PRIVACY CONCERNS IN THE AGE OF SOCIAL MEDIA*

VRINDA BHANDARI

INTRODUCTION

Every transaction of an individual user and every site that she visits, leaves electronic tracks generally without her knowledge. These electronic tracks contain powerful means of information, which provide knowledge of the sort of person that the user is and her interests. Individually, these information silos may seem inconsequential. In aggregation, they disclose the nature of the personality: food habits, language, health, hobbies, sexual preferences, friendships, ways of dress and political affiliation. In aggregation, information provides a picture of the being: of things which matter and those that do not, of things to be disclosed and those best hidden.

Justice D. Y. Chandrachud
in *K. S. Puttaswamy v Union Of India* (Privacy case)

....As we move towards becoming a digital economy and increase our reliance on Internet-based services, we are creating deeper and deeper digital footprints—passively and actively....These digital footprints and extensive data can be analysed computationally to reveal patterns, trends, and associations, especially relating to human behaviour and interactions and, hence, is valuable information. This is the age of 'big data'...Thus, there is an unprecedented need for regulation regarding the extent to which such information can be stored, processed and used by non-State actors. There is also a need for protection of such information from the State.

Justice S. K. Kaul
in *K. S. Puttaswamy v Union Of India* (Privacy case)

These observations were made by the nine-judge bench of the Supreme Court, while declaring and reiterating the fundamental right to privacy, in its seminal judgement in *K. S. Puttaswamy v Union of India.*[1] The Court's concerns about the loss of privacy of state and non-state actors reflect the modern reality of living in the age of big data, data analytics, and the 'Internet of Things'. In recent times, privacy considerations arising from the Cambridge Analytica scandal, Facebook leaks, Aadhaar leaks, and the Snowden revelations have dominated the news cycle. This is because technology has today made it possible to collect, store, mine, share and use personal information to create a rich profile of a person—a feat that was unimaginable even a decade ago. Advances in technology have also been accompanied by warnings against techno-utopianism, especially with respect to its impact on the poor (Eubanks, 2018), leading to conversations about 'balancing' big data with privacy concerns.

Our daily interaction and hence reliance on the Internet and social media have increased partly as a result of network effects, and partly because of the addictive designs that have deliberately been inserted to keep people 'hooked' to these platforms.[2] We are also living in an age of 'dataveillance', where an individual's actions and communication can be easily and more systematically monitored through the use of information technology (McDermott, 2017). This has caused privacy concerns, emanating from both state and private actors. The upshot of this is the problem of the 'privacy paradox', where users profess to, and are indeed, concerned about their right to privacy, but their behaviour does not reflect their apprehensions (Blank, et al., 2014).

Justice Chandrachud, while writing his dissent, striking down the Aadhaar Act in *K. S. Puttaswamy v Union of India*[3] (Aadhaar case), noted that although technology has become a universal language, which straddles culture and language, it has also reshaped the dialogue between citizens and the state, and has the potential to confront the future of freedom and power itself.

Privacy concerns have also been fuelled by the almost unchecked practice, and capability, of both state and private actors to collect and process vast troves of metadata of individuals. Metadata is the 'data about data', which can give a fuller profile of individuals, including their likes and dislikes, and their habits, rather than simply the content

of data. Thus, as a simple example, traditional surveillance is concerned with eavesdropping on a telephone call or reading an e-mail, acts that would reveal the *content* of the conversation. However, the metadata generated about such an e-mail—such as the sender's name, e-mail and IP address; the recipient's name and e-mail address; the date, time and time zone of the e-mails; message ID, content type, subject and status of e-mail—reveal a far broader pattern of the individual subject's behaviour patterns and location.[4] As explained in the internationally accepted Necessary & Proportionate International Principles on the Application of Human Rights to Communications Surveillance, over time, such metadata—which is generated through the use of phones, e-mails and Internet browsing—can disclose medical conditions, religious and political beliefs, and the circle of friends and acquaintances of a person with a reasonable accuracy that is chilling.[5]

