NIPFP Working paper series

Towards a privacy framework for India in the age of the Internet

No. 179
03-Nov-2016
Vrinda Bhandari and Renuka Sane

National Institute of Public Finance and Policy
New Delhi

Towards a privacy framework for India in the age of the internet

Vrinda Bhandari[*] and Renuka Sane[**]

Abstract

Over the last decade, there have been vast improvements in surveillance technology and the availability, storage, and mining of personal information online, supported by developments in big data analytics. This has created a public policy conundrum over balancing the benefits of big data with the threat to the right to privacy. In an environment of pervasive surveillance and intrusive technology, there is a need for improved protection of privacy rights through a mixture of legislation and regulation, and building public awareness and demand for safeguards. This paper makes a case for the need for privacy from both the State and the private sector; examines the jurisprudential development of the right to privacy in India, and lays down privacy principles, that will underlie any proposed privacy law. It then evaluates the Indian IT Act, and the recently legislated Aadhaar Act, against the proposed privacy principles.

Keywords: Privacy, big data, India

JEL classification codes: H10, L86

[*] Vrinda Bhandari (Email: vrinda.bhandari@gmail.com) is a practicing advocate in Delhi.
[**] Renuka Sane (Email: renuka@saner.org.in) is Visiting Faculty at the Indian Statistical Institute, Delhi Centre. We thank Sunil Abraham and participants at the 1st Law Economics Policy Conference 2016, for useful comments. All errors are our own.

1. Introduction

In recent years, the Snowden leaks and the NSA revelations on government surveillance, the Apple-FBI dispute, and the WhatsApp-Facebook privacy sharing arrangements have made global headlines. The rise of big data[1] and data analytics and the increasing availability, storage, and mining of personal information online has created a public policy conundrum over balancing the benefits of big data with the threat to the right to privacy (Tene and Polonetsky, 2012; White House, 2014).

Countries such as the U.K. and the U.S. have begun to respond to some of these concerns by revisiting their privacy legislation and imposing additional safeguards. For example, the US and the EU recently entered a new data transfer framework agreement, the "Privacy Shield", intended to protect the privacy of data of European users stored in the U.S.[2] The E.U., too, has adopted the General Data Protection Regulation in 2016 for improved data protection across Europe. The discussions in these agreements range from the right to privacy to the right to be forgotten.

Meanwhile, the Indian Supreme Court in August 2015, in *Justice K.S. Puttaswamy (Retd.) v UOI and Ors, (2015)*, put into question whether the right to privacy is a fundamental right at all under Part III of the Indian Constitution and referred the questions to a larger five-judge bench.[3] In the process, it brought the debate on the right to privacy to the forefront of public discourse in India once again.

A lot of work has been done on the examination of the state of law of privacy in India (CRID, 2006; CIS, 2011; Justice Shah Report, 2012) and even in proposing a privacy bill (CIS, 2013; Hickok, 2014). Our contribution to this debate is two fold - *first*, we seek to conceptualise the right to privacy in the context of the State and private actors in the age of the internet and big data. *Secondly*, using globally accepted privacy principles, we propose a privacy framework on the basis of which to evaluate any future privacy law.

We begin with a discussion on what is the right to privacy in Section 2. We explore why

[1] Big data is defined as "high-volume, high- velocity and/or high-variety information assets that demand cost-effective, innovative forms of information processing that enable enhanced insight, decision making and process automation" (Gartner, 2001; Government of Australia, 2015). It has various benefits, including in in the creation of social value by improving the delivery of goods and services.

[2] This agreement replaced the 16-year-old Safe Harbour Agreement, which was declared invalid by the European Court of Justice in October 2015 in the wake of Snowden's revelations about the NSA's surveillance activities.

[3] The Court made this referral during the hearings challenging the "Aadhaar Card Scheme" under which the Government of India was collecting and compiling the demographic and biometric information of its residents for use for various purposes since 2009-10. This scheme was finally given statutory backing with the passage of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits, and Services) Act, 2016 [Aadhaar Act] in early 2016. The Act undertook such collection and storage of demographic and biometric information of residents in India for their use in targeted delivery of subsidies, benefits and services.

privacy matters in the age of big data, both in the context of the State and private entities, and examine the consequences of the loss of such privacy in Section 3. The right to privacy against the State is premised on the idea of personal freedom in a liberal democracy, and primarily focused on surveillance. The right to privacy against private actors on the other hand is founded on principles of contract law, most prominently involving notice and consent, and focused on the collection, storage, processing, transfer, and use of personal data of customers for business purpose. In both cases, inadequate privacy protection can have significant consequences - ranging from identity theft, and increased profiling and discrimination of individuals to a loss in free speech due to an ensuing "chilling effect".

