BOOK REVIEW

PRIVACY 3.0: UNLOCKING OUR DATA-DRIVEN FUTURE BY RAHUL MATTHAN

*Amlan Mishra**

This review analyses Rahul Matthan's book titled "Privacy 3.0: Unlocking our data-driven future". It discusses three key ideas advanced by Matthan in the book: (i) the conception of privacy and privacy law, as one which is constantly shaped by technological changes; (ii) the critique of the Indian privacy policy, as one shaped by the Indian bureaucracy; and (iii) the need to transcend 'consent' as the core idea of privacy and explore new principles.

First, this review critiques the dialectic, context-specific relationship between privacy law and technology which forms a crucial component of Matthan's account of privacy. The critique highlights that privacy should not be comprehended in a manner that undermines the normative conceptions of privacy. Second, the book's critique of the privacy policy in India is examined by undertaking an analysis of the court decisions and the privacy regime in India. Lastly, the suggestion of the author to "transcend the consent standard", is sought to be understood in the context of the contemporary scholarship and court decisions regarding the same. In addition, the provisions of the Data Protection Bill, 2019 have been weighed against the insights of the book.

* Amlan Mishra is a 3rd year B.A., LL.B. (Hons.) student at National Law University, Jodhpur. He may be contacted at amlanmishra1999@gmail.com.

CONTENTS

INTRODUCTION

The years of 2017 and 2018 have brought the right to privacy to the fore of constitutional jurisprudence in India. The debate regarding the constitutional status of the right to privacy was reignited when the then Attorney General, Mukul Rohatgi, submitted during the hearing of the constitutional validity of the Aadhaar scheme that the right to privacy was not recognised in India.[1] While a nine-judge bench of the Supreme Court in *K.S. Puttaswamy v. Union of India* (hereinafter "*K.S. Puttaswamy*"), held that privacy is a fundamental right under the Indian Constitution,[2] there is a lack of doctrinal clarity regarding the scope of

[1] Utkarsh Anand, *Where's right to privacy? You decide, Govt tells Supreme Court*, The Indian Express (July 23, 2015), https://indianexpress.com/article/india/india-others/wheres-right-to-privacy-you-decide-govt-tells-sc/ (last visited May 1, 2020).
[2] K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.

this right, and how it extends to data privacy in this data-driven age.[3] Thus, it becomes germane to develop scholarship regarding the contours of the right to privacy in the Indian context. Rahul Matthan, in his book titled "*Privacy 3.0: Unlocking our data-driven future*", makes an attempt to comprehend the scope of the right to privacy in India.[4]

The book adopts a narrative-building, story-telling approach instead of a terse, academic style. The book focuses on the unexplored issues in the Indian privacy regime such as the dialectic relationship between technology and privacy; the failure of the Indian bureaucracy to take privacy seriously; and the potential solutions to address the challenges to privacy posed by the data-driven age.

Matthan has been a technology, media, and telecom (TMT) lawyer for over two decades and used to serve on the management committee (MC) of the Indian law firm called Trilegal. He has recently stepped down from the MC and moved to the supervisory board of Trilegal. The book is a testament to his experience in helping the Indian business industry navigate the hotchpotch of Indian technology laws. Using his professional expertise, Matthan provides insights into how a healthy concern for privacy is crucial to unlocking India's data-driven potential. He also draws from his experience with the Indian bureaucracy in drafting an approach paper on privacy laws in collaboration with the Department of Personnel and Training to highlight India's bureaucratic inefficiencies in dealing with privacy issues.

The book makes three main arguments. It seeks to give narrative shape to the conception of privacy and privacy law, as one born out of and shaped in response to the putative dangers posed to the right to privacy by the emerging digital technology in the society (discussed in Part I and II of this review). The strongest contribution of the book lies in its critique of the policy paralysis that plagues the executive branch of the Indian government and how that has led to a piecemeal development of the privacy laws (discussed in Part III). Furthermore, the book makes the case that the Indian privacy regime must transcend 'consent' as a standard informing the notion of privacy and develop other robust principles (discussed in Part IV). These complex arguments have been explained lucidly in the book. Before delving into the critique of the book, it is important to set out the context of the notion of privacy in order to assess the book's contribution to the existing literature.

[3] Apar Gupta, *Balancing Online Privacy in India*, 6 INDIAN J. L. & TECH. 43, 62 (2010).
[4] RAHUL MATTHAN, PRIVACY 3.0: UNLOCKING OUR DATA-DRIVEN FUTURE (2018).