These concerns have come to the forefront ever since the government argued, during the Aadhaar hearings in August 2015, that the right to privacy is not a fundamental right. This led the Supreme Court to refer the question to a nine-judge bench, which culminated in the *Puttaswamy* judgement in August 2017. During the *Puttaswamy* hearings, the government constituted an Expert Committee headed by Justice B. N. Srikrishna, which acknowledged the need for a privacy law, and released a White Paper soliciting responses on a variety of privacy and data protection issues. In July 2018, the Ministry of Electronics and Information Technology released the draft Personal Data Protection Bill, 2018 (Draft Bill), drafted by the Srikrishna Committee, and opened it for comments. However, no further movement has taken place thereafter.

It bears noting that India does not have a privacy or data protection law, a fact acknowledged even during the recent Aadhaar case. In fact, even after the release of the Draft Bill, there is no guarantee whether, and *if*, such a law will come into place, especially given the upcoming elections and the fact that there have been previous failed attempts, in 2011 and 2014, in translating a draft privacy bill into law.

Given this backdrop, relying on papers that I have previously written, I will briefly explore the privacy concerns against state actors and private entities; why we should be worried about their actions; and the way forward (Bhandari and Sane, 2018; Bhandari and Sane, 2016).

PRIVACY FROM THE STATE

LEGAL REGIME

Throughout history, concerns of privacy have traditionally been expressed *qua* the state. The state has the power to lawfully conduct surveillance against its citizens, generally on grounds of national security, public emergency, crime prevention, etc., and courts are usually deferential to the state's exercise of such powers. In fact, even in 2014, the Supreme Court in *Ex-Armymen's Protection Services Private Limited* v. *Union of India & Ors.* noted that 'what is in the interest of national security is not a question of law. It is a matter of policy. It is not for the court to decide whether something is in the interest of the State or not. It should be left to the executive'.[6]

Surveillance in India is primarily regulated by two laws. The first is the Telegraph Act of 1885, which broadly permits interception and surveillance on 'the occurrence of a public emergency, or in the interest of public safety', if it is 'necessary or expedient' to do so in the interests of the sovereignty and integrity of India, the security of the state, friendly relations with foreign states, or public order, or for preventing incitement to the commission of an offence.

Internet surveillance is governed by the provisions of the Information Technology Act, 2000 (IT Act), which has given wider powers to the government to intercept, monitor or decrypt Internet data, even in cases where there is no public emergency or public safety. The IT Act provides two additional grounds for surveillance, viz., 'defence of India' and the 'investigation of any offence'. It also permits the monitoring of Internet metadata by 'any' government agency for 'enhanc[ing] cyber security' or for 'identification, analysis and prevention of any intrusion or spread of computer contaminant in the country'. Section 69 of the IT Act further requires Internet service providers (the intermediaries) to 'extend all facilities and technical assistance' to the intercepting agency.

The recent Draft Bill, drafted by the Srikrishna Committee, grants an almost[7] absolute exemption from the obligations of the Bill when the processing of personal data is: 'in the interests of security of the State' if the processing is authorised pursuant to a law made by Parliament; in accordance with the procedure established by such law; and is necessary for, and proportionate to, such interests being achieved. While this is a definite improvement over the

current regime, on the requirement of necessity, and proportionality, in particular, the Bill falls short on some grounds.

Unlike the two previous draft Privacy Bills, the draft 2018 Bill does not have a separate chapter on surveillance. Nor does it deal with the reform of law enforcement agencies or the intelligence apparatus, as proposed by the Intelligence Services (Powers and Regulation) Bill 2011 (introduced as a Private Members' Bill by Manish Tewari), and recommended even by the Srikrishna Committee in its Report. The Report acknowledges that the lack of any inter-branch oversight of law enforcement agencies, through a statute, is 'deleterious in practice... and potentially unconstitutional', and that the central government ought to 'carefully scrutinise the question of oversight of intelligence gathering and expeditiously bring in a law to this effect'. However, it stops short of including such provisions in the draft 2018 Bill.