We next elaborate on the state of privacy law and regulations in India in Section 4, and find that India lacks any authoritative guidance on privacy principles, and in fact, the very basis of the right has been put to question. In an environment of pervasive surveillance and intrusive technology, we argue in Section 5 that there is a need for improved protection of privacy rights through a mixture of legislation and regulation. The Supreme Court may, or may not, eventually consider privacy as a fundamental right. However, that should not stop the State from defining the circumstances in which it may intervene with an individual's rights, and private entities use and share individual data.

There are four questions that assume importance: a) whether, and if so, when, individual control should be prioritised over data, b) what is the role of consent and choice of individuals, c) whether the focus should be on collection, use and release of data by the State and third parties, and d) what are the means of accountability and measures of redress. These questions can only be answered by looking at the principles that would underlie a national privacy law. Section 6 describes the principles that would underline such a law while Section 7 proposes a framework for a privacy law in India. Our endeavour is to provide a usable structure that can be applied to assess the privacy implications of any legislation.

We use this framework to evaluate the Information Technology Act, 2000 [IT Act] in Section 8 and the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits, and Services) Act, 2016 [Aadhaar Act] in Section 9.

It is also important to note the limitations of this framework - given that the paper is contextualised in the age of big data, it does not deal with traditional modes of surveillance and information gathering. Further, while privacy is understood variously as being linked to decisional autonomy, secrecy, and freedom from intrusion, both in the physical and information data sphere, we focus primarily on data privacy and the privacy of personal information. Finally, it is important to bear in mind that any law on privacy will have the unenviable task of keeping pace with the development of technology.

2. What is the right to privacy?

Before proposing a privacy framework, it is important to spend some time understanding what is meant by the term "privacy", and how we plan to use it in this paper.

There are various accounts and definitions of privacy. A 'descriptive' account of privacy views it as a condition or state of being (Moore, 2008). Thus, at the lowest common denominator, it is seen as the *right to be left alone* (Warren and Brandeis, 1890), or *being able to be free from certain kinds of intrusions* (Scanlon, 1975). According to Parent, (1983) privacy is the *condition of not having undocumented personal knowledge about one possessed by others*. Thus, in such an account, the right to privacy would include a bundle of rights such as the right to privacy of beliefs, thoughts, personal information, home, and property.

This is also recognised internationally in Article 8 of the European Convention of Human Rights [ECHR] and Article 17 of the International Covenant of Civil and Political Rights [ICCPR] as the right to respect for private and family life, home and correspondence. A similar notion has been incorporated in the Fourth Amendment of the US Constitution, which protects the people against unreasonable search and seizures. This is premised on the notion that "a person's home is their castle", which is a zone of privacy that is secure from the prying eyes of the State (Cooley, 1871; Hafetz, 2002).

The descriptive account of privacy stands in contrast with the 'normative' account of privacy, which understands privacy as a moral claim against third parties to desist from certain actions (Moore, 2008). The former answers the question - why value privacy?. Under such an account, privacy has come to be viewed as central to our identity, dignity, sense of self, and ability to have intimacy and meaningful inter-personal relations. It is also seen as the claim of individuals to "determine for themselves when, how, and to what extent information about them is communicated *to* others" (Westin, 1967). Privacy, thus, determines our interaction with our peers, the society and the State, and our power to control and share information selectively.

Such a normative account of privacy, underlying the dignity and autonomy of an individual, was recognised by the Inter-American Court of Human Rights in *Artavia Murillo et al. ("*In Vitro Fertilization"*) v Costa Rica (2012)*, while deciding a challenge to the presumed general prohibition of in vitro fertilisation in Costa Rica. The IACHR ruled that the protection of private life includes a "series of factors associated with the dignity of the individual", including, for instance, the ability to develop one's own personality and aspirations, to determine one's own identity, and to define one's personal relationships.

