] *The world's most valuable resource is no longer oil, but data*, The Economist (May 6, 2017), https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data; *Data is giving rise to a new economy*, The Economist (May 6, 2017), https://www.economist.com/briefing/2017/05/06/data-is-giving-rise-to-a-new-economy. However, *per contra*,

Concomitantly, the advancement of big data technologies and the ensuing ease of re-identification has disrupted the faith placed in anonymisation and pseudonymisation as measures to protect the privacy of an individual.[27] These developments give rise to a vociferous debate – *from whom* do we need to protect our privacy, and *why* do we need to do so, especially if we have nothing to hide, or because there are other benefits to be accrued, especially by the poor, who may value privacy differently. These questions, which we answer in this section, assume importance in light of the differential treatment to the State and private sector by the Srikrishna Committee in the 2018 Bill.

A. Privacy from the State

The debate around right to privacy has its origins in the capacity (and asymmetric power) of the State to intrude into the lives of its citizens. Traditionally, individuals have different privacy expectations from different classes of people and have a greater privacy expectation from the State than from private actors.

This is partly due to the fact that relationships between individuals and corporations or between individuals *inter se*, are defined by *consent, choice,* and *control*, even if illusory.[28] This is unlike the relationship between citizens and the State, where governments wield greater influence in our lives, primarily due to their coercive and police powers, including the power to prosecute and punish; to legally place citizens under surveillance; and even to harass/intimidate dissidents.[29] The State thus, enjoys a monopoly of power in every sphere of human existence and privacy rights against it are premised on the ideals of freedom, liberty, and dignity.

---

see Bernard Marr, *Here's Why Data Is Not The New Oil,* Forbes (Mar. 5, 2018), https://www.forbes.com/sites/bernardmarr/2018/03/05/heres-why-data-is-not-the-new-oil/#7bb076d33aa9.

[27] A recent study analysing three months of credit card records of 1.1 million individuals found that using only four spatio-temporal points was enough to uniquely re-identify 90% of individuals (Yves-Alexandre de Montjoye et al, *Unique in the Shopping Mall: On the Reidentifiability of Credit Card Metadata*, 347 (6221) Science 536 (2015). See also Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. Rev. 1701 (2010); Latanya Sweeney, *Simple Demographics Often Identify People Uniquely*, CMU Data Privacy Working Paper 3 (2000); Arvind and Vitaly Shmatikov, *Robust De-anonymization of Large Sparse Datasets*, Proceedings of 2008 IEEE Symposium on Security and Privacy, 111 (2008).

[28] Apart from the choice to opt out of technology (even if that is not always a preferred option), customers have some modicum of choice in choosing the extent to which they will engage with technology, and a choice between service providers in a competitive big data market. For instance, the maximum power that Uber can exercise over me is by throwing me off the Uber Platform. Nevertheless, I still have the option to turn to other transportation service providers, such as Ola. The problem, however, is that network effects make it difficult for viable alternatives to proliferate – many people do not think that Facebook has any alternatives; DuckDuckGo, despite offering better privacy protection, is not even close to Google in its market share for search engines. The problems arising due to this will be detailed in the next part.

[29] Laurent Sacharoff, *The Relational Nature of Privacy*, 16(4) Lewis & Clark L. Rev. 1249, 1274-1280 (2012), identifying three harms caused by the State, in the case of a search and seizure, namely (a) intrusion harm (b) downstream harms and (c) conviction and punishment.

This power is best reflected in the practice of surveillance. While surveillance has existed for long, technological advances have allowed government to engage in new forms of electronic surveillance and predictive policing[30] at an unprecedented scale, without being impeded by traditional resource constraints. This has made it almost impossible to realise that one's privacy is being infringed, or to know what information is being held about oneself, as was best illustrated in the Snowden and GCHR/PRISM program revelations in the U.S. and U.K. Even courts have become cognizant of these shifts in technology (such as GPS monitoring) that enable continuous long-term tracking of the movements of individuals.[31] China now has a 'social credit system', which continuously monitors and evaluates citizens to eventually arrive at a trust score. It is said to have already blocked citizens from taking more than 11 million flights and 4 million train trips.[32]

India has traditionally had weak regulation of surveillance and oversight of law enforcement agencies. Communications surveillance by the government is regulated by the Telegraph Act, Information Technology Act, 2000 ('IT Act'), and the relevant Rules notified thereunder.[33] We also have the Central Monitoring System ('CMS'), which provides the Government with instantaneous and direct access to the traffic flowing through TSP networks, without their manual intervention; and the Networks Traffic Analysis ('NETRA'), which is a dragnet surveillance system that can analyse internet traffic based on pre-defined search filters such as 'bomb', 'attack', 'kill'.[34] However, the legality of these tools is sus-

---

[30] Perry Walter et al, *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations*, *RAND Corporation* (2013); Karn Singh, *Preventing crime before it happens: How data is helping Delhi Police*, Hindustan Times (Feb. 27, 2017), https://www.hindustantimes.com/delhi-news/delhi-police-is-using-precrime-data-analysis-to-send-its-men-to-likely-trouble-spots/story-hZcCRyWMVoNSsRhnBNgOHI.html.

[31] *United States* v. *Jones*, 2012 SCC OnLine US SC 13 : 181 L Ed 2d 911 : 132 S Ct 945, at 955-956 : 565 US 400 (2012) (Sotomayor J. concurring) and *Carpenter* v. *United States*, 2018 SCC OnLine US SC 60 : 201 L Ed 2d 507 : 585 US (2018). A lot of litigation is currently taking place around the change in WhatsApp's privacy policy, after its acquisition by Facebook and India, the Supreme Court is currently hearing the petition in *Karmanya Singh Sareen* v. *Union of India*, SLP (C) No. 804 of 2017 (SC) (Pending).

[32] Rachel Botsman, *Big data meets Big Brother as China moves to rate its citizens*, Wired (Oct. 21, 2017), https://www.wired.co.uk/article/chinese-government-social-credit-score-privacy-invasion; Tara Chan, *China's social credit system has blocked people from taking 11 million flights and 4 million train trips*, Business Insider (May 21, 2018), https://www.businessinsider.in/Chinas-social-credit-system-has-blocked-people-from-taking-11-million-flights-and-4-million-train-trips/articleshow/64255175.cms.

[33] Section 5(2) of the Telegraph Act read with Rule 419A of Telegraph Rules regulates telephone tapping. The relevant provisions of the IT Act, that govern surveillance of communication devices and activities over the internet are Sections 69, 69B, 28, 29 and various Rules. Apart from this, various conditions, including for CMS, have been included in telecom license agreements that enable surveillance. For more details, see, Vipul Kharbanda, *Policy Paper on Surveillance in India*, The Centre for Internet & Society (Aug. 2015), https://cis-india.org/internet-governance/blog/policy-paper-on-surveillance-in-india.

[34] CMS was announced by a press release in 2009 and NETRA in 2014. *See* Press Information Bureau, *Centralised System to Monitor Communication*, (Nov. 26, 2009), http://pib.nic.in/newsite/

pect, especially after the ruling in *Puttaswamy*[35] and the provisions in the new Bill, that will be discussed later. Notably, one of the main planks of challenge to the constitutionality of the Aadhaar Act is its creation of an architecture for mass surveillance, and the Supreme Court's judgment on this is awaited.