ROLE OF TECHNOLOGY AND BIG DATA

Government surveillance has been aided by developments in technology, both in terms of improving its abilities and reducing its costs, and in facilitating an increased interaction/reliance on private parties to conduct the surveillance (e.g., under Section 69 of IT Act). The Supreme Court of the United States remarked on the first facet of improved technological ability, in the case of *US v Jones*,[8] while holding that the installation of a GPS tracking device in a car to monitor its movements was unlawful. In her concurring opinion, Justice Sotomayor noted that GPS monitoring generated a precise, comprehensive record of a person's public movements, and this data could be stored and efficiently mined for information for many years in the future, and that:

> With increasing regularity, the government will be capable of duplicating the monitoring undertaken in this case by enlisting factory or owner-installed vehicle tracking devises or GPS enabled smartphones.... Awareness that the government may be watching chills associational and expressive freedom...it may alter the relationship between citizen and government in a way that is inimical to democratic society.

The explosion of big data is also demonstrated in its application in law enforcement, whether it is in tracking search results to identify human trafficking networks or in creating a more rounded suspect profile. This has meant that large swathes of personal information about an individual have become more easily known to the police. One of big data's more controversial uses is in predictive policing, which uses analytics software, such as 'PredPol', to identify geographical hot spots to help the police anticipate and prevent the crime (Perry, et al., 2013). Already popular in various cities in the United States, such as Chicago, Boston, New York, Washington DC and Los Angeles, it is slowly being embraced by the Indian police, particularly in New Delhi and Jharkhand (Routray, 2012; Singh, 2017). What is disquieting about this trend is that it is now being used to identify an individual's propensity to crime (Podesta, et al., 2014). This will inevitably lead to widespread profiling, increased surveillance, and the hard reality that on many occasions the predicted results will be incorrect. In fact, in recent times, there has been a vociferous debate about the biases that are encoded in risk assessment or crime prediction algorithms currently in use in America. For instance, a study conducted by *ProPublica* found that crime forecasting algorithms were twice as likely to falsely flag black defendants as future criminals as white defendants (Angwin, et al., 2016).

THE INTERACTION BETWEEN THE STATE AND PRIVATE PARTIES

On the aspect of the state leveraging the powers of the private sector for its own benefits, Justice Kaul in *Puttaswamy* noted that the Indian government had been successful in compelling Blackberry to give it the ability to intercept data sent over Blackberry devices. The Apple–FBI dispute raised similar questions, and Indian jurisprudence indicates that national security considerations would prevail over privacy and require the company to create a backdoor.

The consequences of this interaction were also visible in the government's proposal to establish a 'Social Media Communications Hub'[9] to create a 'social media monitoring tool' that can help 'facilitate creating a 360 degree view of the people who are creating a buzz across various topics'; conduct 'predictive analytics' and sentiment analysis; and store metadata information in a 'big data database'. While hearing a PIL filed to challenge this move,

the Supreme Court made scathing observations, noting that the plan to monitor social media usage could turn India into a 'surveillance State'. After this criticism, the Request for the Proposal was withdrawn.[10]

Morozov (2011) argues that the Internet is not a one-way street and dictatorial regimes are equally adept at and technologically savvy enough to use the Internet to further their propaganda, to target dissidents and suppress free speech. Using these arguments, he debunked the myth of the 'Twitter revolution' in Iran in 2009, and argued that, instead, the government monitored the Internet activity of the protestors, both at home and abroad.