There are other accounts and definitions of privacy as well. As we explain in the appendix, different countries have adopted differing approaches to privacy. Privacy has also been studied as a relational concept, based on the nature of inter-personal interaction

(Green, 1934); as an account of control and access (Parker, 1974); and as a cultural[4] concept (I. Altman, 1977). It also has to be understood in respect of the answer to the question - privacy from whom (Hetcher, 2001), whether the State or a private actor?

Our view, in line with that of Solove (2008), is that a single definition of privacy is "not possible, and perhaps not necessary", so long as its value and meaning are understood in a comprehensive fashion. In our paper, we view privacy primarily from a descriptive account, being the right to privacy of personal information, and then try and understand why we worry about the actions of the State and private entities from a normative perspective.

[4] For instance, Germany has one of the strongest data protection and privacy laws in the world, in part due to its history and the rise of the Third Reich. On the other hand, India, with its large joint families and way of life, has traditionally not viewed privacy as a central tenet to daily living, although this is changing.

3. Why does privacy matter?

Privacy is rarely eroded by a single act or by a single person. Instead it comprises multiple small acts of surveillance and information collection, both by the State and private actors from the monitoring of our call records and the contents of our calls to tracking our movement and browsing history. The advancement of big data technologies and the ensuing ease of re-identification has disrupted the faith placed in anonymisation and pseudonymisation as measures to protect the privacy of an individual (Sweeney, 2000; Narayanan and Shmatikov, 2008; Ohm, 2010).[5]

If we think of privacy as secrecy i.e. the right to keep certain information about ourselves private, we need to ask why do we care if information about us is being collected? The most obvious answer to this is if information about us can be used against us in a harmful manner. Does this vary depending on who is collecting the information? In this section, we first describe the kind of information that is, or can be, collected about us by different entities.

3.1 Loss of privacy from the State

The debate around right to privacy has its origins in the capabilities of the State to intrude into the lives of its citizens. Traditionally, individuals have different privacy expectations from different classes of people and have a greater privacy expectation from the State than from their friends and acquaintances.

This is because governments wield enormous influence and have coercive powers including those related to law enforcement and criminal justice, making citizens wary about the invasion of their privacy by the State (Sacharoff, 2012). Thus, information about individuals, especially dissidents and protesters, in the hands of the State, gives cause for worry about the manner in which such information can be used against them in an unforeseeable manner.

The pervasiveness of State surveillance is perhaps best exemplified through programmes such as those conducted by the NSA/GCHQ. New forms of electronic surveillance have now made it almost impossible for us to even realise that our privacy is being infringed, or to know what information is being held about us. The Snowden revelations have proved that data collection, retention and analysis by the State is an immutable reality and that we have effectively, as the UK Information Commissioner Richard Thomas put it, "sleepwalked into a surveillance society" (Booth, 2004).

[5]A recent study analysing three months of credit card records of 1.1 million individuals found that using only four spatio-temporal points was enough to uniquely re-identify 90% of individuals.

The basis for such fears in India also seems real, when we consider the current surveillance regime we operate under. The Software Freedom Law Centre in its Report on Surveillance in India, found on the basis of RTI inquiries, that, on average the Central government alone taps more than 1 lakh phone calls a year, while issuing around 7500-9000 phone interception orders monthly. Combining this with requests from the State Government, the Report frighteningly concluded that "Indian citizens are routinely and discreetly subjected to Government surveillance on a truly staggering scale" (SFLC, 2014). There are three systems that are worth mentioning in this context (Montjoye et al., 2015):

i. The "Centralised Monitoring System" (CMS) allows authorised security agencies to instantly intercept and directly monitor communications on mobile phones, landlines and the internet in the country (including on social media) to "strengthen the security environment."

ii. The soon to be launched internet spy system, "Networks Traffic Analysis" (NETRA) is going to be equipped to analyse internet traffic (including emails, blogs, VoIP like Skype, internet forums etc.) based on pre-defined search filters and will facilitate multiple-user access to security agencies (PTI, 2014).

iii. The NATGRID project seeks to create a centralised database streaming sensitive information from 21 data sources, including banks, travel details etc. (Press Information Bureau, 2015).

