The Weight of Secrets: Assessing the Regulatory Burden for Informational Privacy in India

*Lalit Panda**

Abstract *Given the galloping pace at which information technology continues to develop and penetrate our lives, it is inevitable that the aspirations of data protection will sometimes appear like hollow promises that the law cannot keep. This makes it essential to study the precise regulatory conditions that can allow for the effective enforcement of legal protections for informational privacy. This Article provides a holistic account of the likely breadth and regulatory burden of an effective data protection regime and attempts to flesh out various regulatory tools that can go into the design of a Data Protection Authority for India so as to account for the weighty duties it must bear. Touching on the proposals of the Srikrishna Committee while drawing on the experiences of other jurisdictions, it justifies the idea of a unified, cross-sectoral data protection regulator with a broad mandate, examines the limits of sectoral regulation, and clarifies the significance of and outlook for models such as co-regulation and responsive regulation, as well as the role of the much-vaunted principle of accountability. In assessing the enforcement burdens created by the substantive rights and duties of data protection, the article also provides pointers as to what we should expect from a privacy watchdog in India and how these expectations can best be met in practice.*

* Research Fellow, Vidhi Centre for Legal Policy. The author would like to thank Damini Ghosh, Senior Resident Fellow, Vidhi Centre for Legal Policy, for her guidance and inputs.

I. Introduction

A number of engaging legal problems in the emerging field of data protection require careful scrutiny as we grapple with questions regarding how to treat personal data, how to characterise the relationship between such data and the data principal/subject, how to identify the legitimate situations in which other persons may use such data, and what persons using such data must do to safeguard the interests of data principals/subjects. As India moves to adopt a governance framework for informational privacy, it is appropriate to closely analyse the substantive rights and duties that are put into place in relation with personal data, whose unique characteristics result in unique reasons to value it.

Even as the contours of various solutions to these problems emerge, the means by which to enforce data protection law equally require close study. The designs of the enforcement mechanisms for informational privacy also have a wide range of correlations with the unique characteristics of personal data and the structure of data protection law. As will emerge in the discussion below, these correlations mean that the design of the regulatory mechanism must proceed simultaneously with the design of the substantive law. The central argument of this article is that the regulatory scheme for data protection must closely match the regulatory burden it entails a burden shaped by the dizzying variety of contexts in which personal data is processed, the volume of such data being processed, the number of entities that process such data, the ease with which such data can change hands, the ease with which the use of the data can be modified, the ease with which possession and use can be obfuscated, and the subtle ways in which the observation of a person can harm them.

The problems related to regulatory burden in data protection are alluded to in the following section though they are further elucidated later in the Article. The third section then relates questions of capacity with two structural choices for a data protection regulator: first, whether to have the regulatory burden shouldered by a single, specialised regulator or have it shared amongst sectoral regulators, and second, whether to have the regulatory burden borne exclusively by the regulator or whether to allow regulated entities to participate in the regulatory process. After explaining why these choices have sparked debate in the context of data protection, the section argues in favour of the appropriate structures that need to be adopted in each case. The fourth section then turns the focus to two further concepts in data protection regulation: accountability and responsive regulation. Both these concepts are broken down and explained and the need for their adoption in data protection is linked, once again, to the unique regulatory burdens of the

field. The fifth and final section concludes with a few additional remarks. The focus throughout will be on the Draft Personal Data Protection Bill, 2018, released by the Srikrishna Committee of Experts on Data Protection ('**Srikrishna Committee**').[1] A new Bill with a number of modifications has since been tabled in Parliament,[2] and while the general regulatory approach discussed in this Article has remained the same, certain notable points of departure worth scrutinising have been identified below.

II. Enforcement Challenges, Old and New

A. A Legacy of Low Capacity

Rights and duties in practice have always depended on the regulatory structures by which they are given life. In India, for example, a recurring theme in regulatory policy is the limitation on capacity: the promises of the law remain unfulfilled because the regulatory structures that effectuate them can be poorly designed, under-staffed, and lacking in good governance incentives and procedures.[3] There can often be infrastructural shortcomings and lack of technical know-how.[4] Since it would be difficult to quickly build up capacity in the early days of a law's implementation, some argue that regulatory structures can collapse under pressure, fall back onto formalistic posturing or fail to follow due process requirements.[5] It is easy enough to say that inad-

---

1 Draft Personal Data Protection Bill, 2018, <https://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill%2C2018_0.pdf> accessed 21 March 2020 (Draft PDPB, 2018).

2 Personal Data Protection Bill, 2019, <http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf> accessed 21 March 2020 (PDPB, 2019).

3 *See*, for instance, Shubho Roy and others, 'Building State Capacity for Regulation in India', in Devesh Kapur and Madhav Khosla (eds), *Regulation in India: Design, Capacity, Performance* (Hart Publishing, 2019) 359 (arguing, on a number of bases, that "*Regulators have … been plagued by poor State capacity.*"); Devesh Kapur and others (eds), 'Introduction' in *Rethinking Public Institutions in India* (OUP, 2017) 5-8 (bemoaning lack of capacity due to the Indian State's "*relatively small size*" and due to its being "*as over-bureaucratized as it is under-staffed*".)

4 This issue is only exacerbated in the digital context. *See*, Geoffrey G. Parker and others, *Platform Revolution: How Networked Markets are Transforming the Economy — and How to Make Them Work for You* (W.W. Norton & Company, 2016) 255 (advising that future models of regulation for digital platforms across the world, including for data protection, will require "*significant talent upgrades on the part of government agencies*".); *See also*, Ananth Padmanabhan and Anirudh Rastogi, 'Big Data', in Devesh Kapur and Madhav Khosla (eds), *Regulation in India: Design, Capacity, Performance* (Hart Publishing, 2019) 272-273 (warning of how big data creates "*new challenges that demand the rapid upgrading of skills from the regulator's end*").

5 Suyash Rai, 'Comment on the White Paper of the Committee of Experts on a Data Protection Framework for India' 1-6 <http://macrofinance.nipfp.org.in/PDF/data_protection_comments_suyash.pdf> accessed 15 February 2019.

equacies in the level of enforcement are to be accepted for budgetary reasons or lack of expertise. However, this under emphasises the effects of deficits in regulatory capacity. Apart from a regulator's posturing and due process failures, the overall effect on the rule of law caused by unenforced rules and unaddressed violations should be recognised as a significant concern, though it may be difficult to measure.

B. Challenges in the Information Age

In addition to the legacy of issues surrounding state capacity in India, there are a number of additional burdens that are likely to emerge in the context of digital governance. One prime consideration is the pace of innovation in data processing techniques. Rule-based governance requires some stability of circumstances if the criteria embedded in the rule are to continue to be relevant and effective. If innovation is extremely fast-paced, the processes for the modification of rules will have to keep up. Governance institutions are already falling behind on many fronts and it seems apparent that this trend will continue.[6] In the realm of data protection, for example, this is apparent in such schemes for privacy protection as anonymizsation.[7] Another aspect of the innovation question is the public interest in actually promoting it. All the fruits of technological advancement have been borne due to the culture of innovation that the tech industry has promoted and the continued channelling of such benefits would require that this culture not be throttled by *ex ante* regulatory schemes like licensing and permissions.[8]

If the speed of change creates one set of problems from a dynamic view, the complexity, context-specificity and opacity of data-related processes

---

[6] William D. Eggers and others, 'The Future of Regulation: Principles for Regulating Emerging Technologies', (*Deloitte Insights*, 19 June 2018) <https://www2.deloitte.com/insights/us/en/industry/public-sector/future-of-regulation/regulating-emerging-technology.html> accessed 23 February 2019 ("*As new business models and services emerge … government agencies are challenged with creating or modifying regulations, enforcing them, and communicating them to the public at a previously undreamed-of pace.*"); for general discussion on the 'ossification' of traditional rulemaking, *See*, Richard J. Pierce, Jr., 'Rulemaking Ossification is Real: A Response to Testing the Ossification Thesis' (2012) 80 George Washington Law Review 1493; Jason Webb Yackee and Susan Webb Yackee, 'Testing the Ossification Thesis: An Emperical Examination of Federal Regulatory Volume and Speed, 1950-1990' (2012) 80 George Washington Law Review 1414; Aaron L. Nielson, 'Optimal Ossification' (2018) 86 George Washington Law Review 1209.