PRIVACY FROM PRIVATE ACTORS

INCREASING THE POWER OF PRIVATE ACTORS

'Data is the new oil' has now become an oft-cited adage, reflected in the growth of tech companies, whose businesses revolve around the buying and selling of personal information to third parties, and who 'now exist to commoditize the conclusions drawn from that data' (Podesta, et al., 2014). The business models of these companies are thus *dependant* on data and are focused on increasing user interaction and reliance on them. This has been accompanied by a simultaneous explosion in wearable technology such as Fitbit; voice-activated, Internet-connected, personal assistants, such as Amazon Echo (Alexa) and Google Home; and facial recognition software that is used for purposes as myriad as crime detection/surveillance, unlocking one's iPhone, and being identified and tagged on photos by others on Facebook. These technologies raise new concerns of privacy and security, while promising all the benefits of artificial intelligence (AI). Justice Kaul in *Puttaswamy* accurately captured the 'A to 'I' of our dependence on these companies and the Internet in the following manner: 'Apple, Bluetooth and chat followed by download, e-mail, Facebook, Google, Hotmail and Instagram.'

It is thus unsurprising that tech companies essentially function as super corporations. The five largest tech companies in the world—Apple, Amazon, Facebook, Alphabet (the parent company of Google) and Microsoft—are collectively worth more than the entire economy of the United Kingdom. These five companies are also worth more than the next 11 most valuable US companies, including Walmart and JP Morgan Chase.[11] Furthermore,

the industry has seen a spate of acquisitions amongst the major players, thus furthering their consolidation and monopoly over various aspects of our private life. For instance, Google bought YouTube in 2006, Facebook purchased WhatsApp and Instagram, and Amazon bought Goodreads and Whole Foods Market.

Private corporations are collecting information about their users (and their friends), tracking their behaviour online, and creating individual profiles. These profiles are then used as the basis for automated decision making, using artificial intelligence and complex computational algorithms. These factors, including the prominent role played by technology giants and our increased reliance on the Internet for all aspects of our daily lives, have contributed to bringing private actors to the forefront of the privacy debate.

USE OF PERSONAL DATA BY PRIVATE ENTITIES FOR PROFILING USERS

There is concern over the loss of privacy of the state. This is because it is a (sort of) monolithic entity and its powers of surveillance and profiling are extensive, and because it can serve as a repository of centralised data—for example, the debate raging over the Unique Identification Authority of India's (UIDAI) role and the centralisation of Aadhaar data. Along with this, unlike private actors, the state has a monopoly over violence and has the backing of the law to take coercive action against individuals. A combination of these factors gives the state immense power over its citizens, which can be misused to track 'subversive' activities and quell dissent.

Concerns about the erosion of privacy *qua* private actors are slightly different, and are linked to the increasing power held by a *few* private entities (particularly technology giants) in terms of their ability to create deep profiles of their users, to engage in behaviour manipulation, or simply share that data with third parties unbeknownst to their users. Private companies have such powers only because of the vast troves of data that they collect, both actively and passively, and the unknown uses the data is being put to.

One of the primary uses of data is for creating individualised user profiles for targeted advertising. In fact, the business model of Google and Facebook—and the reason why they are able to provide these service for 'free'—is premised on this. This also creates business for behavioural advertising companies, such as WPP Plc

(founded as Wire and Plastic Products plc, a communication services and advertising group), which has built over 500 million profiles in North America, Europe and Australia based on the Internet activity of those individuals across various websites (Brown, 2015). Target, the American supermarket chain, collects demographic information about its users, including their addresses, estimated salaries, the credit cards in their wallets, and famously built a pregnancy-prediction model, including estimating the due date within a small window, so that they could sell more products to newly pregnant customers (Duhigg, 2012).

Facebook, too, has repeatedly found itself at the centre of controversy on issues surrounding the privacy and security of its users. However, even in 2013, it was reported that Facebook's browser code was storing half-typed posts, comments and status updates as metadata, even if it was deleted by the user before pressing 'Enter'. While Facebook tracks such 'self-censorship' behaviour (although they claim not to know the *content* of the deleted posts), most users are not aware of this and have not expressly consented to such data collection, nor do they derive any benefit from it (Golbeck, 2013). However, Facebook data scientists in their study claim to have an interest in furthering this research, partly because 'users and their audience could fail to achieve potential social value from not sharing certain content, and the [social-network service] loses value from the lack of content generation' (Das and Kramer, 2013).