These examples help demonstrate that the government's surveillance capabilities have vastly improved over the last couple of decades, leading to a real possibility of mass surveillance, as opposed to targeted surveillance. The emergence of such new technologies comes with the possibility of misuse, especially considering the relatively low level of effective oversight and awareness about such programmes.

In fact, similar mass surveillance concerns have also been raised in the context of centralised data collection under the Aadhaar Card Scheme in India (Abraham, 2015; Dreze, 2016; Ramanathan, 2016b). Under this scheme, the Government of India has been collecting and compiling the demographic and biometric information of its residents for use for various purposes since 2009-10. This information is then stored in a centralised data repository, and the residents in turn are issued a 12-digit unique identity number, i.e. their Aadhaar number.[6] Even apart from surveillance, the Aadhaar Act raises a host of privacy concerns that will be dealt with later in Section 9.

Besides surveillance, governments across the world, and in India are under pressure to release data about their functioning in order to promote transparency and good

[6] This scheme was finally given statutory backing with the passage of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits, and Services) Act, 2016 [Aadhaar Act] in early 2016. The Act undertook such collection and storage of demographic and biometric information of residents in India for their use in targeted delivery of subsidies, benefits, and services.

governance. This has meant that large amounts of information about individuals, as well as agencies, is being continuously released to the public, without a consistent framework that accounts for privacy of data subjects (M. Altman et al., 2016).

3.2 Loss of privacy from private parties

Traditionally, we have worried about safeguarding citizens' privacy from the instrumentalities of the State, particularly in relation to surveillance. Private actors were never really the focus of the debate. This has, however, changed with the rise of big data and of global corporations such as Google, Facebook, and Amazon, whose business model relies on the collection, storage, and use of customer data. It has also been aided by the increasing popularity of social media, which encourages people to share more information about themselves.

The emergence of data as the new currency has resulted in the creation of an entire industry around the buying and selling of personal information to third parties. This industry "now exists to commoditize the conclusions drawn from that data" (Podesta et al., 2014). Private actors also have a deep interest in our lives and actions, in terms of tracking and possibly sharing information about what we read, what we write, where we are, and ultimately, what we think. This behaviour is not dissimilar to that of the State.

Despite increasing awareness about online privacy and demand for simplified terms of service, firms have not changed their behaviour. In fact, as Hetcher, (2001) points out, private actors have focused on "simulating privacy *respect* rather than providing the *real* thing*."* The debate around the right to privacy against private entities is thus centred on principles of notice and consent and collection and use limitation, that underlie the contract (terms of service) between the user and the company.

The primary distinction between the private sector and the State relates to security considerations that influence the actions (and surveillance targets) of the State. However, given the ease of tracking our movements through geo-location and Wi-Fi on smartphones, and the data sharing requests sent by the Government to these corporations, the difference in the privacy protections sought against the State and private entities is slowly disappearing.

For example, in 2011, Google ranked India as the third most intrusive State, after USA and Brazil, in terms of number of requests for data on users - 1430 user data requests were made to Google alone during January to June 2010 (Times, 2011). Five years later, this number increased to 3087 user data requests for the period of January to June 2015 (Google, 2015) and India is now ranked the second most intrusive State after the United States (Khedekar, 2013). Such requests are not limited to Google alone. Facebook and Twitter have also reported a spike in the Indian governments request for data of its users or for data removal (Bhargava, 2015).

3.3 Consequences of Inadequate privacy protections

We have, so far, described the threats to the privacy of individuals from the State and private actors in the age of big data. However, this still leaves the question - Why does it, or should it, matter to us if the State is keeping tabs on the movement of its citizens (especially if it is in public interest for security purposes) or if private actors are storing and sharing personal information about their users? More specifically, why does it matter if such actions are undertaken without any safeguards to privacy?

Very often the notion of privacy is countered by a variation of the "have nothing to hide" argument. Under this view, only people with something to hide are concerned about the loss of privacy. If you have nothing to hide, then information about you cannot really be used against you.

In this section, we explain why such a view is wrong, and why the consequences of inadequate privacy protections go far beyond this nothing to hide paradigm, and extend to concerns about the loss of breathing space, chilling effect, identity theft, and potential profiling and discrimination.