The Indian surveillance framework suffers from two limitations – the first relates to the broad mandate given to the law enforcement agencies ('LEAs'), the lack of judicial/independent oversight, and the absence of narrow tailoring (for e.g., CMS and NETRA).[36] The second issue relates to state capacity. The decision to place individuals under surveillance is highly discretionary in terms of the number of surveillance requests made.[37] This makes it difficult to adequately store, analyse, and use the data in a manner that safeguards civil liberties. In fact, even a White House-commissioned Report cautioned against using algorithmic systems such as predictive policing software, given its subjectivity and possibility of increasing profiling and discrimination.[38] In Section IV, we demonstrate how, despite the Report's acknowledgement of these concerns with the current surveillance architecture, the Bill does not go far enough in constraining State action in surveillance.

We have, paraphrasing the words of U.K. Information Commissioner Richard Thomas, effectively sleepwalked into a surveillance society.[39] However, it is not just the actual or potential *use* of surveillance tools that is worrying. Instead, it is the *existence* of concentrated and centralised State power that creates a chilling effect[40] and leads to a 'psychological restraint' on the ability to think and act

---

PrintRelease.aspx?relid= 54679 and PTI, *Govt. to launch internet spy system 'Netra' soon*, The Times of India (Jan. 6, 2014), https://timesofindia.indiatimes.com/india/govt-to-launch-internet-spy-system-netra-soon/articleshow/28456245.cms.

35 Vrinda Bhandari, Smriti Parsheera, and Faiza Rehman, *India's communication surveillance through the Puttaswamy lens*, The Leap Blog, (May 18, 2018), https://blog.theleapjournal.org/2018/05/indias-communication-surveillance.html. See also Bhandari et al, *supra* note 24.

36 *See* Gautam Bhatia, *State Surveillance and the Right to Privacy in India: A Constitutional Biography*, 26 Natl L. School of India Rev, 128 (2014); Chaitanya Ramachandran, *PUCL v. Union of India Revisited: Why India's Surveillance Law Must Be Revised for the Digital Ag*e, 7 NUJS L. Rev. 105 (2014).

37 RTI inquiries reveal that, on average, the Central government taps more than 1 lakh phone calls a year, while issuing around 7500-9000 phone interception orders monthly. The number of requests from various State governments is expected to be even higher, leading the report conclude that "*Indian citizens are routinely and discreetly subjected to Government surveillance on a truly staggering scale*". *See* Software Freedom Law Centre, *India's Surveillance State: Other provisions of law that enable collection of user information* (2015), https://sflc.in/indias-surveillance-state-other-provisions-of-law-that-enable-collection-of-user-information.

38 Cecilia Munoz, Megan Smith and D.J. Patil, *Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights*, Executive Office of the President, White House (2016), at 21-22.

39 Jenny Booth, *UK 'sleepwalking into Stasi state'*, The Guardian (Aug. 16, 2004), https://www.theguardian.com/uk/2004/aug/16/britishidentity.freedomofinformation.

40 Neil M. Richards, *The Dangers of Surveillance*, 126 Harv. L. Rev. 1934, 1949-50, 1964 (2013); Zachary Smith, *Privacy and Security Post Snowden: Surveillance Law and Policy in the United States and India,* 9 Intercultural Human Rts. L. Rev. 137, 155 (2014); *Whitney* v. *California*, 1927 SCC OnLine US SC 126 : 71 L Ed 1095 : 274 US 357 (1927).

freely, as recognised by Justice Subba Rao in his dissent in *Kharak Singh*,[41] that is a cause for concern.

B. Privacy from non-State actors

As explained earlier, traditional debates around privacy (and surveillance) – of the body, home, correspondence – centred around instrumentalities of the State. Private actors were not really the focus of the debate. Nevertheless, the distinction between State and non-State actors has increasingly blurred with the rise of big data analytics, especially since the business models of technology giants such as Facebook,[42] Google, and Amazon is premised on the collection, storage, and use of customer data in an opaque manner, while being powered by network effects. A recent study found that an individual's Facebook 'likes' could be used to predict with reasonable accuracy their ethnicity, religious and political leanings, sexual orientation, personality traits, intelligence, and even substance use.[43] This form of data harvesting has given rise to the age of 'surveillance capitalism',[44] leading to debates[45] about the relevance of the traditional notice and consent contractual frameworks that defined these relationships.

The emergence of data as the new currency has resulted in the creation of an entire industry around the buying and selling of personal information to third parties. This industry now exists to commoditize the conclusions drawn from that data.[46] Private actors also have a deep interest in our lives, in terms of tracking, learning, and possibly sharing information about what we read and write, our actions and location, and ultimately, what we think. This is not dis-similar to the State. Two examples bear out this blurring distinction. *First*, the Cambridge Analytics scandal, which demonstrates that data, especially about voter preferences, profiles, and habits, is the key to manipulation and persuasion in electoral

---

[41] *Kharak Singh* v. *State of U.P.*, AIR 1963 SC 1295. Justice Subba Rao construed State "*coercion"* as including physical and psychological restraints, which can be directly or indirectly brought about by calculated measures. Notably, Justice Nariman, in *Puttaswamy*, paras 446, 452 termed this as one of the three great dissents since independence and the Supreme Court unanimously overruled the portion of the majority judgment in *Kharak Singh* that held that privacy is not a fundamental right.

[42] *See* Brian Chen, *I downloaded the information that Facebook has on me. Yikes*, The New York Times (Apr. 11 2018), https://www.nytimes.com/2018/04/11/technology/personaltech/i-downloaded-the-information-that-facebook-has-on-me-yikes.html.

[43] Michal Kosinski, David Stillwell, and Thore Graepel, *Private Traits and Attributes are Predictable from Digital Records of Human Behavior*, 110 (15) PROC. OF THE NAT. ACAD. OF SCIENCES 5802 (2013).

[44] Shoshana Zuboff, *Big Other: Surveillance Capitalism and the Prospects of an Information Civilization*, 30 J. OF INFO. TECH. 75 (2015).

[45] Rahul Matthan, *Beyond Consent: A New Paradigm for Data Protection*, Takshashila Institution: Discussion Document (July 2017), http://takshashila.org.in/wp-content/uploads/2017/07/TDD-Beyond-Consent-Data-Protection-RM-2017-03.pdf.

[46] Podesta et al, *supra* note 3, at 50.

politics. It represents a new practice of profiling by politicians and data mining firms to influence elections.[47]

Second, the Request for Proposal issued by the India government in April 2018, to select an agency to operate a 'Social Media Communications Hub'[48] illustrates the State's co-option of private actors to create a 'social media monitoring tool' that can help "*facilitate creating a 360 degree view of the people who are creating buzz across various topics*"; conduct 'predictive analytics' and sentiment analysis; and store metadata information in 'big data database'. After the Court's observations during a hearing challenging this Request for Proposal, it was withdrawn.[49]

Unsurprisingly, despite increasing awareness about privacy and demand for simplified terms of service, firms have not changed their behaviour. Instead, as Hetcher notes, private actors have focused on "*simulat[ing] privacy respect rather than providing the real thing*."[50] In fact, Facebook's profits rose by 63% between January-March 2018, despite the Cambridge Analytica scandal.[51]

Additionally, national security considerations that were once limited to the State, now govern the actions and assistance by private actors in limiting privacy. The Chinese social credit system is such an example of private sector enterprise feeding into government surveillance.[52] In India as well, the government is increasingly relying on private intermediaries to help conduct surveillance, whether it is incorporating encryption restrictions into telecom licenses[53] or requiring intermediaries to 'extend all facilities and technical assistance' to LEAs under Section 69(3), IT Act for monitoring, interception or decryption. According

---

47 Adrian Chen, *Cambridge Analytica and our Lives Inside the Surveillance Machine*, The New Yorker (Mar. 21 2018), https://www.newyorker.com/tech/elements/cambridge-analytica-and-our-lives-inside-the-surveillance-machine; *As Congress, BJP Trade Blows Over Cambridge Analytica, Facts Go Out the Window*, The Wire (Mar. 22 2018), https://thewire.in/politics/congress-bjp-cambridge-analytica-controversy-facts.