Similarly, in a study conducted in 2013 of more than 58,000 volunteers, it was found that an analysis of as few as 68 Facebook 'Likes' of an individual could be analysed to predict, with reasonable accuracy, their race (95 per cent), gender (93 per cent), sexual orientation for males (88 per cent), political party and religious affiliation (more than 80 per cent), their smoking/drinking habits (75 per cent), substance use (73 per cent), and other personality traits and intelligence, among others (Kosinski, et al., 2013). The authors of the study surmised that the predictive power of 'Facebook Likes' could be found as well in browsing and purchase histories, and search queries of individuals. While these might have some benefits in terms of improving products and services, and research in human psychology, the study concluded that 'the predictability of individual attributes from digital records of behavior may have considerable negative implications, because it can easily be applied

to large numbers of people without obtaining their individual consent and without them noticing.' Even though these predictions are never going to be 100 per cent accurate (which itself is a big problem), they could be used to make decisions about one's life/finances/career in a way that could pose a threat to their 'well-being, freedom, or even life' (ibid.). This is reflected in the darker side of social media, discussed next.

THE 'DARKER' SIDE OF SOCIAL MEDIA

Big data analytics have allowed companies to identify statistical relationships between discrete data sets, and use this to create detailed personal profiles and predict seemingly unrelated outcomes. In this endeavour, companies are aided by the fact that digital data is usually persistent (it can be stored automatically and for longer periods); searchable (making specific information easier to find amongst vast gigabytes/terabytes of data); and replicable (easily shareable in a machine readable format) (Brown, 2015).

Such profiling usually has a discriminatory impact on the poor and serves to perpetuate inequalities. Eubanks discusses the impact of algorithms that are intended to match vulnerable homeless people with appropriate available resources by creating electronic registries, or to predict which children are likely to become victims of abuse. She demonstrates how these algorithms, meant to eliminate human bias by removing any discretion, end up simply shifting the bias, for instance, by prioritising services that are most 'cost effective', or conflating 'parenting while poor with poor parenting' (Eubanks, 2018).

The biases that are inherent in the algorithms that are increasingly making important decisions about humans with regard to the grant of aid, welfare, housing, credit, employability, etc., have led to an increased debate on algorithmic accountability or algorithmic fairness. The European Union has recognised the right to object to decisions made solely by automated processing, and to profiling, as part of ensuring the lawfulness and accountability of data controllers/data fiduciaries who process our data. While the Srikrishna Committee recognised that such a right—based on emerging challenges from big data and artificial intelligence—may legitimately 'curb harms due to prejudice and discrimination in output data owing to evaluative determinations without human

review', it eschewed the inclusion of such a right in the Draft Bill, 2018, leaning instead in favour of *ex ante* accountability structures.

The darker side of social media has also manifested itself in the form of spreading false information and rumour-mongering, with consequential effects on behaviour. This is best reflected in the Cambridge Analytica scandal and concerns of influencing votes. In India we have seen this in the WhatsApp rumours that are forwarded with apathy and impunity, without consideration for the truth, and which have resulted in the death of more than 22 people over the last year.[12]

WAY FORWARD

THE NEED FOR A LAW

Privacy is not an absolute right and is often pitted against competing considerations such as national security, crime prevention, innovation, or public interest. How these competing rights are accommodated together depends on each country's particular social structure; its cultural, historical, social and economic fabric; and the importance given to ideas of privacy, dignity, autonomy and choice. As a *starting point,* thus, it is absolutely imperative to enact a specific privacy and data protection law.

It could be argued that especially in the private domain, relations are governed by consent and contract, and users are willingly giving their data in exchange for 'free services'; thus there is no need to regulate private entities such as Facebook or Google. The argument goes that if customers are worried about privacy, it will reflect in their changed online activities, forcing companies to offer improved privacy protections.