3.3.1 Loss of breathing space

Let us think about a typical home in the 21st century. Very often the residents of the home will draw their curtains so that they are not visible to their neighbours, or to passerby's on the street. Most people will certainly draw the curtains in the evening, once they switch on the lights in their house. They may not necessarily be committing an immoral act, or doing something that needs to be hidden, but because, their home is their space, to do and be as they like, free from the gaze of others. Now imagine, that drawing curtains is not possible, or drawing curtains will bring allegations that there must be something immoral going on inside the house - for if the person had nothing to hide, why were curtains being drawn?

This example underscores the problem with the nothing to hide paradigm, as it makes a moral judgment about the kinds of information people want to hide. As described in the example above, privacy is important from the point of view of self- development, and in fact, is a shorthand for "breathing space" (Cohen, 2012). An integral part of individual autonomy is the ability to make, and be answerable for, one's own choices, maintain different and intimate relations with different persons, and exercise power over the information one wishes to make about them public (Rossler, 2005).

The loss of privacy, or even the fear thereof, however seemingly harmless whether in monitoring the websites accessed or the number of times a place of worship is visited may eventually influence these patterns of behaviour and content of conversations (Rachels, 1975). It may result in an unconscious change in behaviour if where we eat, who we meet, what we say, and even what movies we enjoy, is subject to scrutiny.

The issue thus has to do with being observed, rather than the content of one's actions, since it is likely that we will behave according to a set of expected social norms rather than our own free will and autonomy, when we believe we are being observed (Introna, 1974). This is likely to lead a society to become a "modulated democracy" where citizens are subject to modulation by powerful commercial and political interests (Cohen, 2012).

3.3.2 Chilling effect on free speech

The loss of breathing space and autonomy that result as a consequence of insufficient privacy protection, will have a knock-on chilling effect on other rights, such as the right to freedom of expression and freedom of association as observed by the UN Special Rapporteur, Frank La Rue.

Individuals may be chilled into silence in their online communications if, for instance, they cannot be assured that their communications are private (Human Rights Council, 2011). President Obama's Review Group on Intelligence and Communications Technologies has reached a similar conclusion, noting, "if people are fearful that their conversations are being monitored, expressions of doubt about or opposition to current policies and leaders may be chilled, and the democratic process itself may be compromised" (Clarke et al., 2013).

One of the foundations of a liberal democracy is the ability to dissent, and to hold views that are unpopular without fear of retribution either by the State or a lynch mob. We are less likely to express a contrarian or controversial view point, or organise social change, if we fear the monitoring and storage of our views and consequent action. This chilling effect will induce self-censorship due to the fear of surveillance and the coercive power of the State and how our speech might be used against us.

While largely a concern of privacy protections from the State, the consequence of the chilling effect is also felt in the domain of private actors, since developments in big data analytics has made it possible that our actions on social media can predict our personal attributes, and maybe in the future, even our private thoughts. A recent study found that Facebook "likes" of an individual could be analysed to predict with reasonable accuracy their ethnicity, religious and political leanings, sexual orientation, personality traits, intelligence, and even use of addictive substances (Kosinski, Stillwell, and Graepel, 2013). This, thus, brings the fear of chilling effect of free speech, central within the interaction between the private actor and the user.

3.3.3 Identity theft

One way in which personally identifiable information can be misused is identity theft (Rockelmann, Budd, and Vorisek, 2011). This has been defined as the combination of unauthorised collection and fraudulent use of the personal information of another individual (CIPPIC, 2007).

Identity theft allows a person to gain unauthorised access to an individual's private information, and use it for their own benefit by masquerading as that individual. Personal information can range from financial information such as credit card details (which can be altered) to inalienable characteristics such as biometric information (which cannot be altered).

Unlike in the case of theft of personal property, where the individual often has the ability to replace the stolen items, identity theft has more severe/long term ramifications in terms of the ability to restore one's stolen identity.

Concerns about identity theft have only increased with the data deluge caused by the rise in big data. We now live in a world where progress in data mining and analytics has led to an ease of re-identification, de-anonymisation, and the possibility of making connections across different datasets (Tene and Polonetsky, 2013), thus making the consequences of loss of privacy more profound.