[7] Jules Polonetsky and others, 'Shades of Gray: Seeing the Full Spectrum of Practical Data De-identification' (2016) 56 Santa Clara Law Review 593, 594 ("*Computer scientists and mathematicians have come up with a re-identification tit for every de-identification tat.*")

[8] Parker (n 4) 230 ("*There is a significant tension between the social goals of promoting innovation and economic development, which argue for a relatively laissez-faire approach to regulating platforms, and the social goals of preventing harm, encouraging fair competition, and maintaining respect for the rule of law.*")

constitute another such set even if we discount change. The very use of information technology exponentially increases the difficulty in detection of violations and makes many kinds of sustained investigations considerably tricky. Issues related to the number of users, physical accessibility of devices, remote access to digital assets, transnational dimensions, speed of data exchange, anonymity and encryption, automation etc. do not all surface simultaneously in non-digital governance areas.[9] The power of platforms to constrain competition, the growth of unmanageably voluminous information flows, and systemic threats with uncertain future realisation constitute further challenges to the existing paradigm for regulatory constructs.[10] As a result of these issues, regulators are looking to bolster various facets of their investigative powers.[11] Even short of investigation, regulators must worry about the appropriateness of their rulemaking. Any regulations issued by a regulatory body should not run slip-shod over the differentiated circumstances in which privacy interests arise.[12] What is more, data protection law in particular must face up to unique issues including the level of regulatory discretion needed to strike the right balance in fair rulemaking or adjudication while coping with the transaction-intensive nature of personal data transfers across industries.[13] Further, key regulatory concerns in data protection linked to context-sensitivity, the ease of change of purpose for process-

---

[9] For a detailed view of such issues, *see*, International Telecommunication Union, *Understanding Cybercrime: Phenomena, Challenges and Legal Response* (September 2012) <http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf> accessed 23 February 2019, at 22-23, 75-81, 227-33, 239-43 (for example, the report notes how investigative agencies were able to meet the challenges of child pornography while it was still transported through the postal services but struggle to do so now); *See also*, for some of the traditional techniques used by violators, Larry Greenemeier, 'Seeking Address: Why Cyber Attacks are So Difficult to Trace Back to Hackers' (*Scientific American*, 11 June 2011) <https://www.scientificamerican.com/article/tracking-cyber-hackers/> accessed 23 February 2019.

[10] Julie E. Cohen, 'The Regulatory State in the Information Age' (2016) 17 Theoretical Inquiries in Law 369, 375, 395.

[11] Oscar Williams, 'Exclusive: Government Considering Boosting ICO's Powers Amid Cambridge Analytica Scandal' (*New Statesman Tech*, 26 March 2018) <https://tech.newstatesman.com/news/government-ico-powers-cambridge-analytica> accessed 23 February 2019); *See also*, Carole Cadwalladr, 'Elizabeth Denham: 'Data Crimes are Real Crimes' (*The Guardian*, 15 July 2018) <https://www.theguardian.com/uk-news/2018/jul/15/elizabeth-denham-data-protection-information-commissioner-facebook-cambridge-analytica> accessed 23 February 2019 (for a view on the kind of personnel required for a large data protection investigation as well as the reliance on journalists, civil society and whistleblowers for bringing forward evidence).

[12] For a leading theory on the contextual approach to privacy, *see*, Helen Nissenbaum, 'Privacy as Contextual Integrity' (2004) 79(1) Washington Law Review 119; for a further view on the contextual nature of digital interfaces in different areas, *see*, Stephen R. Miller, 'First Principles for Regulating the Sharing Economy' (2016) 53 Harvard Journal on Legislation 147, 151, 153.

[13] Rai (n 5) 3-5.

ing, and the diffused nature of privacy harms play equally significant roles in shaping the regulatory burden under study and will be elaborated upon in appropriate sections below.

It is in the face of such legacy and emerging issues that a regulatory framework for data protection must be built up. How far privacy law sees active implementation will depend on the way these challenges are dealt with.

III. The Structural Choices for a Privacy Watchdog

There is a broad consensus across jurisdictions that data protection regulation benefits from the existence of regulatory bodies instead of just legislations implemented by government departments and courts.[14] Setting this question aside, there are some further standard questions on regulatory structure that must be answered at the threshold - whether regulation can be better done by a specialised, unified regulator or by sectoral regulators acting in their specific sectors, and how far can private entities be trusted to share regulatory burdens. Both questions are dealt with in turn below. However, they have one common theme animating the concerns over whether a regulator will be able to bear its regulatory burdens all by itself. The amelioration of such concerns may seem to necessitate solutions involving some form of 'decentralisation' of regulatory controls. However, not all of these forms of sharing of burdens are equally appropriate and the manner in which these approaches can go wrong is elaborated upon below in justifying particular structural choices.

A. The Perils of a Worm's-Eye View

As discussed above, our preferences regarding our own personal information can be strikingly contextual. What we are willing to reveal or communicate regarding ourselves depends on who we are talking to and who else can hear us. Taken to its logical end, this line of reasoning would suggest that the best rules for the regulation of personal information flows must be developed within the different walks of life in which we operate. Would it then not be appropriate for there to be sectoral regulators handling data protection questions in their respective sectors? Finance, health, news media, social

[14] The kinds of problems that necessitate specialised regulatory bodies include the inability of legislatures to keep up with dynamic areas of law and their lack of intricate industry knowledge coupled with the fact that government departments have a similar lack of expertise and specialisation, weak processes to absorb market feedback, a continued culture of central planning, the potential politicisation of individual transactions due to direct ministerial control, and conflicts of interest where departments own elements of the production process. *See*, for an instance of this listing, Roy (n 3).

media, governmental agencies, legal proceedings etc. can each have different standards for privacy with agencies dedicated for these areas handling data protection issues according to the in-depth understanding of their field.

However, even a cursory glance at developments in other jurisdictions dispels this notion. The move towards comprehensive privacy legislations has been gradual but decisive, with comparative experiences in implementation playing a key role. Even the EU's shift from the 1995 Data Protection Directive to the recent General Data Protection Regulation ('**GDPR**') was largely driven by concerns regarding fragmentation in the implementation of data protection law in different European jurisdictions.[15] The US is a prominent outlier on this front with the applicability of key federal legislations being restricted only to specific types of data and specific types of entities. However, such a focus on a limited set of identified contexts of information use results in gaps in coverage. Enforcement actions are constantly forced to proceed only after threshold determinations are first made regarding the applicability of legislation to a particular situation.[16] This means that every time privacy rules are sought to be enforced, the legal process must first ascertain whether certain, specific rules are applicable to particular entities - a determination made on the basis of how a sectoral law defines the entities it seeks to regulate or otherwise specifies its own applicability, eg a law on financial privacy will often have to delineate which financial organisations it will apply itself to. States also chip in with laws for their own territories, adding to the already veritable patchwork such that there is reduced clarity, increased complexity and sometimes even conflicts between the different laws in a fragmented regime.[17]

The examples of the health and telecommunications sector in the US have been used to indicate that the definitions used to identify the relevant players in the industry or the definition of specific kinds of information fail to address even those privacy concerns that relate to that industry, often because the said definitions are confusing or inadequate. This is in the nature of the ease of modification of data use and is especially troublesome given the increased big data analytics practices that lack fixed purposes and allow data to break sectoral silos.[18] As noted privacy scholar Daniel Solove notes,

---

[15] *See*, General Data Protection Regulation (EU) 2016/679, Recital 9.

[16] Paul M. Schwartz, 'The Value of Privacy Federalism' in *Social Dimensions of Privacy: Interdisciplinary Perspectives* (Roessler & Mokrosinska eds.) (2015).

[17] Nuala O'Connor, 'Reforming the US Approach to Data Protection and Privacy' (*Council on Foreign Relations*, 30 January 2018) <https://www.cfr.org/report/reforming-us-approach-data-protection> accessed 28 March 2019.