I. CONCEPTUALISING PRIVACY

Theories of privacy across the world have attempted to isolate the 'essence' of privacy in order to understand its conceptual underpinnings. In the United Kingdom, the *Semayne* case decided in 1604, authoritatively declared the essence of privacy through the paradigm of property in the following terms: "*a man's house is his castle*".[5] Therefore, early privacy violations involving private correspondences were sought to be covered under copyright laws.[6] Later, Warren and Brandeis, in their seminal writing, proffered that the 'inviolate personality' of a human is the essence of privacy. Accordingly, they sought to move the conceptualisation of privacy away from the perspective of 'property' to 'personhood'.[7] Others have sought to understand privacy as 'secrecy' in terms of avoiding the revelation of personal information to others.[8] Several cases on abortion rights, relying on the centrality of bodily integrity, have linked the notion of privacy with the 'dignity' of an individual.[9]

The above characterisations highlight that privacy has several dimensions. Privacy violations have no common denominator. Hence, it is not theoretically possible to isolate the 'essence of privacy'.[10] An apt theorisation of the right to privacy has been provided by Daniel Solove which entails reviewing privacy concerns from the standpoint of a 'pragmatist'.[11] Solove creates a new taxonomy of privacy wherein 'family resemblances' between different privacy issues are used to conceptualise an account of privacy based on actual practices.[12] For instance, the problem of *information processing* poses different concerns than the challenges created by *information collection* or bodily *invasion*.

---

[5] Peter Semayne v. Richard Gresham, 77 Eng. Rep. 194, 195 (K.B. 1604).
[6] Ronan Deazley, *Commentary on Pope v. Curl (1741)*, in PRIMARY SOURCES ON COPYRIGHT (1450-1900) (L. Bently & M. Kretschmer eds., 2008).
[7] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4(5) HARV. L. REV. 193 (1890).
[8] RICHARD A. POSNER, THE ECONOMICS OF JUSTICE 272-73 (1981); *See* in the Indian context, District Registrar v. Canara Bank (2005) 1 SCC 496, 523, which held that bank records remain confidential vis-à-vis the person, even though they are made known to the bank, and thus, it cannot be further publicised without consent.
[9] Griswold v. Connecticut, 381 U.S. 479 (1965); Roe v. Wade, 410 U.S. 113 (1973); *See* in the Indian context, Selvi v. State of Karnataka (2010) 7 SCC 263, which recognised that the inviolability of human dignity is hindered, when polygraph test is administered.
[10] DANIEL SOLOVE, UNDERSTANDING PRIVACY 6, 46 (2008).
[11] DANIEL SOLOVE, UNDERSTANDING PRIVACY, 101-171 (2008).
[12] Solove's taxonomy consists of four principal groups: (1) information collection; (2) information processing; (3) information dissemination; and (4) invasion. Each group encompasses a variety of activities that can create privacy concerns.

This review attempts to underscore that while Matthan attempts to utilise this 'pragmatist' approach to privacy, his account of privacy disproportionately emphasises on context-specificity. This is exemplified by the fact that Matthan believes that the privacy laws and the permissibility of restrictions on privacy should change with contexts. As will be demonstrated later, it is here that his account differs from Solove's conception of privacy, who advocates that though privacy problems ought to be understood in their specific contexts, the law devised to deal with the same should incorporate normative standards.

A. Legal Standards for Privacy Violations

Broadly, two tests are adopted in most constitutional democracies to weigh privacy violations: (i) the proportionality test; and (ii) the reasonable expectation of privacy test.[13] The proportionality test,[14] which has also been adopted by the Indian Supreme Court,[15] evaluates whether the governmental measure is the 'least restrictive way' of achieving the legitimate goal. Thus, if the same goal can be achieved using a less infringing measure, then the law will be declared unconstitutional.[16] It is important to note that the concept of 'societal expectation of privacy' is not a part of the proportionality test. The proportionality test incorporates a normative standard rather than a socio-empirical standard that entails taking into account the public perception of reasonability of a particular restriction.[17]

On the contrary, the 'reasonable societal expectation of privacy test', which is widely accepted in the United States (hereinafter "US"), incorporates "*a twofold requirement, first that person [has] exhibited an actual (subjective) expectation of privacy and, second, that the expectation [is] one that society is prepared to recognize as 'reasonable'*."[18] It is apparent that this test is more responsive to technological and social changes which may influence the perceptions of individuals.[19] Along the lines of the reasonable expectation test, proponents of the Aadhaar scheme have

[13] Gautam Bhatia, *Aadhaar Judgement and the Constitution- I*, Indian Constitutional Law and Philosophy Blog (September 30, 2018), https://indconlawphil.wordpress.com/2018/09/28/the-aadhaar-judgment-and-the-constitution-i-doctrinal-inconsistencies-and-a-constitutionalism-of-convenience/ (last visited May 2, 2020).

[14] The proportionality test has four prongs: (i) the restriction has a legitimate state goal; (ii) there exists a rational nexus between the restriction and the goal; (iii) the restriction should be necessary and the least restrictive way of achieving the goal; and (iv) the need for a balancing exercise to enquire whether the cost of infringement is disproportionately high vis-à-vis the public purpose.

[15] *See* K.S. Puttaswamy, at paras. 509, 632.

[16] In K.S. Puttaswamy v. Union of India II, (2018) SCC Online SC 1642, the petitioners contended that smart cards were less restrictive than Aadhaar cards.

[17] DANIEL SOLOVE, UNDERSTANDING PRIVACY 72 (2008).