48 Broadcast Engineering Consultant India Ltd., *RFP invited for Selection of Agency for SITC of Software and Service and Support for function, operation and maintenance of Social Media Communication Hub, Ministry of Information and Broadcasting, Government of India*, BECIL/Social Media/MIB/02/2018-19 (Apr. 25, 2018).

49 Centre withdrawing notification on social media hub, AG informs Supreme Court, Hindu Business Line (Aug. 3, 2018), https://www.thehindubusinessline.com/info-tech/social-media/centre-withdrawing-notification-on-social-media-hub-ag-informs-supreme-court/article24590834.ece.

50 Steven Hetcher, *Changing the Social Meaning of Privacy in Cyberspace*, 15(1) HARV. J. OF L. AND TECH. 149, 151 (2001).

51 Ben Chapman, *Facebook profits soar 63% to $5bn despite Cambridge Analytica data privacy scandal*, The Independent (Apr. 26, 2018), https://www.independent.co.uk/news/business/news/facebook-profits-latest-q1-rise-cambridge-analytica-data-scandal-mark-zuckerberg-a8323331.html.

52 Chan, *supra* note 32.

53 Part 1, Clause 2.2(vii) of the Internet Service Provider (ISP) License Agreement requires ISPs to obtain prior governmental approval to deploy encryption, which is higher than 40 bits. More importantly, Clause 37.1 of the Unified License Agreement, Clause 39.1 of the UASL and Part 1, Clause 2.2(vii) of the ISP license agreement all prohibit bulk encryption by TSPs.

to Google Transparency and other reports, requests by Indian LEAs for user data have been steadily rising over the years.[54] It is thus clear, that the distinction between the privacy concerns and expectations from the State and private actors is blurring. The Bill acknowledges this, and places additional constraints on the private sector; but it does not go far enough in checking exercise of State power.

C. Why the "I have nothing to hide" argument is misconceived

A common rebuttal to any privacy-based argument is that only people with something to hide or who have done something wrong are concerned about the loss of privacy, since only they fear harm from the public disclosure of their personal information. This is an argument that gets used as justification for privacy intrusions or surveillance by the State.

However, as we have argued elsewhere,[55] some harm is caused to us when our privacy is breached. Privacy is shorthand for 'breathing space'[56] that encourages self-expression and gives us the freedom to do and be as we like, without the fear of public judgment. It explains why we draw curtains at our homes, or why we share personal information selectively. The "nothing to hide" argument, by equating privacy with secrecy, makes an incorrect moral judgment about the kinds of information people want to hide.

Privacy and secrecy are distinct concepts. Privacy is about autonomy and the choice to control the access to information about our private lives. Conversely, secrecy is about withholding information that people may have a right to know. Or in the words of Jill Lepore, "*Secrecy is what is known, but not to everyone. Privacy is what allows us to keep what we know to ourselves.*"[57]

The "nothing-to-hide" paradigm evaluates any breach of privacy only from the perspective of disclosure of possibly illegal/immoral information and thus over-emphasises the *instrumental* value of privacy. In doing so, it ignores the

---

[54] The government made 4,508 requests to Google between July-December 2017 for information 8,589 accounts (up from 3,843 requests for 6,343 accounts for January-June 2017). See Google Transparency Report, *Requests for User Information: India* (2018), https://transparencyreport.google.com/user-data/overview?user_requests_report_period=authority:IN. There has also been a similar spike in requests by the Indian government from Facebook and Twitter. See Yuthika Bhargava, *India Tops Facebook's List of Content Restriction Requests*, The Hindu (Nov. 13 2015), https://www.thehindu.com/news/national/india-tops-facebooks-list-for-content-restriction-requests/article7870072.ece.

[55] Vrinda Bhandari and Renuka Sane, *Privacy and the 'nothing to hide' argument*, Livemint (Aug. 9 2017), https://www.livemint.com/Opinion/kA7bY2M5gtpIkjtJgDAyxK/Privacy-and-the-nothing-to-hide-argument.html. See also Daniel Solove, *'I've Got Nothing to Hide' and Other Misunderstandings of Privacy*, 44 SAN DIEGO L. REV. 745 (2007) for a more detailed treatment of the issue.

[56] Julie Cohen, *What Privacy Is For*, 126 HARV. L. REV 1904, at 1918 (2012).

[57] Jill Lepore, *The Prism: Privacy in the Age of Publicity*, The New Yorker (June 24, 2013), https://www.newyorker.com/magazine/2013/06/24/the-prism.

intrinsic value of privacy, its expression as of the core value of security[58] and harms caused by the disclosure of personal information that are linked to intrusion, the loss of autonomy, and the unwanted social intrusion.[59] In fact, social intrusion is a particular concern in conservative and gender-imbalanced societies such as India, where equating privacy with secrecy would only serve to stigmatize the status of vulnerable sections of society.[60]

D. Need for a privacy law

There is a need to enact a comprehensive legislation covering the actions of both the State and private actors. Currently, the regulation of State surveillance is the subject of a patchwork of laws and executive actions.[61] However, given the power imbalance between the citizen and the State, the only effective mechanism to constrain State action is a holistic law that limits what the State can do; narrowly defines the circumstances in which it may interfere with fundamental rights; regulates the LEAs, particularly intelligence agencies; provides for control and oversight mechanisms; and empowers the citizen to hold it to account, when it exceeds the bounds of the law.

The situation is not different for private actors. The traditional response to privacy concerns in the private sector would have been the market, where competition between data controllers would have led to improved privacy protections. However, this has not happened for two reasons. *First*, because of information asymmetry between the individual consumer and the firm/data collector, which is widening in our increasingly networked and digitised world, customers do not know what kind of data is collected about them or what it is used for. The fact

---

[58] For more details on the debate surrounding the instrumental and intrinsic value of privacy see, James Rachels, *Why Privacy is Important*, 4(4) PHIL. AND PUB. AFFAIRS 323 (1975); Deborah Johnson, Computer Ethics (2nd Edn., 1994); James Moor, *Towards a Theory of Privacy in the Information Age*, Computers and Society 27, 28-29 (1997).

[59] Daniel Solove's taxonomy of privacy involves (a) information collection; (b) information processing; (c) information dissemination through breach of confidentiality, disclosure, exposure, increased accessibility, blackmail, appropriation, distortion and (d) invasion, through intrusion and decisional interference. Intrusions are "*invasions or incursions into one's life. It disturbs the victim's daily activities, alters her routines, destroys her solitude, and often makes her feel uncomfortable and uneasy. Protection against intrusion involves protecting the individual from unwanted social invasions, affording people what Warren and Brandeis called "the right to be let alone*." See Daniel J. Solove, *A Taxonomy of Privacy*, 154(3) UNIV OF PENN. L. REV. 477, at 490-491, 533 (2006). In this paradigm, the "nothing to hide" argument would focus primarily on the consequences of disclosure, exposure, blackmail. However, this would ignore the harms caused by privacy violations that are in the nature of breach of confidentiality, increased accessibility, appropriation, intrusion and decisional interference.