[18] Kirk J. Nahra, 'Is the Sectoral Approach to Privacy Dead in the U.S.?' (*Privacy and Security Law Report*, 2016) 15 PVLR 153.

the sectoral regime in the US has resulted in widespread uncertainty regarding the protections available for different kinds of personal data, a resultant lack of respect for US privacy law, failure in the law keeping up with sectoral shifts, and persistence of gaps where data remains unprotected.[19]

In sum, it is relevant to keep in mind that informational flows have never respected sectoral barriers as personal data can be easily transposed for the creation of value across industries. Not only does data flow across sectors but private entities also span across multiple industries allowing them to freely shuffle around datasets internally if left unchecked. As Cohen notes:[20]

> Understanding economic power and its abuses in the era of informational capitalism requires discussions about the new patterns of intermediation and disintermediation that information platforms enable, and about the complexity and opacity of information-related goods and services.

Bewildering as the information age is, one solution may lie in constitutionalism. In advising that India follow the EU route for a strong, comprehensive legislation instead of the US sectoral/self-regulatory route to data protection regulation, Greenleaf points out the significance of privacy being a fundamental right:[21]

> The position in India … is in general principle the same as the EU: privacy is a fundamental inalienable right, with the ability of governments to derogate from it requiring considerable justification … [Data protection in India] will have to meet standards approximating those of EU laws if it is to constitute the background environment within which particular legislative interferences with privacy can be justified.

This does, of course, depend on the extent to which one sees fundamental rights like privacy being applicable in the context of the activities of private entities, either directly or in the form of a duty of the state to intervene and protect individuals from such entities.[22] While concerns may exist regarding

---

[19] Daniel Solove, 'The Growing Problems with the Sectoral Approach to Privacy Law' (*TeachPrivacy*, 13 November 2015) <https://teachprivacy.com/problems-sectoral-approach-privacy-law/> accessed 28 March 2019.

[20] Cohen (n 10) 375.

[21] Graham Greenleaf, 'Data Protection: A Necessary Part of India's Fundamental Inalienable Right of Privacy – Submission on the White Paper of the Committee of Experts on a Data Protection Framework for India' UNSW Law Research Paper No. 18-6 (2018) 4.

[22] For studies on the 'horizontal' applicability of fundamental rights, *see*, Stephen Gardbaum, 'The "Horizontal Effect" of Constitutional Rights' (2003) 102(3) Michigan Law Review 387; Mark Tushnet, 'The Issue of State Action/Horizontal Effect in Comparative Constitutional Law' (2003) 1(1) International Journal of Constitutional Law 79; Stephen Gardbaum, 'The Indian Constitution and Horizontal Effect' in *The Oxford Handbook*

the unclear position of a unified data protection regulator in its relations with various other sectoral or statutory authorities, these are not intractable issues and should be viewed in light of the increasing need for formal coordination mechanisms between different public agencies. This requirement has notably been addressed in the Draft Bill released by the Srikrishna Committee by inserting a requirement for the proposed Data Protection Authority ('**DPA**') to consult other regulators and authorities and a power to enter into agreements with them.[23]

B. Between a Public Devil and a Private Deep Sea

The potential for involvement of private organisations in processes for their own regulation is an old theme in data protection policy discourse and has been agitated in the past in the context of the divide between the US and the EU in their approaches. The debate generally outlines three different models for regulation: command-and-control, self-regulation and co-regulation.[24] The first variety refers to governmental regulation, often with a rule-based mechanism for determining how the conduct of the regulated entities should look like. It thus constrains market behaviour through enforcement and sanctions handled by a governmental authority. On the other hand, self-regulation involves private organisations creating and enforcing standards themselves, often by enhancing the conditions for market exchange. Thus, in the context of data protection, some argue that businesses have various incentives to protect privacy since they would lose customers if they didn't. In contrast with both the above, co-regulation involves sharing of responsibility between public agencies and industry for drafting and enforcing regulatory standards.[25] While this combines elements of governmental regulation with elements of self-regulation, some claim that it can be "*typified by a specific combination of state and non-state regulation*".[26] The possibility of such combinations indicates that a system of regulation with a few limited but significant elements of non-state regulation would still be considered co-regulation. The essential aspects of state regulation, including approval and oversight of the non-state actions, need not be sacrificed. What

---

of the Indian Constitution (OUP, 2016), ch 33; *See also*, for a leading case touching upon horizontal effects in the context of the right to education, *Society for Unaided Private Schools of Rajasthan v Union of India* (2012) 6 SCC 1, especially paras 126, 159 and 222.

[23] Draft PDPB 2018, cl 67.

[24] Dennis D. Hirsch, 'The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation?' (2011) 34 Seattle University Law Review 439.

[25] ibid 441.

[26] Hans-Bredow-Institut for Media Research, Final Report: Study on Co-Regulation Measures in the Media Sector (2006) 17, <https://www.hans-bredow-institut.de/uploads/media/default/cms/media/cd368d1fee0e0cee4d50061f335e562918461245.pdf> accessed 10 March 2019 (emphasis added).

limited non-state aspects may be retained? A well-understood co-regulatory mechanism is for "*[government] agencies [to] collaborate with industry groups or other third parties to develop detailed substantive rules … [which] may then become enforceable law, frequently (though not always) subject to some approval or ratification by government regulators*."[27] In a world where privacy interests can be contextual, the development of 'codes of conduct' embodying best practices through collaboration with industry bodies can provide necessary sectoral adaptation where comprehensive legislations and agency-driven regulation-making are likely to fall short. What is important is that while these codes may draw upon the inputs and even the drafts of private entities, the exact form of the code that is finally approved is still the decision of the government.

At the outset, it is appropriate to note that the Report of the AP Shah Group of Experts in 2012 had endorsed the use of co-regulation in the context of privacy governance. It envisaged self-regulatory organisations voluntarily adopting standards not lower than certain national privacy principles, thus allowing "*for both high level principles to be achieved and for specific privacy standards to be enforced*".[28] Similarly, the White Paper released by the Srikrishna Committee for consultation purposes also endorsed co-regulation as "*an appropriate middle path that combines the flexibility of self-regulation with the rigour of government rulemaking*".[29] Notably, discussion of this provisional view is absent in the Committee's final Report.[30] Further discussion of the responsive regulatory model endorsed in the final Report is in the fourth section of this article. However, the adoption of a regulatory scheme that is responsive does not prevent sharing of regulatory burdens through co-regulation. Suffice it to say that the questions raised by the White Paper may still require close attention.

Whatever calls for self-regulation existed in the context of privacy have seen a decided cutback over the last two decades. In its White Paper, the

---

[27] William McGeveran, 'Friending the Privacy Regulators' (2016) 58 Arizona Law Review 959, 980; Ira Rubinstein, 'Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes' (2011) 6 I/S: A Journal of Law & Policy for the Information Society 356, 383.

[28] Report of the Group of Experts on Privacy (Chaired by Justice A.P. Shah, Former Chief Justice, Delhi High Court) (2012) <http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf> accessed 10 March 2019 at 57, 69 and 75.

[29] White Paper of the Committee of Experts on a Data Protection Framework for India (2017) <https://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_171127_final_v2.pdf> accessed 10 March 2019 at 145-146.

[30] *See*, Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (2018) ch 9 <https://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report-comp.pdf> accessed 10 March 2019 (Srikrishna Committee Report).

Srikrishna Committee couched the debate regarding regulatory approaches as being largely captured in an EU-US binary - the distinction between a comprehensive legislation with strong regulatory powers and a market-oriented, sectoral model.[31] On the other hand, in his submissions to the Committee in response to the White Paper, Greenleaf argued that this was "*a considerable understatement and misunderstanding*" and outlined the variety of jurisdictions that had adopted privacy standards, largely in the form of comprehensive laws with high-powered regulators in the European mould. The US approach thus appears to have fallen terribly out of step with global practice[32] despite official calls for a strict, general law issuing at least as early as 2000.[33] With it, self-regulation has increasingly appeared an infeasible mode of privacy governance.[34] Even conceptually, the prospect of self-regulation in data privacy is fraught with problems given that it is unable to overcome significant market failures as a result of collective action problems (because of shared interest in personal information) information asymmetries ("*[I]ndividuals today are largely clueless about how personal information is processed through cyberspace*").[35]

The prospect for co-regulation, on the other hand, has been more promising. In the context of the US, given the initial dependence on self-regulation, Rubinstein views co-regulatory measures, including privacy safe harbours, as an effective and flexible policy instrument if well designed. She points to a holistic approach for privacy protection that relies on organisational data governance systems and internal privacy methodologies as well as reliance on best practices: a greater reliance on internal policy over state-heavy prescription.[36] Some argue that it may be appropriate for developing economies

---

[31] White Paper of the Committee of Experts on a Data Protection Framework for India (n 29) 10-14.