[18] Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

[19] Lior Jacob Strahilevitz, *A Social Networks Theory of Privacy*, 72 U. CHI. L. REV. 919, 937 (2005).

argued that privacy is an elitist construct which has no 'reasonable necessity' in a society which struggles with food security.[20] As I explain later, Matthan accepts the Aadhaar scheme as necessary for preventing corruption and improving efficiency. While Matthan does not discuss its proportionality, he seems to have accepted the 'reasonable expectation of privacy' test.

B. Government Intervention in Regulation

Theories of privacy regulation vary between two polarities of 'free market' and 'complete governmental regulation'. The allure of the 'free market' theories is that they are driven by concerns about customer confidence and publicity.[21] Companies pride themselves on their privacy features with an aim to attract more customers. It is apparent that the underlying concern of these theories lies in addressing the huge asymmetry of information between the data controller and the data subject.

On the other hand, governmental regulation theories propose a 'complete' intervention by the government as the solution to privacy concerns. However, the lack of industry experience of the government officials may make the rules framed by such regulators untenable and undermine the innovation efforts of the industry.[22]

A third path of 'self-regulation' by the industry presents itself in this context. An industry created body may make rules and policies and ensure compliance with the rules by the members of the industry.[23] The industry bodies can develop mechanisms to ensure industry compliance as per the expectations of the consumers. This approach allows industry experts to devise rules by taking into account the dynamics of the industry. In some contexts, self-regulation has resulted in the creation of ecosystems of compliance through the training of industry peers in the best privacy practices.[24]

However, across the world, complete self-regulation finds very few takers. In the European Union, the privacy laws provide for a designated, statutory regulator, as industry

[20] Harish V Nair, *Aadhaar hearing: Right to life of poor more important than elite class' privacy concerns, says Centre,* India Today (July 27, 2017), https://www.indiatoday.in/mail-today/story/aadhaar-hearing-privacy-supreme-court-1026499-2017-07-27 (last visited May 2, 2020).
[21] Peter Swire, *Markets, Self-Regulation, and Government Enforcement in the Protection of Personal Information*, in PRIVACY AND SELF-REGULATION IN THE INFORMATION AGE (US Dep't of Commerce, 1997).
[22] *Id.*
[23] Henry H. Perritt, Jr., *Regulatory Models for Protecting Privacy in the Internet*, in PRIVACY AND SELF-REGULATION IN THE INFORMATION AGE (US Dep't of Commerce, 1997).
[24] *Id.*

self-regulation has been historically perceived as an invitation to corruption.[25] Countries like Canada have adopted a co-regulatory model whereby the industry develops 'enforceable standards' that are overseen by a privacy agency of the government.[26] Matthan believes that some variant of self-regulation coupled with minimum government oversight should be encouraged given the red tape in the Indian bureaucratic set-up.

II. THE RELATIONSHIP OF PRIVACY WITH TECHNOLOGY AND SOCIETY

In the first part of the book, Matthan builds a dialectic narrative of how the conception of privacy was born out of technology and consequently, shaped by it. The early humans, it is argued, did not have any conception of privacy. In fact, privacy was deemed to be not just "*unacceptable, but dangerous*".[27] Humans wanted to herd together in order to meet the needs of the population for security and food.[28] Matthan relies on sociological studies to contrast our fixation with privacy with the absence of this idea in ancient societies. Matthan argues that this apathy to privacy reached a tipping point when walls were discovered. Walls, as per Matthan, "*facilitated self-expression in a way humans had never experienced before.*"[29] The Western religious traditions with their focus on seclusion as a prerequisite for private communication with God, encouraged individualism which highly valued privacy.[30] Thus the concept of privacy is portrayed as alien to natural creation, arising out of a human quest for creativity, imagination, and similar activities of solitude.[31]

How does technology shape human society once walls allow for the consciousness of privacy? Matthan marshals early cases of privacy in common law to show how the courts conceptualised the right to privacy in response to the inventions of the printing press, yellow journalism, and cameras.[32] For instance, the first authoritative work on privacy by Warren and Brandeis is written as a response to the growth of photography in the West.[33] The article

[25] Barbara Crutchfield George et al., *U.S. Multinational Employers: Navigating Through the "Safe Harbor" Principles to Comply with the EU Data Privacy Directive*, 38 AM. BUS. L. J. 735, 743 (2001).
[26] David Banisar & Simon Davies, *Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments*, 18 J. MARSHALL J. COMPUTER & INFO. L. 1, 13-14 (1999).
[27] MATTHAN, *supra* note 4, at 7.
[28] MATTHAN, *supra* note 4, at 11.
[29] MATTHAN, *supra* note 4, at 18.
[30] MATTHAN, *supra* note 4, at 22.
[31] MATTHAN, *supra* note 4, at 24.
[32] MATTHAN, *supra* note 4, at 27-56.
[33] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 197 (1890).

reflects deep concern about the circulation of photographs and personal documents made possible by modern technology.[34] The article is pivotal as it propounds the conception of an 'inviolate personality' of a human being as the basis for privacy rights and thereby rejects the earlier notion of 'physical places/property' as the foundation for privacy rights.[35] One of the authors of the article later became an Associate Judge of the US Supreme Court and dissented in *Olmstead v. US*.[36] Brandeis, J., in his dissenting opinion, held that the 'inviolate personality' of a human being and not his 'physical property' was the subject of protection under the Fourth Amendment of the US Constitution which imposes a prohibition on illegal search and seizures.[37]