3.3.4 Profiling and discrimination

The advent of big data has meant that analytics can identify statistical relationships between discrete data sets, and use this to predict seemingly unrelated outcomes (Barocas and Selbst, 2016). Data from previous instances of payment default on loans, as an example, can be fed into a machine learning algorithm, which can then identify characteristics or activities that serve as proxies for the outcome of interest (Barocas and Selbst, 2016). This can have a bearing on our relationships in the marketplace, and can result in discrimination.

Consider the example of a credit algorithm that scores migratory jobs lower than others. This by itself may not have a discriminatory intent but will tend to have a disparate impact while assessing loan applications if mostly minorities or individuals from a particular area or caste are engaged in such work (Citron and Pasquale, 2014).

Consider another example - Acurian Inc., one of America's biggest recruitment companies, uses seemingly harmless personal information such as a preference for jazz music, being a cat owner or participating in sweepstakes to help recruit patients for an arthritis study. As Acurian's Vice President, Roger Smith told Wall Street Journal, "we are now at a point where, based on your credit card history, and whether you drive an American automobile and several other lifestyle factors, we can get a very, very close lead on whether or not you have the disease state we're looking at" (Walker, 2013).

Moving from the commercial realm, big data's application in law enforcement, whether it is in tracking search results to identify human trafficking networks or in creating a more rounded suspect profile, has meant that large swathes of personal information about an individual become known to the police.

One of big data's more controversial uses comes 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 counties in the US, such as Chicago, Boston, New York, Washington DC and Los Angeles, it is slowly being embraced by the Indian police, particularly in New Delhi (Sumit Singh, 2015; Shekhar, 2015) and Jharkhand (Routray, 2012). 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.

All of the examples can also be touted as the benefits of "big data" and many of them are. Statistical discrimination may lead to benefits for several customers, and enable companies to actually provide better services and more competitive pricing. Predictive policing may be able to prevent crime. But before we applaud these benefits we need to keep in mind the possibility that predictive modeling may lead to several Type I and II errors, with severe ramifications for the persons concerned. We also need to be mindful that we may be creating a self-fulfilling prophecy since the cost of transactions for already at risk groups automatically increases, making it harder to further transact in the market place.

If we believe that we have a right to be protected from discrimination on the basis of immutable personal characteristics such as religion, caste, or gender as well as the right to make intimate personal decisions, then the instances of profiling and discrimination that big data makes possible should alert us to the costs of loss of privacy. A more detailed conversation is necessary about the use of big data in law enforcement, and in commerce.

Our privacy concerns should thus extend to the use and sorting of such data into a discriminatory or disfavoured pile, which can potentially overshadow long-standing rights protections in the use of personal data in varied sectors such as health, education, employment, housing etc. (Podesta et al., 2014).

4. The right to privacy in India

As we have discussed in the previous section, the costs of inadequate privacy protections are manifest, even when individuals have nothing to hide. However, this does not necessarily imply that the government can never engage in surveillance, or the private sector can never collect data which will result in a loss of privacy. Instead, we would like to make a case for having meaningful methods of oversight and accountability in cases of data collection and surveillance by the private sector and the government. In this section, we evaluate how well the Indian legal and regulatory landscape carries out these functions.

4.1 The regulatory framework

At the outset, it is important to reiterate that there is no privacy law in India. Hence, the activities of the State and the private sector are regulated through sector-specific laws and the jurisprudential development of the right to privacy.

The interaction between the State and its citizens that has immediate privacy implications involves surveillance. The State has many justifiable reasons for surveillance, especially on grounds of national security. The important question, however, is whether there are adequate oversight mechanisms when such surveillance is conducted, and whether such surveillance is actually connected to security considerations.

In Indian law, surveillance or tapping is authorised under the Indian Post Office Act, 1898 providing for the interception of postal articles, and Section 5(2) of the Indian Telegraph Act of 1885 (read with Rule 419A of the Indian Telegraph Rules, 1951), regulating the interception of messages, along with the relevant Police Rules. These laws deal with targeted surveillance.

The Telegraph Act and Rules provide for a two-tiered threshold test, which require first, "the *occurrence* of a public emergency, or in the interest of public safety" to empower the Central or State government or any officer authorised therein to order the interception of postal/telegraphic messages. Second, interception is permitted only "if it is satisfied that it is necessary *or* expedient *so* to do 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". Pertinently, the definition of "telegraph" under Section 3(1AA) of the Act is broad enough to cover communication via telephone.