[32] Greenleaf (n 21) 3-4.

[33] *See*, for instance, Federal Trade Commission, 'Privacy Online: Fair Information Practices in the Electronic Marketplace – A Report to Congress' (May, 2000), <https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf> accessed 10 March 2019.

[34] Robert Gellman and Pam Dixon, 'Many Failures: A Brief History of Privacy Self-Regulation in the United States' (*World Privacy Forum*, 14 October, 2011) <http://www.worldprivacyforum.org/wp-content/uploads/2011/10/WPFselfregulationhistory.pdf> accessed 10 March 2019; Ryan Moshell, 'And Then There Was One: The Outlook for a Self-Regulatory United States Amidst a Global Trend Toward Comprehensive Data Protection' (2005) 37(2) Texas Tech Law Review 357; Morey E. Barnes, 'Falling Short of the Mark: The United States Response to the European Union's Data Privacy Directive' (2006) 27 Northwestern Journal of International Law & Business 171.

[35] Jerry Kang, 'Information Privacy in Cyberspace Transactions' (1998) 50 Stanford Law Review 1193, 1253.

[36] Rubinstein (n 27) (safe harbour provisions seek to encourage participation in self-regulatory programs by treating an entity that has complied with the program guidelines as

to consider co-regulatory models even before adopting national legislations. The approach may best capture the benefits of a growing e-commerce sector. While one justification is that developing countries may have substantial budgetary constraints in meeting desired privacy objectives, another is that they may lack technical expertise and effective judicial systems. The stifling of innovation may be a further concern for an economy that is eager to grow.[37] In India particularly, apart from the 2012 Report of the AP Shah Group of Experts mentioned above, others have also called for the adoption of co-regulatory initiatives for data protection.[38]

In describing how regulatory institutions have been changing in recent years, Cohen characterises the models as "*procedurally informal, mediated by networks of professional and technical expertise that define relevant standards, and financialized*".[39] The rise of informal guidance, non-binding interpretations, and the development of and reliance on best practices are thus to be viewed alongside the growth of collaborative proceedings that result in consensus-based standards that may require private enforcement. While these developments align well with the unique regulatory challenges of the information age, they also create new transparency and accountability problems.[40] Greenleaf does not see any successes emerging from co-regulation efforts at all and considers them to be of no significance in Asian data privacy laws. While it had been considered a key part of Australia's regulatory approach to privacy, it appears to have been discontinued. The most significant concern is the risks involved in any scheme that allows vested interests in industry bodies to gain control over privacy regulation-making.[41] A weak track record on transparency, complaints handling and the failure in the revocation of privacy marks constitute further corroboration of general concerns.[42]

---

having complied with statutory requirements).

37 Tiffany Curtiss, 'Privacy Harmonization and the Developing World: The Impact of the EU's General Data Protection Regulation on Developing Economies' (2016) 12 Washington Journal of Law, Technology & Arts 95.

38 Rahul Matthan and others, 'A Data Protection Framework for India: In response to the White Paper released by the Justice Srikrishna Committee' (*Takshashila Policy Advisory 2018-01*, February 2018) <http://takshashila.org.in/wp-content/uploads/2018/02/TPA-Data-Protection-Framework-for-India-RM-MV-AP-2018-01.pdf> accessed 28 March 2019, 65; Amber Sinha, 'India's Data Protection Regime must be Built through an Inclusive and Truly Co-Regulatory Approach' (*The Wire*, 1 December 2017) <https://thewire.in/business/inclusive-co-regulatory-approach-possible-building-indias-data-protection-regime> accessed 28 March 2019 (favouring an inclusive and participatory approach to rule-making, including in relation with the conduct of the Srikrishna Committee itself).

39 Cohen (n 10) 395.

40 ibid.

41 Greenleaf (n 21) 22.

42 Graham Greenleaf, *Asian Data Privacy Laws: Trade and Human Rights Perspectives* (OUP, 2017) 524, 525.

Concerns of this nature are appropriate in light of the hazards of self-regulation. Co-regulation can easily appear like an official channel allowing for the systematic compromise of public agencies. However, it is not appropriate to define our concepts on the basis of potential outcomes that we do not like. Co-regulation as a coherent concept and regulatory approach is based on the idea of sharing regulatory burdens with private bodies and there need be no presupposition as to how much or what kind of burdens are to be shared. The EU's GDPR is seen as a very promising standard for stricter privacy protections[43] but it is easily recognisable that it contains co-regulatory features as well.[44] If one is not frightened by the very use of the term 'co-regulation', it should be accepted that well-designed elements such as the formal assessment and approval of best practices through codes of conduct, the utilisation of privacy marks or scores, mandated organisational complaints redressal systems, and reliance on private entities like data protection officers and auditors can reduce much of the regulatory burden of data protection without compromising on integrity.[45] Significant conditions for the efficacy of co-regulation are the maintenance of transparency in the approval of codes

---

[43] Dr. Sebastian Golla, 'Is Data Protection Law Growing Teeth? The Current Lack of Standards in Data Protection Law and Administrative Fines under the GDPR' 8(1) Journal of Intellectual Property, Information Technology and E-Commerce Law (2017) <https://www.jipitec.eu/issues/jipitec-8-1-2017/4533> accessed 28 March 2019; as described by UK's Information Commissioner: "*The new European law – the GDPR – has a global pedigree. Regulatory instruments and practices developed elsewhere in the world were embedded in its DNA during its drafting. We in the EU made vigorous efforts to learn from abroad and embrace policy instruments that were pioneered in other countries. Fair information practices and breach notification originated in the US; accountability and Privacy by Default and Design in Canada; Codes of Practice from the UK and New Zealand; and innovation measures from East Asia.*" (Elizabeth Denham, Speech to the International Privacy Forum, 50th Asia Pacific Privacy Authorities Forum, Wellington, New Zealand (4 December 2018) <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/12/international-privacy-forum-forum/> accessed 2 April 2019.

[44] Irene Kamara, 'Co-regulation in EU Personal Data Protection: The Case of Technical Standards and the Privacy by Design Standardisation "mandate"' (2017) 8(1) European Journal of Law & Technology <http://ejlt.org/article/view/545> accessed 28 March 2019 (noting the shift from pure command-and-control regulation to co-regulatory approaches, with the example of the development of standards for privacy management); Hirsch (n 24) (citing the scheme for codes of conduct under the EU 1995 Data Protection Directive as an instance of co-regulation worth studying further); Greenleaf (n 21) 22 (referring to and endorsing the EU GDPR's scheme for codes of conduct under Arts. 40 and 41 as "*a very highly-regulated approach*" for the introduction of "*elements of co-regulation*").

[45] Such features may be noted in the Srikrishna Committee's Draft PDPB, 2018, <https://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill%2C2018_0.pdf> accessed 28 March 2019 (*see*, cls 35, 36, 39, and 61); *See also*, Padmanabhan and Rastogi (n 4) 268 (maintaining that "*the Expert Committee veers towards co-regulation*"); in this view, it may be too quick to say that the Bill 'prohibits' co-regulation as some have noted (*see*, 'Assessing India's Proposed Data Protection Framework: What the Srikrishna Committee could Learn from Europe's Experience' (*Access Now*) 15 <https://www.accessnow.org/cms/assets/uploads/2018/10/Assessing-India%E2%80%99s-proposed-data-protection-framework-oct18.pdf> accessed 28 March 2019. The most appropriate label to employ

of conduct and opportunity for appeal from tardy complaints redressal mechanisms.[46] Such features can ensure that co-regulatory rulemaking and enforcement are being adequately overseen and checked by the state and data subjects/principals respectively. They should definitely be integrated into any implementation of the model.