[60] The discrimination against individuals on the basis of their caste, religion, sexual orientation, and even medical status such as HIV AIDS and the consequent fear of social ostracism may cause individuals to exercise control ("hide") in the manner in which they disclose such information about themselves to third parties. This is an exercise of their right to privacy, and should not be equated with illegality.

[61] *Supra* note 33.

that data, almost inevitably involves secondary use for purposes not originally envisioned and involves multiple participants (for collection, storage, aggregation, analytics, and sale), increases the asymmetry.

Another contributor to the rising asymmetry is that web-platforms can covertly or overtly change their privacy policies after consumers have signed up. The network effects enjoyed by the users makes it difficult to opt out of these platforms/apps, even if they are unhappy about the policy changes. We have seen this in the WhatsApp-Facebook example, where after acquisition by Facebook, WhatsApp changed its privacy policies, expanding the information-sharing rules, causing outrage and even, legal troubles for it.[62]

These examples demonstrate the market failure in creating time-consistent conditions to enable consumers to make privacy decisions under perfect information and understanding. The complexity of requiring consumers to consider multiple outcomes and associated probabilities leads them to "*highly imprecise estimates of the likelihood and consequences of adverse events, and altogether ignore privacy threats and modes of protection.*"[63]

Second, is the problem of bounded rationality. Under rational choice theory, individuals make time consistent decisions, using all available information to maximise their utility over time. However, studies have shown that the actual decisions taken by individuals, when faced with choices concerning disclosure of their personal data, do not follow such patterns. This is partly due to the inability to read and comprehend the fine print of privacy policies and partly due to bounded rationality, causing a failure to process how personal information is being traded further in secondary markets.[64]

On many occasions, by merely allowing individuals control over information dissemination, irrespective of their actual control, firms encourage data subjects to reveal more personal information. This is 'control paradox'.[65] For instance, simply on seeing the phrase 'privacy policy', without reading the actual policy,

---

[62] WhatsApp has been asked to stop sharing its user data with Facebook by regulators in France and Germany, whereas in the U.K., Facebook agreed to stop collecting WhatsApp user data. The EU even fined Facebook for providing misleading information with respect to its acquisition. See Shannon Liao, *WhatsApp ordered to stop sharing user data with Facebook*, The Verge (Dec. 18, 2017), https://www.theverge.com/2017/12/18/16792448/whatsapp-facebook-data-sharing-no-user-consent.

[63] Alessandro Acquisti, and Jens Grossklags, *What Can Behavioral Economics Teach Us About Privacy*, in Digital Privacy: Theory, Technologies and Practices 363, 365 (Taylor & Francis Group, 2007).

[64] Nathan Newman, *Search, Antitrust and the Economics of the Control of User Data*, 31(2) YALE J. OF REG. 401 (2014). See also Acquisiti, *ibid*, at 364.

[65] Laura Brandimarte, Alessandro Acquisti, and George Loewenstein, *Misplaced Confidences: Privacy and the Control Paradox*, Ninth Annual Workshop on the Economics of Information Security (WEIS). Harvard University, 1-43 (2010).

users are more willing to believe that their data will be safe and not shared forward.[66]

Consequently, a privacy law that regulates the actions of private data controllers is necessary to counter this market failure. Another reason is that while State action can be challenged for violation of fundamental rights under writ jurisdiction, absent a specific law, it is much more difficult to seek relief against private entities.

IV. ANALYSING THE PERSONAL DATA PROTECTION BILL 2018 AND ITS TREATMENT OF THE STATE AND THE PRIVATE SECTOR

The Justice Srikrishna Committee submitted its Final Report, along with the draft law, to the Government in July 2018. Much has been written about various aspects of the Bill,[67] and considerations of space do not permit a comprehensive discussion on the Bill in its entirety. Instead, given our focus on the dissolving distinction between the State and private sector, we examine those aspects of the Bill that touch upon the public-private distinction. Specifically, we evaluate how it has fared in regulating the actions of the State and private sector, with a broad focus on consent, surveillance, and the power of one over the other.

The Bill is an important step forward towards giving meaning to the right to privacy and creating a robust data protection framework for India. It goes far beyond existing legislation in recognising the harms caused by the private sector, and consequently, in regulating their actions. In fact, the Report expressly recognises the potential for discrimination, exclusion, and harm that are likely in a digital economy and the limitations of the existing framework under the IT Act and the Sensitive Personal Data and Information Rules.[68] Surprisingly though, it seems to underestimate the harms caused by privacy intrusion by the State,

---

[66] Joseph Turow et al, *The Federal Trade Commission and Consumer Privacy in the Coming Decade*, 3(3) J. OF L. & POLICY FOR THE INFORMATION SOC. 723, 724, 729 (2007).

[67] *See* for instance, Amber Sinha, Draft privacy bill and its loopholes, Livemint (July 28, 2018), https://www.livemint.com/Opinion/zY8NPWoWWZw8AfI5JQhjmL/Draft-privacy-bill-and-its-loopholes.html; Sunil Abraham, *Spreading unhappiness equally around*, Business Standard (July 31, 2018), https://www.business-standard.com/article/opinion/spreading-unhappiness-equally-around-118073100008_1.html; Vrinda Bhandari and Renuka Sane, *Data privacy: Too many hats for UIDAI*, The Economic Times (July 30, 2018), https://blogs.economictimes.indiatimes.com/et-commentary/data-privacy-too-many-hats-for-uidai/; *The Good, Bad and Ugly on India's Template for How Your Data Will be Protected*, The Wire (July 29, 2018), https://thewire.in/tech/india-template-data-protection-draft-bill; Arghya Sengupta, *A free & fair digital economy: Draft data protection bill asserts our sovereignty and safeguards citizens' interests*, The Times of India (July 30, 2018), https://blogs.timesofindia.indiatimes.com/toi-edit-page/a-free-fair-digital-economy-draft-data-protection-bill-asserts-our-sovereignty-and-safeguards-citizens-interests/.

[68] Report, *supra* note 8, at 5-7.

inasmuch as it gives wide leeway to the government in certain situations to override the lack of consent of the individual (or 'data principal', as defined in the Bill).

Chapter II on 'Data Protection Obligations' requires both the State and private entities (as data fiduciaries)[69] to follow principles of fair, lawful and reasonable processing; collection and purpose limitation; data storage limitation; proper notice; and accountability. Chapters III and IV on Grounds for Processing of Personal Data and Sensitive Personal Data establish the importance of consent and 'explicit' consent respectively, although they create certain exemptions for both State and private entities. Processing has been defined very widely in the Bill to include collection, recording, storage, use, disclosure, dissemination, erasure etc. of personal data.

The rights of the data principal have been enumerated for the first time in Chapter VI, and include the right to confirmation and access; the right to correction; the right to data portability (although not when the processing is necessary for functions of the State under Section 13); and the right to be forgotten. The Bill also enshrines transparency and accountability principles (such as privacy by design), and security safeguards in Chapter VII, and creates a Data Protection Authority ('DPA') in Chapter X.