However, market forces may not adequately reign in the increasing powers of global technology giants. For one, by leveraging network effects, these companies and Internet platforms function as monopolies in their spaces, making important decisions, with almost no oversight mechanism or appeals' process. As a vast part of our life has shifted online, these companies have become the adjudicators of our fundamental rights (Tambin, 2018).

Furthermore, information asymmetry is a problem where users often know less than data controllers about the extent of data collection; its manner of processing, sharing and use; and the associated consequences of sharing such data with third parties, or

feeding it into an algorithm (Acquisti and Grossklags, 2007). In fact, in most cases, users are never notified if and when their information is being shared with third parties.

Related to this is the fact that for most users it is difficult, if not impossible, to comprehend the import of the privacy policies to which they must agree before registering on an Internet/social media platform. The fine print of these policies is complex and hard to follow. For instance, an empirical analysis of 261 privacy policies of various companies found that the average length of such policies was 2,176 words—which is far from the desired model of simple, short and easy-to-understand privacy policies—while still being silent on crucial categories (Marotta-Wurgler, 2016).

Finally, users suffer from bounded rationality, which makes it difficult for them to process all the relevant information in a privacy policy, and act on it accordingly, thus compelling them to rely instead on simple heuristics. Researchers have found that the very presence of a privacy policy, regardless of its contents, is seen as a notable privacy protection; or that users often view privacy policies as guarantees of data protection, instead of liability disclaimers for firms (Acquisti and Grossklags, 2007; Tene and Polonetsky, 2012). A Pew Research study also showed that even though many Americans do not trust companies or the government to protect their personal data, they still frequently neglect cybersecurity best practices in their own personal lives (Smith, 2017).

THE (ABSENT) LEGAL FRAMEWORK IN INDIA

India does not have a privacy law. Although there have been two previous attempts to draft privacy laws in 2011 and 2014, and the introduction of a Data Privacy and Protection Bill in 2017 in the Lok Sabha by Baijayant Panda as a Private Member Bill, none of these have translated into a law.

The current legislative framework is limited to the Information Technology Act, 2000, parts of which have been criticised as being 'inadequate' by the Srikrishna Committee in its White Paper. The IT Act has limited scope as it does not regulate the activities of the government or the non-profit sector, and it has weak accountability and enforcement structures. The Act does not incorporate principles of proportionality or data minimisation either (Bhandari and Sane, 2016).

Additionally, as explained earlier, surveillance in India is governed by the IT Act and the Telegraph Act. However, neither regulate the establishment, functioning, or accountability of law enforcement agencies, allowing these agencies to function in a shadowy manner without adequate supervision.

In light of this, the Draft Data Protection Bill, 2018, recommended by the Committee of Experts headed by Justice Srikrishna, is a welcome step. It has engaged in public consultation and helped move the debate forward on privacy and data protection, taking into account global developments, such as the adoption of the European Union General Data Protection Regulation (GDPR), as well as the Supreme Court's privacy decision in *Puttaswamy*. Although the Srikrishna Committee Report acknowledged the need for amendments to the Aadhaar Act and intelligence services reform, these unfortunately do not find mention in the Bill. It is worth noting that the Bill has been criticised on various grounds, although that is outside the scope of this article.

The Ministry of Electronics and Information Technology had solicited comments from the public, which had to be submitted by 10 October 2018. It is unclear, however, what the next steps are, and whether such a Bill will be introduced in Parliament on the eve of the general elections. This is the third time that a draft bill has been prepared under the aegis of a ministry. It will be a tragedy if it too gets dropped in the humdrum of everyday politics.

THE NEED TO IMPROVE STATE CAPACITY

While the current debates have centred on the need for a privacy law and a definition of the scope of rights, we must not forget that a law will not by itself solve all our problems. First, there is the question of implementation. State capacity in India, which can be measured by the ability to write good regulations and the ability to enforce the law, is weak. For instance, for the law to be successful, the grievance redressal mechanism should be effective and citizen-friendly. Second, and related, is the ability to ensure the financial and functional independence of the Data Protection Authority (or any other ombudsman), proposed to be created under the Draft Bill of 2018. Third is the larger question of the unintended effects of regulations in terms of further entrenching the monopoly of existing players by increasing the cost of entry into business.