Matthan traces a similar evolution of the right to privacy in India by drawing on the Indian Court decisions regarding DNA use, phone tapping, etc., to demonstrate how the courts reconciled the right to privacy with the use of emerging technology.[38] In *PUCL v. Union of India*,[39] the Supreme Court was confronted with the question of the validity of telephone tapping. The Court, in this case, laid down guidelines that disallow bulk surveillance and impose 'use-restrictions' on the data collected through tapping. Similarly, the courts have allowed DNA testing only in cases of 'eminent need'.[40] Matthan stresses on these cases to underscore that though several technological inventions have raised serious privacy concerns, "*the technology survived and the society taught itself to adjust to account for these challenges*."[41] Thus, he expresses that "*any study of the evolution of privacy law should take place in the context of the technological changes*."[42]

A. Evolution of Privacy: Sacrificing Normativity for Context?

Matthan's narrative seeks to draw a picture of human privacy as one which is highly context-specific and amenable to radical technological changes. However, other scholars have argued that with respect to activities like urination, defecation, and sexual intercourse, humans

[34] *Id.*
[35] *Id.*
[36] Olmstead v. United States, 277 U.S. 438, 478 (1928).
[37] The text of the Fourth Amendment of the US Constitution disallows illegal 'search and seizure' in a physical place.
[38] MATTHAN, *supra* note 4, at 107-108.
[39] PUCL v. Union of India, AIR 1997 SC 568.
[40] Bhabani Prasad v. Orissa State Commissioner for Women, AIR 2010 SC 2851.
[41] MATTHAN, *supra* note 4, at 26.
[42] MATTHAN, *supra* note 4, at 26.

have drawn private boundaries throughout history. Therefore, at least, a part of the human psyche has genetically craved for private spaces irrespective of the context and social conditioning. Even today, in some tribes, who live as hunter-gatherers, privacy of bathing is secured.[43] Thus, Matthan inaccurately attempts to construct a sense of contingency and fluidity in privacy values which has never existed in human society.

However, the overarching theme of the book that privacy laws should evolve in response to particular technological changes is well taken. Recall the discussion in the first part of this review regarding the conception of privacy. Daniel Solove, in 'Understanding Privacy', has similarly sought to conceptualise privacy by using a 'bottom-up' approach based on 'privacy problems' rather than by making generalised assumptions regarding the essence of privacy in isolation.[44] Solove emphasises that it is useful to develop a classification or taxonomy of privacy values based on 'privacy problems' that we encounter. Solove states that inquiry must be "*experimental, making generalizations based on one's encounters with problems, and then testing these generalizations by examining their consequences in other contexts.*"[45]

Does that imply that the normative standards of privacy can be discarded in favour of context-specific evolution of privacy values and privacy laws as suggested by Matthan? According to Solove, while the 'identification and grouping' of these problems ought to be a contextual exercise and therefore, making it responsive to technological change, 'the law' to address these problems should be based on a normative conception of privacy. Solove states that "*we construct laws to bring about a state of affairs we want, not just to preserve existing realities... The law should thus be a tool used proactively to create the amount of privacy we desire.*"[46] The drawback, associated with the context-specific responsiveness to the concerns of privacy is that it may result in individuals voluntarily giving up their privacy without realising the risks involved in surrendering one's privacy.[47] Furthermore, an Orwellian government may gradually condition its people to become normalised to grave violations of privacy.[48] Solove rightly identifies that

[43] *See* Adam D. Moore, *Privacy: Its Meaning and Value*, 40 AM. PHILOS. Q. 215, 221-22, 223 (2003); *See also* John M. Roberts & Thomas Gregor, *Privacy: A Cultural View*, in PRIVACY: NOMOS XIII 199, 203-14 (J. Roland Pennock & J. W. Chapman eds., 1971).
[44] DANIEL SOLOVE, UNDERSTANDING PRIVACY 9 (2008).
[45] *Id.* at 75.
[46] *Id.* at 74.
[47] DANIEL SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 81-92 (2004).
[48] DANIEL SOLOVE, UNDERSTANDING PRIVACY 73 (2008).

"*a theory of privacy should leave room for cultural and historical variation, but not err by becoming too variable.*"[49] Solove believes that in privacy law-making, societal conceptions should have a limited role of 'identifying and grouping' privacy problems.

Thus, Matthan's claim that society and law have changed and should invariably evolve to accept technological changes does not account for the concerns raised by Solove about authoritarianism. Further, it fails to take into consideration the role of law as an instrument to bring about a desirable state of affairs regarding privacy.

B. The Indian Courts on Normativity: From KS Puttaswamy to Aadhaar

I argue here that the Indian courts, with the notable exception of *K.S. Puttaswamy v. Union of India II* (hereinafter "*the Aadhaar case*"),[50] have for good reasons rejected complete contextuality in privacy values by applying the proportionality test. In the *Aadhaar* case, the Supreme Court digressed from its initial position and indirectly attempted to incorporate the standard of the societal expectation of privacy. The Supreme Court, in upholding the larger exercise of the Aadhaar scheme, echoed Matthan's contextuality in dealing with privacy laws.