These principles take the welcome first step in putting constraints on the State and the private sector and in safeguarding individuals' rights, but as we shall demonstrate, do not go far enough, especially in recognising and limiting State power.

A. Consent

Although Section 12 of the Bill highlights the need for free, informed, specific, and clear consent as the basis for processing (i.e. collecting, sharing, using, disclosing, storing) personal data, Sections 13-17 create exceptions to this principle. The primary exception for private entities is Section 16, which allows employers to process personal data of their employees, if it is necessary for their recruitment or termination; for the provision of service or benefit sought by them; for verifying the attendance of the data principal; or for any other activity relating to their performance assessment. As long as consent in such situations is "not appropriate" or would "involve a disproportionate effort on the part of the data fiduciary" (exceptions in Section 16(2)), the consent of the data principal/employee becomes irrelevant.

[69] As per Section 3(13) of the Bill, both the State and any company, juristic entity, or individual are "data fiduciaries" when they determine the purpose and means of processing of personal data. Data fiduciary is similar to a "data controller" as defined in the EU GDPR.

In the case of the State, the exception is couched in even wider terms. Section 13(1) allows processing of personal data without the consent of the data principal as long as such processing is "necessary for any function of Parliament or State Legislature". Section 13(2) goes further in authorising non-consensual processing if it is necessary, *inter alia,* "for the exercise of *any* function of the State authorised by law for the provision of *any* service or benefit by the State, even though the terms "service" or "benefit" have not been defined in the Bill.

For sensitive personal data, the only additional safeguard in Section 19, which similarly authorises non-consensual processing of such data for certain functions of the State, is that such processing is "strictly necessary". The ambiguity of this phrase raises questions about how it will be interpreted and whether it can serve as an actual constraint on State power. For example, if we were to consider the case of Aadhaar, the government can reasonably argue that the processing of biometric information of the residents, *without their consent*, is "strictly necessary" for the delivery of welfare benefits and targeting of services.

The text of the Bill is all the more surprising given the Committee's recognition of the 'imbalance of power' that is present during citizen-State interactions, which affects the validity of the consent given; and the fact that data protection law, to be 'meaningful', should apply to the State.[70] The Report does not adequately explain why, instead of strengthening consent or providing additional safeguards in such cases, Sections 13 and 19 give an almost complete exemption when the State is processing personal data/sensitive personal data.[71] It argues that the State may need access to various data sets for performing certain functions – such as preparing suitable employment plans – and thus, collective interest should not be made to suffer at the hands of consent.[72] Nevertheless, it is unclear why such State functions cannot be fulfilled using anonymised data, whose processing is excluded under Section 2(3) from the ambit of the Bill.

The Bill's re-formulation of consent is notable for its recognition of the cognitive problems associated with the traditional notice and consent framework, and for highlighting the primacy of individual autonomy.[73] However, the breadth of these exceptions serves to undermine, and essentially negate these steps forward, especially when it comes to data processing by the State.

---

[70] Report, *supra* note 8, at 108.

[71] *See* also Amba Kak, *The Srikrishna Committee's Data-Protection Bill Does Not Do Enough To Hold The Government Accountable For Use Of Personal Data*, The Caravan (July 28, 2018), http://www.caravanmagazine.in/governance/government-policy/srikrishna-committee-data-protection-government-accountable; Madhav Khosla and Ananth Padmanabhan, *Draft data protection Bill pays little attention to the dangers of State power*, The Print (July 30, 2018), https://theprint.in/opinion/draft-data-protection-bill-pays-little-attention-to-the-dangers-of-state-power/90511/.

[72] Report, *supra* note 8, at 108-109.

[73] Report, *supra* note 8, at 32.

B. Surveillance

Apart from providing for non-consensual grounds for processing data, the Bill also lays out various exemptions, when data processing is exempt from nearly all the obligations and safeguards under the Bill – specifically those enshrined in Chapter II (except Section 4), Chapters III-VI, Chapter VII (except Section 31), and Chapter VIII.[74]

The most significant of these exemptions, in Section 42, clarifies that processing of personal data "in the interests of the security of the State" shall be exempt from the aforesaid obligations of the Bill as long as it is authorised by law; in accordance with the procedure established by law, made by Parliament; and is necessary for, and proportionate to, such interests being achieved. These three tests seem to be in line with the Supreme Court's formulation in *Puttaswamy*,[75] and are a welcome step forward.

Notably, the Report itself recognises that "*national security is a nebulous term, used in statutes of several jurisdictions to denote intelligence gathering activities that systematically access and use large volumes of personal data*" and that the "*key question is what safeguards can be instituted to ensure that the use of this ground is restricted to genuine cases of threats to national security.*"[76] Thus, the question arises, are the safeguards enshrined in Section 42 enough?

The requirement of authorisation by law calls into question, the continued validity of the government's controversial CMS and NETRA surveillance programs, since they have been introduced by executive action.[77] Further, the necessity and proportionality standard seem to close the door for any mass surveillance program, since the State will be hard pressed to justify that mass surveillance is a proportionate response to a security threat.[78]

The Bill also represents a missed opportunity for key surveillance reform, that are likely to eventually render the safeguards in Section 42 inadequate. *First*, it

---

[74] Chapter II deals with Data Protection Obligations; Chapters III and IV are on Grounds for Processing Personal Data and Sensitive Personal Data respectively; Chapter V is on Personal and Sensitive Personal Data of Children; Chapter VI is on Data Principal Rights; Chapter VII is on Transparency and Accountability Measures; and Chapter VIII is on Transfer of Personal Data Outside India. Section 4 deals with fair and lawful processing and Section 31 with security safeguards.

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

[76] Report, supra note 8, at 122.

[77] Press Information Bureau, *Centralised System to Monitor Communication* (Nov. 26, 2009), http://pib.nic.in/newsite/PrintRelease.aspx?relid= 54679; *Government to launch 'NETRA' for internet surveillance*, The Economic Times (Dec. 16, 2013), https://economictimes.indiatimes.com/tech/internet/government-to-launch-netra-for-internet-surveillance/articleshow/27438893.cms.

[78] *See* also, Vrinda Bhandari, *Data Protection Bill: Missed Opportunity for Surveillance Reform*, The Quint (July 28, 2018), https://www.thequint.com/voices/opinion/personal-data-protection-bill-2018-draft-srikrishna-committee-loopholes-surveillance.

does not propose any amendments to the surveillance architecture present in the Telegraph Act or the IT Act. Thus, there is no judicial oversight (like in other countries such as Canada, Austria, or the U.S.);[79] or *ex ante* judicial determination of whether a proposed surveillance measure complies with Section 42's conditions of authorisation by law, in accordance with procedure established by law, and necessity and proportionality. This assumes importance since in most cases, individuals will be unaware of any surveillance activity on them,[80] and hence, the likelihood of *post-facto* challenging the invocation of the "security of State" exemption or non-compliance with Section 42 is minimal.

Second, the Bill does not prescribe any parliamentary, regulatory, or executive oversight. Pursuant to Section 42, the State is exempt from complying with all transparency and accountability measures enshrined in the Bill, including oversight by the DPA. Thus, it has no obligation to disclose, even in an anonymised form, the number of surveillance operations undertaken; the kind of personal and sensitive personal data collected; the duration for which such data is stored, and the procedure followed for destruction of data – information that is necessary to ascertain the proportionality of surveillance measures.