CONCLUSION

All these factors ought to be considered when we take into account the impact of the erosion of our privacy by the actions of state and non-state/private actors. We are living in a world where technology will always outpace the law. Today, big data has allowed both the state and private corporations to create deep profiles of citizens/individuals, which has given them immense powers to conduct surveillance or make consequential decisions that have a direct impact on people's lives. We have taken a step forward in the right direction through the public consultation with the Srikrishna Committee Report and the draft Data Protection Bill of 2018. However, it remains to be seen whether the Bill will ever get translated into law, and, if so, if there will be adequate and transparent public consultation preceding such a move. For the sake of our privacy, we can only hope that the answer to both the questions is, yes.

◆

ACKNOWLEDGEMENTS

*Vrinda Bhandari is an advocate practising in Delhi. This article has been adapted from a previous co-authored paper in 2016, 'Towards a Privacy Framework for India in the Age of the Internet', that was presented at the 1st Law and Economics Policy Conference, New Delhi, and a co-authored piece, 'Protecting Citizens from the State Post *Puttaswamy*: Analysing the Privacy Implications of the Justice Srikrishna Committee Report and the Data Protection Bill, 2018', that was published in the *Socio-Legal Review* 14 (2).

NOTES

1. (2017) 10 SCC 1.
2. See the interview with Tristan Harris, a former Google engineer, at <https://www.cbsnews.com/news/brain-hacking-tech-insiders-60-minutes/>.
3. (2018) SCC Online SC 1642.
4. Office of the Privacy Commissioner of Canada. 'Metadata and Privacy: A Technical and Legal Overview.' October 2014. < https://www.priv.gc.ca/media/1786/md_201410_e.pdf>.
5. Necessary & Proportionate. 'International Principles on the Application of Human Rights to Communications Surveillance.' 2014. <https://necessaryandproportionate.org/principles#footnote4_iysd83f>
6. (2014) 5 SCC 409.
7. Section 42 of the Bill states that processing of personal data 'in the interests of the security of the State' shall be exempt from the obligations of the Act, except

sections 4 and 31, on fair and reasonable processing and network security safeguards.

8. 132 S. Ct. 945 (2012).
9. Broadcast Engineering Consultant India, Ltd. 'RFP invited for Selection of Agency for SITC of Software and Service and Support for function, operation and maintenance of Social Media Communication Hub, Ministry of Information and Broadcasting, Government of India'. BECIL/Social Media/MIB/02/2018–19. 25 April 2018.
10. PTI. 'Centre Withdrawing Notification on Social Media Hub, AG Informs Supreme Court', *Hindu Business Line*, 3 August 2018. <https://www.thehindubusinessline.com/info-tech/social-media/centre-withdrawing-notification-on-social-media-hub-ag-informs-supreme-court/article24590834.ece>.
11. AP 'Apple, Amazon, Facebook, Alphabet, and Microsoft are Collectively worth More than the Entire Economy.' 27 April 2018. <https://www.inc.com/associated-press/mindblowing-facts-tech-industry-money-amazon-apple-microsoft-facebook-alphabet.html>.
12. https://www.news18.com/news/immersive/death-by-whatsapp.html.

REFERENCES

Acquisti, Alessandro and Jens Grossklags. 2007. 'What Can Behavioral Economics Teach Us about Privacy', *Digital Privacy: Theory, Technologies & Practices*, 363, 365.

Angwin, Julia, Jeff Larson, Surya Mattu and Lauren Kirchner. 2016. 'Machine Bias: There's Software Used across the Country to Predict Future Criminals. And it's biased against Blacks', *ProPublica*, 23 May. <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>.