IV. Accountability and Responsive Regulation

Under the Srikrishna Committee's Draft Personal Data Protection Bill, the proposed DPA is endowed with a dizzying array of powers and functions ranging from specifying 'reasonable purposes' under Clause 17 to identifying residuary categories of sensitive personal data under Clause 22, from managing data auditors to registering significant data fiduciaries, from monitoring cross-border flows of data to responding to data security breaches, from raising awareness to handling and adjudicating on complaints, and from issuing codes of practice on a host of subjects under Clause 61 to making regulations on an equally numerous set of subjects under Clause 108.[47] The substantive bases for liability on data fiduciaries also enter into considerable detail with various broad principle-based duties like purpose specification and privacy by design existing side by side with specific obligations like data breach notification and data portability. Some rights, such as the right to be forgotten, require the proposed DPA's adjudicating officers to enter into a balancing act guided by a nuanced set of criteria.[48] The sharing of burdens across alternative regulatory tracks such as co-regulation forms only one response. Two further solutions, accountability and responsive regulation, are discussed below.

A. Accountability: The Real Measure of Responsibility

In describing the contours of privacy (including decisional privacy) and assessing an anti-totalitarian conception of the right vis-à-vis state power,

---

for the Committee's model would probably be "command-and-control with co-regulatory features.")

[46] *See*, Draft PDPB 2018, cls 39 and 61 (2), (3) and (4); a crucial method by which to ensure that regulation is not controlled by regulated entities is to also involve public interest and consumer protection groups in the regulation-making process in a system of 'tripartism' (*see*, Ian Ayres and John Braithwaite, *Responsive Regulation: Transcending the Deregulation Debate* (OUP, 1992), 55, 56).

[47] Draft PDPB 2018, cl 60.

[48] Draft PDPB 2018, cl 27; commentators have noted that data protection law requires intensive, detailed and discretionary regulatory action due to the large number of transactions that require regulatory decisions as well as the imperfect and incomplete information available for such decisions [*See*, Rai (n 5) 3-4].

Solove argues that we must view it as not only involving prohibitions against intrusions but also active protections:[49]

> In fact, privacy is both a positive and negative right; it is not just a freedom from the state, but a duty of the state to protect certain matters via property rights, tort law, criminal law, and other legal devices. Without protection against rape, assault, trespass, collection of personal information, and so on, we would have little privacy and scant space or security to engage in self-definition. To preserve people's ability to engage in self-definition, the state must actively intervene to curtail the power of customs and norms that constrain freedom.

This powerful account of the evolution of privacy jurisprudence draws on the steady movement that the concept has seen from negative rights as prohibitions to positive duties of protection and advancement. Though it is argued in relation with state power, this evolution is also very much in line with how we may see private power in the context of personal information. The development of data protection law, policy and regulation are core parts of the state's positive duties towards informational privacy. What form of positive duties can private entities have under data protection? These duties should appropriately be designed with a keen eye for the systemic threats created by the information age. In Cohen's astute analysis of the risk and information-oriented regulatory responses to the growing recognition of systemic threats, she finds:

> As societal understandings of harm have evolved to encompass more long-term and systemic effects of development, regulatory methodologies have evolved as well. The contemporary toolkit includes constructs oriented toward measuring, demonstrating, and responding to harms that are nascent and systemic, and those constructs are themselves predominantly informational. … As threatened future harms have become more abstract, diffuse, and technologically complex, disputes about appropriate regulatory response have become struggles for control over the modeling and representation of systemic threats and over the burden of proof required to justify regulatory actions.

The probabilistic and diffused nature of certain kinds of privacy harms is an important aspect of study relevant to data protection, with one scholar distinguishing 'subjective' and 'objective' privacy harms and even analogising them with assault and battery respectively (the former is an apprehension

---

[49] Daniel J. Solove, 'Conceptualizing Privacy' (2002) 90(4) California Law Review 1087, 1120.

or threat of the latter).[50] These informational considerations mean that individuals have considerably reduced abilities to safeguard themselves against harm through privacy self-management. This situation is considerably aggravated due to what is variously called 'infoglut'[51] or informational overload and the consequent occurrence of 'consent fatigue' due to which individuals find themselves with a surplus of material making it difficult for them to identify points of information relevant to their choices.[52] From the perspective of those handling personal data, the 'data deluge' caused by the increased availability and transfer of large quantities of data also multiplies the risk of grave data breaches.[53]

At the same time, it also means regulatory authorities have reduced abilities to detect, investigate and conclusively fix liability for the creation of diffused harms and systemic threats. Ordinary concepts of liability relying on chains of causation can be difficult to work with when proofs regarding remotely-caused harm from opaque operations lie only in ephemeral digital objects and processes. Equally, subjective harms (dependent upon a feeling of being observed, for instance) do not lend themselves to quantification and concrete evidence, making the harm component difficult to prove as well.

This is the context in which we must understand the principle of accountability. The term itself is a very mundane one, used in common parlance with little regard for any technical meaning that it could have. One may argue that it is a bit superfluous to speak of accountability as a separate coherent legal concept at all given how implicit it can be in the context of any and every legal duty. For example, consider the specific provision embedded in the GDPR regarding accountability. In Article 5(2), the principle is formulated with two prongs: first, that a data controller "*shall be responsible*" for compliance with the data protection principles in sub-article (1) of the same Article, and second, that the controller shall "*be able to demonstrate*" the said compliance.

In the context of a legal duty, the first prong can appear somewhat redundant. Isn't a regulated entity 'responsible' for compliance with its legal duties anyway? Isn't the allocation of responsibility through the concept of liability

---

50 M. Ryan Calo, 'The Boundaries of Privacy Harm' (2011) 86 Indiana Law Journal 1131.

51 Mark Andrejevic, *Infoglut: How Too Much Information is Changing the Way We Think and Know* (Routledge, 2013).

52 Daniel Solove, 'Privacy Self-management and the Consent Dilemma' (2013) 126 Harvard Law Review 1880; B. W. Schermer and others, 'The Crisis of Consent: How Stronger Legal Protection may Lead to Weaker Consent in Data Protection' (2014) 16(2) Ethics and Information Technology.

53 Article 29 Data Protection Working Party, Opinion 3/2010 on the Principle of Accountability (2010), para 6.

the very reason why we have laws at all?[54] We should understand this formulation, however, in the context of the recent developments in the course of which it came to be adopted. For one matter, it is certainly not a new concept in data protection law. Accountability has featured in prior legal instruments and had been discussed and put into practice under the EU's 1995 Data Protection Directive before official advisories and negotiations resulted in its explicit inclusion as a provision in the GDPR.[55] Why was there a need for such an explicit inclusion? It is difficult to understand the reasoning for the first prong but it is likely traceable to the generalised anxiety created by the prospect of a 'post-privacy' age or the 'death of privacy'. As noted by the Srikrishna Committee in its White Paper:[56]

> The processing of personal data entails an increase of power (in terms of knowledge and its consequent insights) of the data controller vis-à-vis the individual. Data protection regulations are a means to help protect individuals from abuses of power resulting from the processing of their personal data. The method by which this protection was traditionally sought to be achieved was using notice and consent, offering the individual the autonomy to decide whether or not to allow her data to be processed … the concept of privacy self-management is coming under pressure given the complexity of the trade-offs between the benefits and the harms of modern technology. To offset the flaws of the notice and choice model, a key principle that has emerged is of accountability …

Accordingly, we can understand the first prong best as an attempt to rebalance power structures and the allocation of responsibility in the digital economy given the shortcomings of privacy self-management. In grappling with the problem of how to ensure the full measure of responsibility on the part of data controllers/fiduciaries, the law has come face to face with society: its intention is to *directly* demand a culture of privacy and thereby

---

[54] Thus, one finds statements such as, "*Arguably, all GDPR requirements require some accountability on the part of the controller and operational policies and procedures to give effect to the legal obligations*." (Centre for Information Policy Leadership, 'The Case for Accountability: How it Enables Effective Data Protection and Trust in the Digital Society' Discussion Paper 1 (of 2) (23 July 2018), 11 <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_paper_1_-_the_case_for_accountability_-_how_it_enables_effective_data_protection_and_trust_in_the_digital_society.pdf> accessed 30 March 2019).