Third, the Bill is silent on the aspect of illegally obtained evidence. It is now well settled in Indian law that illegally obtained evidence is admissible in court, as long as the State can demonstrate its relevance and genuineness.[81] This is partly based on the fact that Indian law does not specifically prohibit admitting otherwise relevant evidence, on the ground that it was improperly or illegally obtained. Thus, Section 42's safeguard requiring the processing of personal data to be "in accordance with procedure established by such law, made by Parliament," is of no avail. Without a specific statutory exclusion, there is little incentives for LEAs to abide by the rules.

Finally, Section 42 exempts the State from complying with purpose/collection/data storage limitation; which means that surveillance data collected for one purpose can be stored for as long as necessary, as long as it is necessary and proportionate.

Apart from this, the State is also exempt from data processing obligations "*in the interests of prevention, detection, investigation and prosecution of any offence or any other contravention of law*" under Section 43, as long as it

---

[79] For more details, see Vrinda Bhandari et al, *Use of personal data by intelligence and law enforcement agencies*, *NIPFP Working Paper*, 22, http://macrofinance.nipfp.org.in/PDF/BBPR2018-Use-of-personal-data.pdf.

[80] The State is exempted from complying with any notice requirements under Section 8, and the data principal has no rights of confirmation and access of the data kept about her under Section 24, once the exemption under Section 42 is invoked.

[81] *See R.M. Malkani* v. *State of Maharashtra*, (1973) 1 SCC 471; *Pooran Mal* v. *Director of Inspection (Investigation)*, (1974) 1 SCC 345; *State (NCT of Delhi)* v. *Navjot Sandhu*, (2005) 11 SCC 600; and *Umesh Kumar* v. *State of A.P.*, (2013) 10 SCC 591.

is authorised by law and is necessary and proportionate. Interestingly, unlike Section 42, there is no requirement for such processing to be in accordance with the procedure established by law; which seems to further widen the scope and breadth of the exemptions given to the State.

In respect of private actors, although the Bill is silent on the issue, the requirement of authorisation by law in Section 42 and 43 coupled with the obligations in Chapter II of the Bill would seem to suggest that private commercial surveillance is illegal, beyond what is already permitted under the IT Act and Rules. However, private individuals would be able to avail Section 46's exemption for "personal or domestic purposes", which would cover CCTV cameras at home.

Interestingly,[82] the Report acknowledges the need for judicial and parliamentary oversight and the adoption of systematic risk management techniques, but the text of the Bill does not reflect this forward approach. This seems to be due to the Committee's view that such recommendations are not in line with its mandate of studying issues relating to data protection and suggesting a draft data protection statute.[83] However, it is worth noting that the government's own Privacy Bill of 2011 and the private member Data (Privacy and Protection) Bill, 2017 introduced by Baijayant Panda, MP in the Lok Sabha contained separate chapters on the prohibition and regulation of surveillance, including private surveillance.[84] These could also have been included under the terms of reference of the Justice Srikrishna Committee on data protection, but now represent a missed opportunity.

C. Interaction between the State and non-State actors

We have argued that the distinction between the impact of the State and private actors on our lives and personal data is blurring. This is best demonstrated by the increasing reliance placed by the State on the private sector in carrying out functions, whether in the aid of surveillance or in implementing the mandate of Aadhaar.

The White Paper expressly recognises that intelligence gathering for national security purposes is premised on "systematic government access", which, in turn is understood as "*direct access by the government to large volumes of personal data held by private sector entities.*"[85] The danger therefore, is not just commercial surveillance per se, but the increased reliance by the State on access to per-

[82] Report, *supra* note 8, at 128.

[83] Report, *supra* note 8, at 128.

[84] A copy of the Privacy Bill of 2011 is available at https://bourgeoisinspirations.files.wordpress.com/2010/03/draft_right-to-privacy.pdf and a copy of Jay Panda's Private Member Bill, as introduced in the Lok Sabha is available at http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/889LS%20AS.pdf.

[85] Report, *supra* note 8, at 122.

sonal data that is collected, stored, and processed by private actors. As explained above, private entities are already obliged to assist the State in monitoring, collecting, decrypting traffic data under Sections 69 and 69B of the IT Act, and through the provisions in telecom licenses.[86]

Despite acknowledging the dangers, and abuse, of the use of private sector data for State purpose, the Bill only increases this public-private interaction. Section 40 of the Bill on data localisation – one of the most controversial[87] provisions – requires data fiduciaries to ensure storage of at least one serving copy of personal data on a server or data centre in India. It is primarily justified on the basis of benefits to law enforcement (apart from other benefits relating to the prevention of foreign surveillance and building an AI ecosystem)[88] although it raises serious concerns about large-scale surveillance[89] (apart from the economic impact on firms).

These fears are compounded by the fact that the Bill seems to be silent on an Apple-FBI type of situation, where the government or LEAs require/request a private entity to hand over certain data. The current legal framework obligates private entities in various situations[90] to provide the State with documents or other information or decrypt information, when called upon to do so. Section 31 of the Bill requires data fiduciaries to implement appropriate safeguards including de-identification and encryption, but it does not envisage, or deal with, requests of decryption or rendering assistance. In the absence of clarity, and given the political realities of the country, it is likely that the legal framework remains unchanged and governments will be able to (mis)use the data localisation provision to conduct surveillance on their citizens.

---

86 For more information see Bhandari et al, *supra* note 79, at 6-8, 12-13.

87 Kritika Bharadwaj, *Data localisation must go, it damages the global Internet*, The Hindustan Times (Aug. 3, 2018), https://www.hindustantimes.com/analysis/data-localisation-must-go-it-damages-the-global-internet/story-Aah1052ExFq6Ylcb9BQ4jJ.html; Aditya Kalra and Aditi Shah, *Exclusive: U.S. tech giants plan to fight India's data localisation plan*, The Reuters (Aug. 20, 2018), https://in.reuters.com/article/india-data-localisation/exclusive-u-s-tech-giants-plan-to-fight-indias-data-localisation-plans-idINKCN1L506U.

88 Report, *supra* note 8, at 88-93.

89 Part of the surveillance concern stems from the ease with which the government would be able to access vast swathes of personal data, which would now be located within the territory of India, using domestic laws such as the IT Act. The fear is compounded by the fact that intelligence agencies function with relatively minimal oversight. *See*, Vinay Kesari, Data localization and the danger of a 'splinternet', FactorDaily (July 26, 2018), https://factordaily.com/data-localisation-and-the-danger-of-splinternet/. *See* also, *supra* note 87.

90 *See* Section 91 of the Code of Criminal Procedure; Section 69 of IT Act; Rule 6(1) of the SPDI Rules; Rule 3(7) of the Information Technology (Intermediaries Guidelines) Rules, 2011; Rule 7 of the IT (Guidelines for Cyber Cafe) Rules, 2011 on the obligations imposed on private entities.

V. MOVING FROM LAW TO IMPLEMENTATION

The protections outlined by the draft Bill, will likely give us the base of an expansive and strong right-protecting law – at least when it comes to the private sector. However, we have to bear in mind that in an environment where state capacity is weak, the effectiveness of such a law may remain limited.