It is important here to juxtapose the proportionality test with the reasonable expectation of privacy test. As mentioned earlier, the former incorporates a normative standard whereas the latter reflects a socio-empirical standard. In *K.S. Puttaswamy*, Nariman, J., explicitly rejected the application of a socio-empirical analysis in determining the constitutionality of privacy violation.[51] He endorsed a proportionality test over a reasonable expectation of privacy test by characterising the role of constitutional privacy law as the norm-setter. He noted that:

> "*Also, as has rightly been held, the (reasonable expectations) test is circular in the sense that there is no invasion of privacy unless the individual whose privacy is invaded had a reasonable expectation of privacy. Whether such individual will or will not have such an expectation ought to depend on what the position in law is.....Shri Dwivedi's argument (that this test is valid) must, therefore, stand rejected.*"[52]

---

[49] *Id.*
[50] K.S. Puttaswamy v. Union of India II, (2018) SCC Online SC 1642, at ¶342.
[51] K.S. Puttaswamy, at ¶582.
[52] *Id.*

The Court, in the case of *K.S. Puttaswamy*, held that privacy values are not subjective but should "*peg its colours to the mast of the Constitution*."[53] This reflects Solove's understanding that privacy values should be determined by normative standards and should not sway with societal expectations.

The context-driven evolution of privacy law that Matthan proposes for India seems to be the approach of the majority in the *Aadhaar* ruling.[54] Though the majority referred to the normative standard of proportionality in the *Aadhaar* case, it applied the reasonable expectation of privacy test by delving into the question of whether the privacy concern arising due to the Aadhaar scheme was a 'societally reasonable expectation of privacy'.[55] In order to answer it, the Court undertook a 'societal analysis' of privacy and concluded that the information collated under the Aadhaar scheme such as fingerprints, iris scan, is also sought by the government in other contexts such as driving license, passport, visa, etc., as they are "*considered to be the most accurate and non-invasive mode of identifying an individual*." Therefore, the Court held that the privacy interest of individuals in such information is minimal.[56]

In the book, Matthan, similarly, expresses the benefits of the Aadhaar scheme in the Indian context in terms of minimising corruption and leakages. At the same time, he maintains that the negative effects of the Aadhaar exercise cannot be quantified properly.[57] His endorsement of the regime irrespective of the harms implies his preference to settle the privacy concerns posed by the Aadhaar scheme, by taking into account the Indian context of corruption and leakages.

[53] K.S. Puttaswamy, at ¶500.
[54] The Aadhaar case. *See also* Mariyam Kamil, *Aadhaar Judgement and the Constitution- II: On proportionality*, Indian Constitutional Law and Philosophy Blog (September 30, 2018), https://indconlawphil.wordpress.com/2018/09/30/the-aadhaar-judgment-and-the-constitution-ii-on-proportionality-guest-post/ (last visited May 2, 2020).
[55] Gautam Bhatia, *Aadhaar Judgement and the Constitution- I*, Indian Constitutional Law and Philosophy Blog (September 30, 2018), https://indconlawphil.wordpress.com/2018/09/28/the-aadhaar-judgment-and-the-constitution-i-doctrinal-inconsistencies-and-a-constitutionalism-of-convenience/ (last visited May 2, 2020).
[56] The Aaadhaar case, at ¶350.
[57] MATTHAN, *supra* note 4, at 107-108.

III. INDIA'S PIECEMEAL POLICY ON PRIVACY AND NAVIGATING THE INDIAN BUREAUCRACY

One of the most astonishing aspects of the Aadhaar exercise is that it was started without any legislative backing.[58] Later, it was passed as a money bill by the lower house of the Parliament, the Lok Sabha, thereby circumventing the upper house of the Parliament, the Rajya Sabha.[59] This reflects how the loopholes in the legislative and executive branches of the government have been exploited in order to enact a measure that directly concerns the privacy of the individuals. In the second part of the book, Matthan explores the functioning of the Indian bureaucracy when the Aadhaar exercise was in its infancy. Pursuant to his meeting with Nandan Nilekani, the chairman of the Unique Identification Authority of India (UIDAI), a regulatory agency responsible for implementing the Aadhaar scheme, Matthan was tasked with the job of creating an approach paper on privacy laws with the Department of Personnel and Training. Matthan's experience reveals how the bureaucracy which is predisposed to value transparency, struggles with the idea of privacy.[60] Matthan highlights that in a workshop with several departments, each department claimed to have developed its own set of regulations to uphold privacy without addressing the broader need to develop a privacy framework in the national context.[61]

The absence of a comprehensive privacy regime has resulted in the executive tweaking the regulatory understanding of privacy to suit its needs. In 2019, the cabinet approved the DNA Technology (Use and Application) Regulation Bill that permits the government to store a individual's personal data concerning his DNA make-up.[62] In a similar vein, the Ministry of Home Affairs issued a surveillance order which authorises several central agencies to intercept, monitor, and decrypt "*any information generated, transmitted, received or stored in any*

---

[58] Shreeja Sen, *Government narrative on Aadhaar has not changed in the last 6 years: Sunil Abraham*, The Livemint (March 8, 2016), https://www.livemint.com/Politics/l0H1RQZEM8EmPlRFwRc26H/Govt-narrative-on-Aadhaar-has-not-changed-in-the-last-six-ye.html (last visited May 2, 2020).