Bhandari, Vrinda and Renuka Sane. 2018. 'Protecting Citizens from the State Post *Puttaswamy*: Analysing the Privacy Implications of the Justice Srikrishna Committee Report and the Data Protection Bill, 2018', *Socio-Legal Review*, 14 (2): 143–169. http://www.sociolegalreview.com/volume–142/.

———. 2016. 'Towards a Privacy Framework for India in the Age of the Internet.' NIPFP Working Paper No. 179.

Blank, Grant, Gillian Bolsover and Elizabeth Dubois. 2014. 'A New Privacy Paradox: Young People and Privacy on Social Network Sites', Global Cyber Security Capacity Centre, Draft Working Paper, Oxford Internet Institute. https://goo.gl/jR80QK.

Brown, Ian. 2015. 'Social Media Surveillance.' *The International Encyclopaedia of Digital Communication and Society*. UK: Wiley–Blackwell. <https://onlinelibrary.wiley.com/doi/pdf/10.1002/9781118767771.wbiedcs122>.

Das, Sauvik and Adam Kramer. 2013. 'Self-Censorship on Facebook.' Proceedings of the Seventh International AAAI Conference on Weblogs and Social Media, pp. 120–28. <https://www.aaai.org/ocs/index.php/ICWSM/ICWSM13/paper/viewFile/6093/6350>.

Duhigg, Charles. 2012. 'How Companies Learn Your Secrets', *The New York Times*, 16 February. <https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html>.

Eubanks, Virginia. 2018. *Automating Inequality: How High-tech Tools Profile, Police, and Punish the Poor* New York: St. Martin's Press.

Golbeck, Jennifer. 2013. 'On Second Thought...Facebook Wants to Know Why You Didn't Publish that Status Update You Started Writing', *The Slate*, 13 December. <https://slate.com/technology/2013/12/facebook-self-censorship-what-happens-to-the-posts-you-dont-publish.html>.

Kosinski, Michal, David Stillwell and Thore Graepel. 2013. 'Private Traits and Attributes are Predictable from Digital Records of Human Behavior', 110 (15), Proceedings of National Academy of Sciences, 5802. https://doi.org/10.1073/pnas.1218772110.

Marotta-Wurgler, Florencia. 2016. 'Understanding Privacy Policies: Content, Self-Regulation and Markets.' Working Paper No. 16–1. Law and Economic Research Paper Series. NYU Center for Law, Economics, and Organisation, April. <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2736513>.

McDermott, Yvonne. 2017. 'Conceptualizing the Right to Data Protection in an Era of Big Data', *Big Data and Society*, 4 (1), January–June, 2017. doi: 10.1177/2053951716686994.

Morozov, Evgeny. 2011. *Net Delusion: The Dark Side of Internet Freedom*. US: Public Affairs, Perseus Group Books.

Perry, Walter, Brian McInnis, Carter C. Price, Susan C. Smith and John S. Hollywood. 2013. 'Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations.' RAND Corporation: Safety and Justice Program (Tech. Report).

Podesta, John, Penny Pritzker, Ernest Moniz, John Holdren and Jeffrey Zients. 2014. 'Big Data: Seizing Opportunities, Preserving Values.' US: Executive Office of the President, The White House.

Routray, Bibhu. 2012. 'Making a Case for Futuristic Predictive Policing in India', *New Indian Express*, 9 September.

Singh, Karn. 2017. 'Preventing Crime Before it Happens: How Data is Helping Delhi Police', *Hindustan Times*, 27 February.

Smith, Aaron. 2017. 'Americans and Cyber Security', Pew Research Centre: Internet & Technology, 26 January. <http://www.pewinternet.org/2017/01/26/americans-and-cybersecurity/>.

Tambin, Damian. 2018. 'What should be done with Facebook: Break It up or Regulate It?', *The Guardian*, 27 April. <https://www.theguardian.com/commentisfree/2018/apr/27/facebook-regulate-tech-platforms>.

Tene, Omer and Jules Polonetsky. 2012. 'Privacy in the Age of Big Data: A Time for Big Decisions', *Stanford Law Review Online*, 63–69.

◆◆