[55] *See*, Article 29 Data Protection Working Party, Opinion 3/2010 (n 53), para 2 (for reference to the Working Party's proposals regarding explicit inclusion of the principle) and paras 16-20 (for prior precedents); *See also*, Canada's Personal Information Protection and Electronic Documents Act 2000, sch 1, para 4.1.

[56] White Paper of the Committee of Experts on a Data Protection Framework for India (n 29) 147.

engender trust in the digital economy.[57] This may have become necessary as such a privacy culture was not emerging naturally, through market competition or assortments of specific legal duties. The focus on changing cultures and mindsets may become more apparent once we start unpacking the first prong and examining what the general principle could look like in practice.

Most sources point to a similar (non-exhaustive) set of obligations that form part of the principle - the establishment of internal procedures such as review and impact assessment mechanism, written and binding internal privacy policies, identification of all data processing operations, appointment of data protection officers and executive oversight, offering data protection training to staff, establishment of internal complaints handling mechanisms, procedures in the event of security breaches etc. as well as the complete internalisation of privacy in processing operations through privacy by design and default.[58] Nonetheless, the legal nature of the obligation poses a characteristic question - if this list is non-exhaustive, how do regulated entities know what constitutes an adequate adoption of accountability measures? One assessment of the complete legal meaning of accountability under the GDPR assigns accountability components to many of its provisions, viewing the principle as one that pervades the Regulation as a whole.[59] It must be accepted that the nature of this legal rule is not the same as ordinary rules given that it is, after all, a principle. Most of its requirements in practice can be collapsible into specific obligations, just as in the case of the principle of transparency.[60] It is difficult to gauge the likelihood of residual, as-yet-unidentified obligations arising from the principle without allowing for further developments in practice and before courts.

---

[57] *See*, for instance, Centre for Information Policy Leadership (n 54) 19 (viewing accountability measures as "*essential prerequisites for trust in technology, systems and the digital market place*"); *See also*, Sebastian le Cat, 'GDPR Top Ten: #2 Accountability Principle' (*Deloitte*) <https://www2.deloitte.com/ch/en/pages/risk/articles/gdpr-accountability-principle.html#> accessed 30 March 2019 ["*(Accountability) implies a cultural change which endorses transparent data protection, privacy policies & user control, internal clarity and procedures for operationalising privacy and high level demonstrable responsibility to external stakeholders & data protection authorities*."].

[58] Article 29 Data Protection Working Party, Opinion 3/2010 (n 53), para 41; UK Information Commissioner's Office, 'Accountability and Governance' <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/> accessed 30 March 2019.

[59] Nymity, 'GDPR Accountability Handbook 2018' 8-67, <https://info.nymity.com/hubfs/Landing%20Pages/GDPR%20Handbook/Nymity-GDPR-Accountability-Handbook.pdf> accessed 30 March 2019 (tabulating a complete view of potential accountability measures for all relevant GDPR obligations).

[60] Srikrishna Committee Report (n 30) 58, 59 (noting that transparency is incumbent throughout the lifecycle of any data processing activity but also identifying specific obligations such as notice, acknowledgement of requests and publication of privacy policies).

This brings us to the second prong of the accountability principle and possibly the focal point of the obligation as a whole: the ability to demonstrate compliance. As has been discussed at length above, the entire regulatory approach for data protection must be seen in light of the unique informational considerations involved in establishing the incidence of harm (which can be in the form of uncertain, diffused threats) and further tracing the causation for the harm to the relevant entities handling personal data (which can often be done in digital format with ephemeral traces). If the first prong of the accountability principle is about the creation of a culture of privacy across and inside organisations, the ability to detect the growth or stunting of this culture is not an easy regulatory burden for any public agency to carry.

The significance of the second prong can thus be encapsulated in this statement: "*[r]esponsibility and accountability are two sides of the same coin and both essential elements of good governance. Only when responsibility is demonstrated as working effectively in practice can sufficient trust be developed*."[61] In a running theme from the discussion of co-regulation in the section above, one may note that a significant method of demonstrating compliance with the broad principles of a general data protection law is to adopt and comply with a specialised code of practice (eg compliance with a code of practice for the insurance sector on data storage can elaborate on a general rule in a data protection law that data may be stored for as long as is 'necessary' for a specified and legal purpose). Thus, various provisions of the GDPR explicitly state that "*adherence to approved codes of conduct… may be used as an element by which to demonstrate compliance…*".[62] It would appear that the demonstration of compliance can involve various aspects. A key first step to compliance would be the identification of specific standards that are applicable in one's industries since it might be a more fraught enterprise to go about demonstrating compliance with a broad vague standard or principle as are found throughout general data protection laws. The formulation and adoption of internal policies may also go some way in demonstrating the seriousness with which an organisation has gone about aligning its specific processing operations and priorities with data protection requirements. At the very least, it demonstrates application of mind as to the ways in which the general legal rules relate to the specific contexts of

---

[61] Article 29 Data Protection Working Party, Opinion 3/2010 (n 53) para 21 (in discussing the choice of 'accountability' for the terminology for the principle).

[62] *See*, GDPR, arts 24(3), 28(5), 32(3) and 35(8). In contrast, the Srikrishna Committee Draft Bill uses a cautious negative phrasing: "*Non-compliance … with any code of practice … may be considered … while determining whether … [a] data fiduciary or data processor has violated the provisions of this Act*." (*See*, Draft PDPB 2018, cl 61(7).

processing by the organisation, aiding official interpreters of the rules along the way. Finally, it is clear that accountability must involve the maintenance of documentation or records. As one source declares, following the explicit inclusion of accountability in the GDPR, organisations are to "*[m]aintain more extensive records of their processing activities*" and that"*[t]his should include the purposes of the processing, the nature of the data, categories of recipients, the categories of data subjects, any transfers of personal data abroad, including documentation of suitable safeguards, timelines for erasure of data, and a general description of the technical and organizational security measures applied to the processing activities*".[63]

Viewed in this manner, the second prong does indeed look like a cross between a record-keeping requirement and a superadded burden of proof rule. This is precisely the way the Srikrishna Committee came to view the provision and this is despite there being explicit references (in the Committee's Draft Bill) to a burden of proof on the data controller/fiduciary only in the context of consent requirements.[64] After all, if compliance with the accountability principle itself ever comes up for adjudication, the evidentiary processes involved in establishing the ability to demonstrate compliance may in practice be very similar to evidentiary rules regarding a burden to prove compliance. However, what constitutes the satisfaction of this burden may at times appear unclear until there is further judicial development in the precision of our understanding of this general principle.

In light of the foregoing discussion regarding the significance of informational burdens and the difficulty of detection of data protection violations, it is considerably unfortunate that the new Bill tabled in Parliament has entirely omitted the second prong of accountability, retaining only the first prong.[65] This is certainly troubling because it may mean that the ordinary rules regarding burden of proof in evidence law for civil disputes would be applicable in data protection as well. The actual outcome of any litigation would likely be very different under the new Bill's version of accountability. If any account is taken at all as to which party has better access to evidence in a data protection dispute, some obligation regarding the ability to demonstrate compliance must be put in place.

---

[63] Hannah Crowther, 'The GDPR's Accountability Principle: A Shift in Mindset' (*Dropbox*, 20 March 2018) <https://blog.dropbox.com/topics/product-tips/gdpr-accountability-principle> accessed 2 April 2019.

[64] Srikrishna Committee Report (n 30) 164; *See also*, Draft PDPB 2018, cl 12(4) (for the provision regarding burden of proof for consent).

[65] PDPB 2019, cl 10; the Draft Bill from the Srikrishna Committee had specified that the data fiduciary "*should be able to demonstrate that any processing undertaken by it or on its behalf is in accordance with the provisions of this Act*" [Draft PDPB 2018, cl 11(2)].

B. Responsive Regulation

In critiquing the idea of co-regulation many commentators have held up an alternative model for regulation which also received the Srikrishna Committee's stamp of approval - responsive regulation.[66] However, as has been explained above, co-regulation needn't involve any significant abdication of state functions at all and may only be a method of remaining sensitive to industry practices and nuances while relying on private resources for enforcement. Responsive regulation, as shall be described below, can easily complement and act in synergy with a system containing limited co-regulatory features.