India has several laws - ranging from the right to food, prohibition of dowry, to environmental safety. Yet, lived experience suggests that the enactment of a law by itself does not guarantee its implementation, or certainly its effective implementation.[91] For instance, state capacity has failed even at relatively simple tasks such as the implementation of loan waiver schemes.[92]

The challenge is greater when implementing the law against the State, and will depend, in large part, on the regulatory capacity of the DPA tasked with implementing the law. Section 49 of the Bill provides for the establishment of a DPA. Section 60(1) outlines the duty of the DPA, "*to protect the interest of the data principals, prevent any misuse of personal data, ensure compliance with the provisions of the Act, and promote awareness of data protection*."

The DPA will at the very least require two capabilities. *First*, is the ability to write regulations. The law outlines several principles that indicate the protections offered to data principals, and also outlines where exceptions may be given to State (or other) agencies. These principles will need to be translated into detailed regulations that serve as guidance for the various stakeholders in the ecosystem. *Second*, is the ability to enforce regulations. This includes executive process such as *ex-ante* mechanisms of monitoring and inspections to check compliance, and *ex-post* measures such as conducting investigations and determining penalties. We turn to analysing the challenges in each.

A. Regulation making

Once the law is enacted, it is up to the Regulator to adopt and enforce the law, through regulations. The process of regulation making involves filling the gaps in the law by writing subordinate legislation, which also have the force of the law. This helps, both the regulatory agencies to fulfil the mission of the particular Act,

---

[91] *See* for instance, the functioning of the Cyber Appellate Tribunal. Section 48 of the IT Act provides for the establishment of multiple Tribunals for hearing appeals against the orders of the Adjudicating Officer. However, only one Cyber Appellate Tribunal had been set up in Delhi and even that has been defunct since 2011, when the previous Chairperson retired. Harsimran Julka, *Cyber Appellate Tribunal in search of a chairperson judge*, The Economic Times (Apr. 20, 2012), economictimes.indiatimes.com/articleshow/12740179.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst. In fact, the last decided case seems to be of 30th June 2011.

[92] Renuka Sane and Amey Sapre, *Implementing loan waivers: Lessons from the 2008 All India Debt Waiver Scheme experience*, The Leap Blog (July 21, 2017), https://blog.theleapjournal.org/2017/07/implementing-loan-waivers-lessons-from.html.

and the regulated entities in understanding how to interpret the principles embedded in such an Act. Section 60(2) lists out the various functions of the DPA, indicating the areas for which regulations will need to be drafted, and the power to make regulations has been vested in the DPA by Section 108.

For instance, Section 17(1) of the Bill suggests that "*personal data may be processed if such processing is necessary for such reasonable purposes as may be specified*...." Regulations will have to specify what a "reasonable purpose" is, and how it varies with specific activities. Section 19(1), adverted to earlier, permits non-consensual processing of sensitive personal data if it is "strictly necessary" for any function of Parliament or any provision of service/benefits. The role of the DPA thus assumes great importance, since phrases such as "reasonable purpose" or "strictly necessary" afford great flexibility to the data fiduciary to engage in non-consensual processing. As another example, Section 10(4) stipulates that "*Where it is not necessary for personal data to be retained by the data fiduciary under sub-sections (1) and (2), then such personal data must be deleted in a manner as may be specified*". Once again, the DPA has the power, and the discretion, to specify the manner of deletion, and determine how rigorous it is.

The DPA has been tasked with monitoring and enforcing the application of the provisions of the Bill, and ensuring consistency in its implementation, in part through issuing "codes of practice". To achieve this, the regulator (DPA) should be able to clearly articulate its standards, and engage in continuous dialogue with the regulated entities (data fiduciaries), that is consultative with all stakeholders, and yet is not excessively influenced by the industry.

Regulation making should, at the very least, consist of two processes - first, a public consultation, where regulations are circulated for public comments, and feedback incorporated. The second element relates to demonstration of expertise, where the regulator is required to show how the proposed regulations will be beneficial for society through a cost-benefit analysis. This is important because action of the State represent coercion, and the State should be obligated to justify why such coercion should be permissible.[93]

Notably, while regulators in India often put out regulations in the public domain, their track record on addressing the various comments and providing a rationale for why a specific position was taken has been poor.[94] Many primary

---

[93] Shubho Roy, Ajay Shah, B.N. Srikrishna and Somasekhar Sundaresan, *Building state capacity for regulation in India*, in *Regulation in India: Design, Capacity, Performance* (Devesh Kapur and Madhav Khosla (Ed(s), Forthcoming, Oxford: Hart Publishing), http://macrofinance.nipfp.org.in/releases/RSSS_building-state-capacity.html.

[94] Anirudh Burman and Bhargavi Zaveri, *Regulatory Responsiveness in India: A Normative and Empirical Framework for Assessment*, IGIDR Working Paper Series, WP-2016-025 (2016), http://www.igidr.ac.in/pdf/publication/WP-2016-025.pdf. See also, Arjun Rajagopal and Renuka Sane, *Difficulties with PFRDA's Draft Aggregator Regulations*, The Leap Blog (July 2, 2014), https://blog.theleapjournal.org/2014/07/difficulties-with-pfrda-draft.html. See also Ashish Aggarwal and

laws such as the SEBI Act, TRAI Act, or the RBI Act do not specify any procedural requirements on how to respond to public consultations, or the need for explanatory memorandums for the final positions taken from the regulators. While Section 61(4) takes a welcome step forward in requiring the DPA to issue "codes of practice" only after a consultation process, it does not prescribe a similar process to be followed by the DPA when issuing regulations.

A cost-benefit analysis is difficult even, when there is relative clarity on the perceived costs and benefits of specific actions. Even then, many regulators in India find it difficult to conduct such analysis.[95] In the space of data protection, where the harms caused by the loss of privacy, and the costs and benefits of regulation are difficult to define, the possibility of writing poor and ineffective regulations is magnified. Poorly drafted laws or excessively detailed regulations often hurt the smaller players by increasing costs of compliance, paving the way for a concentrated market as only large and dominant players can muster enough resources to meet specific requirements of the regulator.

Given the powers and discretion of the DPA, the Bill does not go far enough in ensuring that the DPA will be better tasked than current regulators when exercising its regulation making powers, or that it will be able to make and enforce its decisions independently.

B. Enforcement

Enforcement typically consists of ex-post measures such as investigations, prosecution and adjudication. These activities club two functions - the executive and the judicial into one entity, which can lead to lack of independence between the two, often to the detriment of the regulated entity. Enforcement provisions can place enormous power in the hands of the State, and easily become tools of intimidation and harassment.

Regulatory capability on enforcement requires the adherence to the principles of rule of law, namely a substantial reduction in discretion in enforcement; a duty to explain the reason behind executive action;[96] followed by the right to appeal against any regulatory order. Substantial reduction in discretion is possible when the processes for carrying out the investigations and prosecution are defined, include judicial oversight for key decisions, and standards of evidence are clearly

Renuka Sane, *Draft IRDAI regulations on insurance commissions: Going back to the beginning*, The Leap Blog (Jan. 30, 2016), https://blog.theleapjournal.org/2016/01/draft-irdai-regulations-on-insurance.html; Chetna Batra, Gausia Shaikh and Bhargavi Zaveri, *A critique of RBI's proposal to regulate pre-paid payment instruments in India*, The Leap Blog (May 1, 2017), https://blog.theleapjournal.org/2017/05/a-critique-of-rbis-proposal-to-regulate.html.