[59] Suhrith Parthasarthy, *Aadhaar as a money bill,* The Hindustan Times (September 28, 2018), https://www.hindustantimes.com/columns/aadhaar-act-as-money-bill-it-can-lead-to-a-great-deal-of-public-harm/story-Xu3TtHMSXyrrydO4VcBZgM.html (last visited May 2, 2020).

[60] MATTHAN, *supra* note 4, at 122-123.

[61] MATTHAN, *supra* note 4, at 125-126.

[62] The DNA Technology (Use and Application) Regulation Bill, 2019; *See also* Suhrith Parthasarthy, *Towards a genetic panopticon,* The Hindu (December 21, 2018), https://www.thehindu.com/opinion/lead/towards-a-genetic-panopticon/article25791126.ece (last visited May 2, 2020).

computer."[63] This order has a direct bearing on the right to privacy of the individuals in the absence of any regulatory mechanism to deal with privacy violations.[64]

In the dissenting opinion in the *Aadhaar* case, Chandrachud J., expressed concern over the role of the executive and observed that "*unless the law mandates an effective data protection framework, the quest for liberty and dignity would be as ephemeral as the wind*."[65] Even the majority in the *Aadhaar* case looked forward to the implementation of a data privacy framework and took note of the committees appointed for the same purpose.[66] Consequently, a data privacy bill titled the Personal Data Protection Bill was finalised. However, the bill was introduced in the Parliament after mere consultation with 'select stakeholders' and without undertaking any public consultation.[67] At present, it has been referred to a Joint Parliamentary Committee which has invited public comments on the bill.[68]

A. Alternatives to Bureaucratic Regulation

Matthan provides insights into how a privacy regime ought to be developed in order to navigate the inefficiencies of the bureaucracy. He is not in favour of a 'privacy authority' which figures in many privacy regimes across the world,[69] in order to ensure compliance with privacy norms.[70] He proposes a novel "*system of intermediaries, incentivised to operate in the interest of the data subject*."[71] Matthan believes that the technical expertise of such intermediaries would make them better equipped to deal with privacy concerns than the bureaucracy. Their function would be akin to financial auditors as they would audit the data practices of the data controllers in order to allow these controllers to remedy the deficiencies in their practices. The auditors would assign ratings to different companies based on their practices. He proposes

---

[63] Ministry of Home Affairs Order No.14/07/2011-T, 2018, THE GAZETTE OF INDIA (2018), pt. II sec. 3 (Dec. 20, 2018).
[64] *See* Apar Gupta, *Is India becoming a surveillance state*, Blackletter (December 25, 2018), https://apargupta.com/is-india-becoming-a-surveillance-state-3eb7dc70821d (last visited May 2, 2020).
[65] The Aadhaar case, at ¶1364.
[66] The Aadhaar case, at ¶¶257.6, 267, 510.4.6.
[67] Nikhil Pahwa, *MEITY privately seeks responses to fresh questions on the data protection bill from select stakeholders*, Medianama (August 20,2019), https://www.medianama.com/2019/08/223-meity-privately-seeks-responses-to-fresh-questions-on-the-data-protection-bill-from-select-stakeholders/ (last visited May 2, 2020).
[68] Surabhi Agarwal, *Joint parliamentary committee wants more time to submit data bill note*, The Economic Times (March 25, 2020), https://economictimes.indiatimes.com/tech/internet/jpc-wants-more-time-to-submit-data-bill-note/articleshow/74800912.cms (last visited May 2, 2020).
[69] For discussion on privacy theory based on complete governmental regulation, refer to Part I.
[70] MATTHAN, *supra* note 4, at 186-187.
[71] *Id.*

governmental intervention only when the companies fail to self-correct the flaws in their practices.[72] Matthan's scepticism of the red tape in the regulatory system leads him to side with this form of government monitored 'self-regulatory' approach.[73]

As discussed earlier, the benefits of self-regulation lie in access to expert advice and the ability of these experts to keep up with the innovation in the industry. Further, self-regulation creates an environment of compliance as opposed to governmental control. Matthan believes that this approach of self-regulation is apt for India. Matthan testifies from his industry experience that the Indian business sector has always valued consumer confidence. They have done so by upholding consumer privacy and complying with international data standards even in the absence of a national privacy framework.[74]

Self-regulatory agencies like the Data Security Council of India have been praised in scholarly writing for the mechanisms adopted by them.[75] Self-regulation is known to create an ecosystem of compliance and educate industry peers in the best data practices.[76] However, as discussed earlier, complete self-regulation has very little acceptance in other countries due to fears of corruption. Matthan does not provide any concrete mechanism to deal with the challenges of corruption and crony capitalism under his proposed privacy regime.