Over a couple of decades the concept of responsive regulation has received a considerable fillip as it has gained greater recognition and application.[67] The core idea behind the approach is that "*governments should be responsive to the conduct of those they seek to regulate in deciding whether a more or less interventionist response is needed*".[68] Most accounts of the theory visualise a pyramid or hierarchy of enforcement tools lying on a spectrum of strictness along which a regulator can escalate so as to ensure that "*[t]he magnitude of escalation and the punitive effect of the regulatory response corresponds to the nature of default*".[69] Thus, a one-time, inadvertent and minor breach can be dealt with quite differently from a grave and intentional violation affecting key rights or large numbers. In escalating order, the regulator can seek information, provide informal guidance, require audits, direct mitigation measures, publicly 'name and shame' an entity, demand undertakings, cause investigations and apply penalties or initiate criminal action.

Since none of the tools in the regulator's toolkit are supposed to be legally excluded in the context of any regulatory action, proponents see the approach as a key method to target enforcement actions effectively. The theory has many merits. For one, it has close linkages to robust democratic ideals of deliberative accountability. Braithwaite argues that responsive theories bring

---

[66] *See*, for forceful defences of the responsive approach for India, Greenleaf (n 21) 22-23; Beni Chugh and others, 'Effective Enforcement of a Data Protection Regime: A Model for Risk-Based Supervision Using Responsive Regulatory Tools' Dvara Research Working Paper Series No. WP-2018-01 (July 2018) <https://www.dvara.com/blog/wp-content/uploads/2018/07/Effective-Enforcement-of-a-Data-Protection-Regime.pdf> accessed 2 April 2019.

[67] For one survey of applications of the theory in practice in Australia and the rest of the world, *see*, Mary Ivec and Valerie Braithwaite, 'Applications of Responsive Regulatory Theory in Australia and Overseas: Update' RegNet Research Paper No. 2015/72 (March 2015).

[68] John Braithwaite, 'Responsive Regulation and Developing Economies' (2006) 34(5) World Development 884, 886.

[69] Chugh (n 66) 9.

democracy to bear on a larger swathe of the population, ensuring that the interpretation of rules is done within a system of "*networked governance*".[70] Similarly, the idea of responsive regulation also appeals to our deepest intuitions regarding justice and align well with the principle of proportionality in areas as diverse as constitutional, commercial and criminal law.[71]

However, in the context of the present study, a significant feature of responsiveness is the manner in which it streamlines regulatory action so as to target and respond to violations with a solid system of prioritisation in place at the outset. The regulatory state is not usually in the business of regulating cultures but when it does descend to fiddling around in such matters, it needs at hand an appropriate theory of regulation that provides it with the ability to credibly and legitimately create the threat of strict measures without actually imposing the same unless the situation warrants. Otherwise, the burden of welding together a privacy culture may prove too heavy for an effective attempt to even be made. As pointed out by Ayres and Braithwaite:[72]

> A fundamental principle for the allocation of scarce regulatory resources ought to be that they are directed away from companies with demonstrably effective self-regulatory systems and concentrated on companies that play fast and loose.

The ideas and concepts behind responsive regulatory theory have already filtered through into data protection far deeper than one might at first imagine. McGeveran enthusiastically points out that responsive regulation in the context of privacy holds many benefits including the retention of flexibility to deal with changing technology, the cost-effective discharge of

---

[70] Braithwaite (n 68) 884-886 (Braithwaite views different actors in a system of regulation acting in "*reflexively related systems*" that affect each other's behaviour simultaneously and finds that abuse of power is "*best checked by a complex plurality of many separated powers*", whether private, public or a hybrid of the two).

[71] See, *K.S. Puttaswamy v Union of India* (2017) 10 SCC 1, para 310 ("*Proportionality is an essential facet of the guarantee against arbitrary State action because it ensures that the nature and quality of the encroachment on the right Is not disproportionate to the purpose of the law.*"); *Excel Crop Care Ltd. v CCI, Competition Commission of India* (2017) 8 SCC 47, para 92 ("*[T]he penalty cannot be disproportionate and it should not lead to shocking results. That is the implication of the doctrine of proportionality which is based on equity and rationality.*"); Andrew von Hirsch, 'Proportionality in the Philosophy of Punishment' (1992) 16 Crime and Justice 55; proportionality also features prominently in data protection law in the context of the various balancing tests that it envisages [*see*, for instance, discussions in Article 29 Data Protection Working Party, Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC (2014)].

[72] Ayres and Braithwaite (n 46) 129 (discussing this advantage in the context of "*enforced self-regulation*"); *See also*, Braithwaite (n 68) (providing serious discussion of responsive regulatory theory in the context of capacity deficits in the developing world).

oversight duties and the consequent improvement of real world data practices.[73] Similarly, the UK's Information Commissioner's Office, arguably the leading data protection regulator in the world, makes clear in its regulatory action policy that a system of prioritisation and pragmatism is key to how it sees its own effective functioning:[74]

> [A]s issues or patterns of issues escalate in frequency or severity then we will use more significant powers in response. This does not mean however that we cannot use our most significant powers immediately in serious or high-risk cases where there is a direct need to protect the public from harm. Our approach will also encourage and reward compliance. Those who self-report, who engage with us to resolve issues and who can demonstrate strong information rights accountability arrangements, can expect us to take these into account when deciding how to respond.

In light of these developments around the world, including in developed countries with considerable state capacity, it may be justified for India to also adopt a responsive approach to data protection regulation. Indeed, the Srikrishna Committee has approved of the approach in its Report.[75] Understandably, though the Committee's Draft Bill does not contain any explicit legal mandate for the proposed regulator to take a responsive approach, the entire toolkit of powers that may be applied by the regulator appears to have been provided for.[76]

One matter that we must remain cognizant of is that a responsive approach carries with it a requirement that the regulatory authority be granted adequate discretion to be able to carry out the dynamic, context-sensitive enforcement actions that such a method entails. While the perils of regulatory discretion are well known, there is also evidence to suggest that it is a key requirement in the context of limited regulatory capacity.[77] Such findings

---

[73] McGeveran (n 27).

[74] UK Information Commissioner's Office, Regulatory Action Policy, 13 <https://ico.org.uk/media/about-the-ico/documents/2259467/regulatory-action-policy.pdf> accessed 2 April 2019; similarly, the UK Information Commissioner has declared: "… *I hope by now you know that enforcement is a last resort. I have no intention of changing the ICO's proportionate and pragmatic approach after 25th of May. Hefty fines will be reserved for those organisations that persistently, deliberately or negligently flout the law.*" [Denham (n 43)].

[75] Srikrishna Committee Report (n 30) 156-158.

[76] Power has even been specifically provided to engage in reputational sanctions through a 'name and shame' approach [Draft PDPB 2018, cl 60(2)(*w*)].

[77] *See*, Esther Duflo and others, 'The Value of Regulatory Discretion: Estimates from Environmental Inspections in India' (*MIT Economics*, 10 March 2018) <https://economics.mit.edu/files/10335> accessed 2 April 2019 (finding, in the context of environmental regulation, that random inspections reveal fewer extreme violators than inspections on the

are also corroborated in the context of other regulatory fields with broad coverage. As it happens, the growth of prioritisation approaches may also be seen in that other significant cross-sectoral regulatory mandate - competition regulation.[78]

It is understandable that we should be wary of unguided discretion in any context but the essential take away from the above discussion must be that we have to create workable systems for granting regulatory discretion in data protection while maintaining systems by which to check and guide this discretion. This is a core enterprise for Indian administrative law which seems to have had an over-emphasis on flexibility, pragmatism and adaptation and a concomitant failure to consolidate into a unified legislation with minimum standards for administrative processes such as in the US Administrative Procedure Act.[79]

An allied area of study is the question of the independence and functional integrity of a data protection regulator. This has been an important area of debate in the context of any proposed Data Protection Authority for India[80] and while it is not the subject matter of this Article, it is nonetheless a crucial problem that scholars and practitioners should direct their energies towards. For the purposes of our discussion on responsive regulation, however, one may see significant need for statutory checks on the most significant discretionary functions of a data protection regulator. In this matter, a data

---

basis of a regulator's discretion and noting the resonance of their findings with literature on limited regulatory capacity at n 6).