[95] *No Research Before Cryptocurrency Ban by RBI, Reveals RTI*, News18 (June 13, 2018), https://www.news18.com/news/business/no-research-before-cryptocurrency-ban-by-rbi-reveals-rti-1777041.html.

[96] *Supra* note 93.

specified. The investigation team should be required to apply its mind before subjecting a regulated entity to its investigative processes, and a clear separation between the investigation and prosecution, and the adjudication teams is made. A hearing must precede the final order, and the order must be reasoned.

The Indian experience on these fronts is poor. For example, on several occasions the State has used a heavy-handed approach, using outright bans (as in the case of FSSAI's ban on Maggi or RBI's ban on crypto-currency) or disproportionate penalties, making state action counter-productive.[97] Several regulators have been inconsistent in passing orders for similar offences creating an environment of regulatory uncertainty where regulated entities find it difficult to evaluate if they are in violation at all, and the likely consequences of any violation.[98]

The current Bill is also likely to throw similar challenges in the field of data protection, as it does not have provisions that are likely to preclude behaviour similar to other regulators in India. For example, there is no provision requiring the DPA to provide reasoned orders. Sections 64-68 lay down the processes that the DPA would follow during an investigation, including the power to conduct a "search and seizure" (which is in the nature of police power); but they do not provide for adequate judicial oversight at various stages of this process. Nevertheless, unlike the Aadhaar Act, the Bill sets up an Appellate Tribunal for hearings appeal against orders of the DPA, which is a step in the right direction.

There are two potential challenges before the DPA in ensuring effective enforcement. The first relates to its independence. Independence is a complex issue, determined by appointment procedures, capacity, financial grants, fixed terms etc.; which will become clearer once the relevant regulations have been notified by the DPA. It will also depend on factors such as the approval given by the Central Government under Section 49(4) to the DPA to establish other offices in India; the speed with which appointments of Adjudication Officers are made; and whether, and how often, the Central Government uses its power under Section 98 to issue binding directions on the DPA on questions of policy.

The second, and related, challenge is likely to be the ability of the DPA to enforce actions against the State, which is dependent on its independence, capability, training, and capacity. There are associated challenges of State capacity as well that can relate, for instance, to the number of regional offices of the DPA that are established with government approval. Thus, care would have to be taken to prevent a situation like the establishment of a solitary Cyber Appellate

---

[97] Nehaa Chaudhari, *The RBI's virtual ban on crypto-currencies is illogical*, Medianama (Apr. 6, 2018), https://www.medianama.com/2018/04/223-rbi-cryptocurrency-ban/; Ajay Shah, *Hollowing out of India's financial markets: Banning trading abroad is not a choice*, The Leap Blog (Feb. 9, 2018), https://blog.theleapjournal.org/2018/02/hollowing-out-of-indias-financial.html.

[98] Ashish Aggarwal and Rhythm Behl, *Evaluating IRDA's orders*, The Leap Blog (Nov. 2, 2016), https://blog.theleapjournal.org/2016/11/evaluating-irdas-orders.html.

Tribunal in Delhi, which severely undermined its effectiveness as an appellate Tribunal.[99] Another illustration of this challenge would relate to the appointment of Adjudication Officers, who comprise the adjudication wing of the DPA and have the power to impose penalties and award compensation. Under section 68, the Central Government has complete power and discretion, to prescribe the number of Officers, their qualifications, terms of appointment, jurisdiction, and procedures for carrying out adjudication under the Act. Governmental interference, if any, in the appointment and functioning of such Adjudication Officers will only become clear once it notifies the relevant regulations in this regard, and will depend on how it implements the same.

Interestingly, Section 69 specifying penalties for the violation of various provisions of the Bill speaks of percentages of global turnover, which seems to only be applicable to private entities and not to the State as a data fiduciary.[100] Even otherwise, it is futile to penalise the State by imposing monetary penalties, since these are ultimately borne by the taxpayer, and may not serve as an adequate disincentive. The focus in regulating State action has to be on department inquiries and internal action, rather than by the DPA.

As the data protection debate evolves, it is important to remember that any action by a state agency is effectively coercing a private citizen/entities and constraining their set of actions. It bears mentioning that coercive action by the State may not always subserve the ultimate aim of law and regulations to protect consumers and data subjects, especially if it is unpredictable or arbitrary. It is, therefore, extremely important that any regulations are drafted with extreme thought and care, with public consultation, and especially in the case of new and untested technology, only when the State has determined that the benefits of regulation exceed its costs. This requires a framework for regulatory governance that places the constraints on the regulator itself.

VI. CONCLUSION

We begin this paper by outlining the different contours of privacy in the context of the historic *Puttaswamy* ruling, and conceptualising it in the contexts of the State and private sector. The advent of big data analytics and corporate surveillance has blurred the traditionally distinct concerns about the loss of privacy to State vis-à-vis to private actors. Insufficient privacy protections create a chilling effect, lead to a loss of breathing space, and enable greater profiling, and hence, discrimination, especially given the various intersections between gender, caste, and religion in India. Market failures only exacerbate this problem. That

[99] Julka, *supra* note 91.

[100] *See* also, Rahul Matthan, *The Achilles heel of the draft personal data Bill*, Livemint (July 31, 2018), https://www.livemint.com/Opinion/sgjyNwQ6yBTBsKz1LAYVuJ/The-Achilles-heel-of-the-draft-personal-data-Bill.html.

is why the nothing to hide argument, which equates privacy with secrecy, is specious.

The Government of India is likely – and hopefully – going to pass a law on data protection, and any such law will draw on the recommendations of the Justice Srikrishna Committee Report and draft Personal Data Protection Bill, 2018. We have argued that the Bill takes welcome steps in regulating private sector entities, but fails to adequately protect citizens (and data principals) from the actions of the State, particularly in the context of consent, surveillance, and the reliance by the State for the data stored by private entities. Given that the State should be a model data fiduciary, this is a cause for concern. We have then highlighted that going from drafting a law to its implementation is non-trivial due to state capacity constraints in India. Given the scale and enormity of the task[101] and its discretionary and "transaction-intensive" nature,[102] effective implementation of the law will require sophistication and a check on abuse of discretion.

We are at a historical moment, poised to enact a privacy law that will affect the lives of more than a billion people. Privacy reform, therefore, must be accompanied with improvements in state capacity, for it to have relevance.

---

[101] As pointed out by Suyash Rai, "*the monitoring and enforcement functions will require directly or indirectly monitoring numerous events in a larger number of data controllers and processors across a number of sectors, and taking decisions about them*." On limits of state capacity to be considered while drafting a data protection law in India, see, Suyash Rai, *A Pragmatic Approach to Data Protection*, The Leap Blog (Feb. 9, 2018), https://blog.theleapjournal.org/2018/02/a-pragmatic-approach-to-data-protection.html.

[102] Lant Pritchett and Michael Woolcock, *Solutions when the Solution is the Problem: Arraying the Disarray in Development*, Center for Global Development Working Paper No. 10 (Sept. 2002), https://www.cgdev.org/sites/default/files/ 2780_file_cgd_wp010.pdf. See also Suyash Rai, *Comments on the White Paper of the Committee of Experts on a Data Protection Framework for India* (2018), http://macrofinance.nipfp.org.in/PDF/data_protection_comments_suyash.pdf.