The proposed Personal Data Protection Bill, 2019, contrary to Matthan's belief, provides for a designated privacy authority for regulation of the industry.[77] Furthermore, the selection committee of the authority will comprise members from the bureaucracy.[78] This raises a pertinent concern that the Data Protection Authority may include an overwhelming number of bureaucrats.

Matthan's column served as a reminder that the Data Protection Authority should have more technical members than bureaucrats to better comprehend the needs of the

[72] *Id.*
[73] *Id.*
[74] MATTHAN, *supra* note 4, at 110.
[75] Adrienne D'Luna Directo, *Data Protection in India: The Legislation of Self Regulation*, 35(1) NW. J. INT'L L. & BUS. 3 (2014).
[76] Perritt, Jr., *supra* note 23.
[77] Shreya Nandi & Japnam Bindra, *Data protection law closer to reality with cabinet nod,* The Livemint (December 4, 2019), https://www.livemint.com/politics/policy/data-protection-bill-gets-cabinet-nod-11575443663959.html (last visited May 2, 2020).
[78] The Data Protection Bill, 2019, §41.

industry.[79] He further states that for better regulation, the authority should undertake the functions of not only a policeman but also of a teacher and an ombudsman. Matthan suggests that a strict, penal approach by the regulator without inspiring and engaging with the industry would be misguided.[80] This discussion begs the question of whether the role of a 'teacher' in inspiring an environment of compliance can be better achieved by 'private intermediaries' coupled with some variant of government monitored self-regulation. While it is difficult to answer with conviction, Matthan's advice to limit the number of bureaucrats in the authority must be implemented earnestly.

IV. TRANSCENDING THE 'CONSENT STANDARD' AND THE 'PUBLIC INFORMATION FALLACY'

The courts have relied on the two standards of 'consent' and 'public information' to gauge privacy violations. The consent standard is a basic test that entails determining whether the person, whose information is collected and processed, has consented to the transaction and whether such consent was 'informed'.[81] The second standard of public information holds that if the information is already in the public domain, its collection and processing would not be subject to privacy regulations.[82] Matthan argues that it is time to move beyond these standards.

A. Consent Fatigue and Processing of Data

The book argues that consent has become redundant in today's age because of the sheer number of applications and devices we use. Consent has become "*just another formality which needs to be completed before we start using that app.*"[83] Thus, no data subject is adequately informed regarding how his data will be utilised by these digital firms. In addition, there are a variety of uses that data can be put to, each of which poses different risks.[84] Data no longer

[79] Rahul Matthan, *A blueprint for an effective data protection authority*, The Livemint (12 November, 2019), https://www.livemint.com/opinion/columns/opinion-a-blueprint-for-an-effective-data-protection-authority-11574183950803.html (last visited May 2, 2020).
[80] *Id.*
[81] K.S. Puttaswamy, at paras. 597, 506.
[82] Petronet LNG Ltd. v. Indian Petro Group, (2009) 95 S.C.L. 207 (Delhi). The origin of this case lies in the US cases on the Fourth Amendment, where the courts only recognised a 'spatial' aspect of the Fourth Amendment, and thereby, restricting its application to bounded spaces: *See* Olmstead v. United States, 277 U.S. 438 (1928).
[83] MATTHAN, *supra* note 4, at 176.
[84] MATTHAN, *supra* note 4, at 174.

exists in 'silos' as modern databases speak to each other in myriad ways in order to generate new insights from the aggregated data rather than gleaning data from one database only. He characterises this as the 'problem of aggregation', a concern that the Indian cyber laws have not been able to effectively deal with.[85] This problem of aggregation, by processing otherwise irrelevant and impersonal data, results in disclosure of more information than the sum of information collected from the user.[86]

As per Solove, data aggregation results in the generation of 'digital persons' as "*each individual is living alongside a counterpart who exists in the world of computer databases.*"[87] These aggregations significantly increase the information about a person than consensually shared raw data could. Further, the data subject has no control over such data and such databases may be replete with distortions because these profiles are by nature reductive as they are gleaned from crude, incomplete data.[88] Matthan's narration of the credit rating system is particularly emblematic of this.[89] Though consent is taken at the beginning of the transaction, the data subject in this system has no remedy once the same data is used to deny him a loan owing to some erroneous, reductive data. Matthan proposes shifting the burden of proof to the data controller by making him accountable for the manner in which data is stored and processed regardless of the consent of the data subject.[90]

In this context, the new Data Protection Bill, 2019, provides users with the right to correction, completion, update, and erasure of the data collected by the data controller.[91] However, contrary to Matthan's insistence on the accountability of the data controller, this right has been made conditional and the controller has been given broad leeway to refuse such a request.[92]

[85] MATTHAN, *supra* note 4, at 173.
[86] MATTHAN, *supra* note 4, at 181.
[87] DANIEL J. SOLOVE, THE DIGITAL PERSON 1-10 (2004).
[88] DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 120 (2008).
[89] MATTHAN, *supra* note 4, at 67.
[90] MATTHAN, *supra* note 4, at 183.
[91] The Data Protection Bill, 2019, §18.
[92] The Internet Freedom Foundation, *A Public brief and analysis of Data Protection Bill* (January 25, 2020), https://saveourprivacy.in/media/all/Brief-PDP-Bill-25.12.2020.pdf (last visited May 2, 2020).