78 Raeesa Vakil, 'Indian Administrative Law and the Challenges of the Regulatory State' in Devesh Kapur and Madhav Khosla (eds), *Regulation in India: Design, Capacity, Performance* (Hart Publishing, 2019) 51.

79 Raeesa Vakil, 'Indian Administrative Law and the Challenges of the Regulatory State' in *Regulation in India: Design, Capacity, Performance* (Kapur & Khosla eds.) (Hart Publishing, 2019) 51.

80 Key to the debate have been the provisions in Draft PDPB 2018, cls 68 and 98 (on the appointment of adjudicating officers and government directions to the proposed regulator); to add to these problematic provisions, the new Bill tabled in Parliament has acceded even more control to the Government by allowing it to have exclusive control over surveillance activities and a stranglehold on the selection committee of the DPA [PDPB 2019, cls 35 and 42(2)] (for examples of concerns regarding of the same, *see*, Graham Greenleaf, 'GDPR-Lite and Requiring Strengthening – Submission on the Draft *Personal Data Protection Bill* to the Ministry of Electronics and Information Technology (India)' UNSW Law Research Paper No.18-83 (2018), at 2, 3 and 11; UK India Business Council, 'Data: The Foundation of Intelligent Economies' (March 2019) 29 <https://www.ukibc.com/data-the-foundation-of-intelligent-economies/> accessed 2 April 2019; *Access Now* (n 45) 10; Amba Kak, 'The Emergence of the Personal Data Protection Bill, 2018: A Critique' (2018) LIII (38) Economic & Political Weekly 12, 14-15); *See also*, for European case law on the level of independence required for data protection authorities, *European Commission v Federal Republic of Germany,* 2010 ECR I-1885, C-518/07 (CJEU) and *European Commission v Republic of Austria*, C-614/10 (CJEU).

protection statute can be seen as a contract that serves to manage the relationship between an independent regulatory authority and an elected government that is directly subject to democratic accountability.[81] One may thus note the attempts made in the Srikrishna Committee's Draft Bill to guide the discretionary functions of the DPA through various prescriptive criteria, for example, in provisions regarding consent and explicit consent (Clauses 12(2) and 18(2)), reasonable purposes (Clause 17(1)), the designation of further categories of sensitive personal data (Clause 22(2)), the right to be forgotten (Clause 27(3)), the classification of significant data fiduciaries (Clause 38(1)), and the determination of penalties and their amounts (Clause 74(4)), as well as through an illustrative list defining the concept of a privacy harm (Clause 3(21)). Other mechanisms that may appear less principle-based but potentially effective are to embed clear mechanisms by which to carry out cost-benefit analyses that are reviewable by courts on a consistent basis.[82] The merits of systematically studying the varieties of privacy harms may be of great significance here, including the recognition of diffused and cumulative harms that are easy to undervalue.

There will be no easy answers to questions regarding how we can balance the grant of discretion and independence with the requirements of constraining executive action for public good and ensuring democratic accountability. Cohen describes navigating the tension as "*charting a course between the Scylla of regulatory capture and the Charybdis of bureaucratic inefficiency*".[83] If and when regulatory practice on data protection proceeds in India, a close eye will have to be kept to ensure that decisions are made with adequate and explicit reasons that are themselves consistent across measures, sectors, entities and individuals. This kind of scrutiny of the functioning of our regulatory authorities may be the only way to marry discretion with efficiency and the protection of our rights.

V. An Eye to the Future

This study has sought to elaborate on the key unique considerations involved in designing a scheme for data protection regulation that can adequately

---

[81] For a detailed view of the considerations involved in taking this view, *see*, Roy (n 3) (treating the legislature represented by the executive as the principal and the regulatory agency as the agent in a classic principal-agent problem in which the necessary discretion of the agent needs to be constrained by employing optimal information and incentive structures).

[82] Eric A. Posner, 'Controlling Agencies with Cost-Benefit Analysis: A Positive Political Theory Perspective' (2001) 68 University of Chicago Law Review 1137; Michael A. Livermore, 'Cost-Benefit Analysis and Agency Independence' (2014) 81 University of Chicago Law Review 609.

[83] Cohen (n 10) 392.

match up to the weighty task at hand. Even after one considers all the exemptions that a data protection law usually provides for, there remains a vast array of entities that any future regulator will have to engage with. In all likeliness, data protection regulation has the widest regulatory mandate in terms of the coverage of entities and volume of transactions and functions that any regulator has ever had to take on, even considering authorities in financial and competition regulation. A successful attempt at taming the roving eyes of public and private surveillance will need more than just clever ideas, however. The project requires a serious look at the unique characteristics of personal data, informational flows and privacy harms. As has been argued above, the most significant regulatory considerations in the regulation of personal information will be informational considerations - answers to the problem of how best an agency can gather the regulatory information needed to protect personal information.

One set of information that will be needed is on-ground awareness of the ordinary practices that computer professionals employ when operating in the information economy. Apart from developing ecosystems and networks of privacy professionals with whom a regulator may engage, an important method of creating a credible threat of the detection of violations may be the initiation of schemes for whistle-blowers who may be willing to call out the illegalities of their organisation as well as the formal institution of whistle-blower awards.[84] Other avenues for the amelioration of informational concerns include the development of awareness regarding data protection amongst individuals generally and the growth of a body of research around how best to create technical safeguards for privacy as well as develop technological solutions to regulatory problems. Unlike in many other instances of Indian regulatory practice, there cannot be any devaluation of regulatory functions like awareness generation and research.

Active support and encouragement must also be given to public interest or consumer interest groups willing to organise and examine the data economy from vantage points other than commercial ones. If we want to look forward to a future where data principals/subjects in India are ready and able to defend their own privacy, the sharing of enforcement burdens cannot just be with regulated entities but also with the persons who are to be protected under the law. Illiteracy, innumeracy and the lack of technical knowledge on data processing may always be concerns going forward but

[84] For a robust scheme developed in this regard in the field of securities regulation (a field with similar difficulties in detection and investigation), *see*, U.S. Securities and Exchange Commission, Office of the Whistleblower <https://www.sec.gov/whistleblower> accessed 2 April 2019.

the entire project of data protection can be streamlined towards the activation of individuals themselves. The evolution of regulatory practice appears to be moving from prescriptive rules, certification and gatekeeping towards the promotion of innovation in an environment of data-driven transparency and accountability.[85] While the traditional scheme of paternalistic regulation seemed appropriate for a time when information was *scarce*, regulatory action can today be bolstered not just with co-regulation but also with collaborations riding on consumer and citizen activism so long as the individual is allowed to know about the future they are being thrust into. This must mean transparency on the part of regulated entities but it also requires the systematic and comparative presentation of the information needed to allow for good choices in a data economy inundated with *too much* information. Hopefully, systems such as data trust scores and consent dashboards can play a role here.[86]

A word of caution is appropriate. While the anxieties of the information age are appropriately regarding the dangers that our liberties face against the unending storm of technological innovation, it is possible that we are anxious only because we do not yet understand what we are dealing with. In 1865, the British Parliament demanded that automobiles travel at 4 miles per hour on highways and 2 miles per hour in towns and villages, that they be manned by crews of at least three persons and that one person walk 60 yards ahead of the vehicle with a red flag to warn everyone of what was coming. Though the time the law was repealed in 1896, the development of automobiles had been stifled as a result.[87] While the anxiety provoked by change is understandable, the method by which we build a society that can trust technology should not strangle innovation to death either.

And yet, as data protection law develops, it may not end up looking anything like what we might see in most areas of legal and regulatory practice. We should be ready to live with such uncertainty but we should accept change only where it promotes human welfare. Cars may carry the weight of our bodies and computers the weight of our secrets, but no one can claim that both weigh the same.

---

[85] Parker (n 4) 253-256.
[86] Srikrishna Committee Report (n 30) 36.
[87] Eggers (n 6).