B. Public Information Fallacy in India

Section 43A of the IT Act, 2000, and the rules framed thereunder provide for 'purpose limitation on data collection'. However, it applies only to personal information and not other public information collected by the data controller such as social media information.[93] It fails to take into account that aggregation of ostensibly public data is equally harmful.[94]

With the Cambridge Analytica scandal coming to light, users have become conscious of the dangers posed by the information that is put on social media platforms.[95] The deployment of user information to tailor propaganda and influence voting patterns has sparked a conversation in the West.[96] In India, the Ministry of Information and Broadcasting proposed a programme called the 'social-media communications hub'. The programme was intended to monitor social media activities in order to collect data regarding the views of social media users regarding government policies and influence them.[97] This attempt was later withdrawn after protests.

It has been highlighted before that aggregating ostensibly innocuous, non-personal data or data available in the public domain permits the generation of intimate profiles of individuals. However, the reluctance, on the part of the judiciary and policy-makers to make rules governing public information, flows from the notion known as the 'secrecy paradigm'. This results in the courts and regulators treating data either as completely private or completely public without recognising that data may merit protection regardless of where it is found.[98] In India, the Supreme Court has explicitly overruled the 'secrecy paradigm'. It held that privacy rights belong to "*persons and not places*" and therefore, the existence of the

---

[93] Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011. These rules have been framed under section 43A of the Information Technology Act, 2000.

[94] MATTHAN, *supra* note 4, at 180-182.

[95] Issie Lapowsky, *How Cambridge Analytica Sparked the Great Privacy Awakening*, Wired (July 3, 2019), https://www.wired.com/story/cambridge-analytica-facebook-privacy-awakening/ (last visited May 2, 2020).

[96] Emma Briant, *I've seen inside the digital propaganda machine. And it's dark in there*, The Guardian (April 20, 2018), https://www.theguardian.com/commentisfree/2018/apr/20/cambridge-analytica-propaganda-machine (last visited May 2, 2020).

[97] Krishn Kaushik, *Why track social media chatter*, The Indian Express (July 16, 2018), https://indianexpress.com/article/explained/supreme-court-social-media-communications-hub-whatsapp-messeges-tapping-modi-govt-5261003/ (last visited May 2, 2020).

[98] DANIEL SOLOVE, UNDERSTANDING PRIVACY 111, 139, 150 (2008); *See supra* note 81 for differing cases.

information in the public domain cannot be the sole factor to decide privacy violations.[99] However, some lower courts have considered the 'public nature' of the information to deny reliefs when such ostensibly public information is collected or further publicised.[100] Given this uncertainty in India, the book rightly rings the warning bells for unchecked data processing by data analytics companies.

Curiously, the Data Protection Bill, 2019, which is currently being reviewed by the Joint Parliamentary Committee, explicitly allows the government to collect non-personal data from private players for 'evidence based policy-making' and 'targeting of services'.[101] It also allows the government to frame policies for digital economies by making use of such non-personal data. These provisions are reminiscent of the social media communications hub programme which sought to similarly monitor the social media activities of the users with an intention to influence them. These provisions ought to be reconsidered given that non-personal data, when processed or aggregated with other government databases, can reveal intimate profiles of individuals.

CONCLUSION

The book is an intellectually stimulating read for those interested in privacy law and provides industry insights for individuals troubled by the specter of being deprived of their privacy. For the former, it offers crucial insights to understand the privacy jurisprudence in India. For the latter, it offers a fresh perspective, in contrast to the Orwellian saga that we often find reproduced in popular culture. Matthan attempts to strike a fine balance between the privacy concerns of individuals and the efforts of the industry to innovate. He encourages such efforts through the creation of a transparent privacy framework, particularly through his suggestion regarding the privacy auditors. However, Matthan's highly context-specific understanding of privacy has the potential to undermine the normative conceptions of privacy.

[99] District Registrar v. Canara Bank (2005) 1 SCC 496,523; *See* Gautam Bhatia, *State Surveillance and the Right to Privacy in India: A Constitutional Biography*, 26 NLSI REV. 127, 145 (2014).
[100] Petronet LNG Ltd. v. Indian Petro Group, (2009) 95 S.C.L. 207 (Delhi); Rajinder Jain v. Central Information Commission, 164 (2009) D.L.T. 153 (Delhi).
[101] The Data Protection Bill, 2019, §91.

The book's most important contribution to the existing scholarship lies in the breadth of the disciplines it navigates in order to comprehend the notion of privacy in the data-driven world. As John Dewey wrote "*inquiry begins with problems in experience, not with abstract universal principles*",[102] Matthan provides a holistic understanding of privacy by marrying law and social theory with technology and praxis.

[102] JOHN DEWEY, EXPERIENCE AND NATURE 9 (1925).