Apart from post and telephone/telegraph surveillance, internet surveillance is governed by Section 69 of the Information Technology Act 2000 [IT Act], which is modelled along the lines of the Telegraph Act. However, there are three notable distinctions that make State surveillance easier under the IT Act. It is important to remember that surveillance by private actors is not authorised or permitted under the IT Act.

i. Section 69 of the IT Act does away with the pre-requisites of "public emergency" or "public safety" for the appropriate government to "intercept, monitor or decrypt" internet data.

ii. The IT Act widens the second-tier of the test under the Telegraph Act by providing for two additional grounds when it is considered necessary or expedient to intercept in the interest of the "defence of India" and the "investigation of any offence".

iii. The IT Act imposes an additional obligation on all internet service providers (the intermediaries), the subscriber and the person in-charge of the computer resources to "extend all facilities and technical assistance" to the intercepting agency, or face imprisonment up to seven years.

Thus, it is clear that Section 69 considerably widens the governments surveillance avenues when compared to telephone interception under the Telegraph Act.

Finally, internet metadata can be monitored and collected by "any" government agency under the low threshold of "enhanc[ing] cyber security" or for *"*identification, analysis and prevention of any intrusion or spread of computer contaminant in the country*"* under Section 69B of the IT Act. This section deals with the power to authorise to monitor and collect "traffic data" (which has been widely defined) or information through any computer resource for cyber security.

While our regulatory surveillance architecture does implicitly recognise some notion of the right to privacy, it is heavily weighted in favour of the State. The IT Act gives a flavour of how electronic surveillance, even much more than physical surveillance, enables extremely intrusive forms of tracking.

However, as we have discussed throughout this paper, concerns of privacy also exist in the private sector, with the advent of big data rendering obsolete many of the traditional methods of de-identification. These concerns assume an increased importance in light of the outsourcing industry in India (Patel and Conners, 2008), which makes it all the more important for companies to adopt privacy policies that focus on the security of the personal data.

Currently, only the IT Act provides for extensive regulations on the storing and sharing of consumer data collected by businesses, but as we elaborate later, these protections are inadequate. Even the recent Aadhaar Act, although ostensibly dealing with the interaction between the State and the residents of India, allows corporate entities to access the centralised database, without appropriate privacy safeguards.

4.2 The jurisprudential development of the right to privacy

In most jurisdictions in the world, questions on State surveillance are evaluated in the context of how the State understands, recognises, and balances the *right to privacy* of its

citizens.

Article 12 of the Universal Declaration of Human Rights, Article 8 of the European Convention of Human Rights [ECHR] and Article 17 of the International Covenant on Civil and Political Rights [ICCPR] recognise privacy as the *right to respect for private and family life, home and correspondence*.

The Fourth Amendment of the US Constitution also secures the rights of the people in their persons, houses, papers, and effects against unreasonable search and seizures, being premised on the notion that a "person's home is their castle".

Unlike the American Constitution or the ECHR, the Indian Constitution is silent about the right to privacy or private life or the protection against unreasonable searches and seizures. It is thus an un-enumerated right. However, India has ratified the International Covenant on Civil and Political Rights, which unequivocally supports the existence of the right to privacy.

The development of the law on privacy began with the decision of the eight-judge bench of the Supreme Court in *M.P. Sharma v Satish Chandra, (1954)*, which in the perspective of search and seizure articulated that, *"*When the Constitution makers have thought fit not to subject such *regulation* to constitutional limitations by *recognition* of a fundamental right to privacy, analogous to the *American Fourth* Amendment, we have no justification to import it, into a totally different fundamental right, by some process of strained construction.*"*

This was followed nearly a decade later in *Kharak Singh v State of Uttar Pradesh, (1964)*, where a six judge bench of the Supreme Court observed in a case involving surveillance, *"*The right of privacy is not a *guaranteed* right under our Constitution and *therefore* the attempt to ascertain the movements of an individual which is merely a manner in which privacy is invaded is not an infringement of a fundamental right *guaranteed* by Part III.*"*

*How*ever, after the 1970s, the Supreme Court started interpreting the right to privacy and the right to life and personal liberty under Article 21 of the Indian Constitution more expansively as is evident in its two-judge bench decisions in *Gobind v State* of *Madhya Pradesh, (1975)*, *Auto Shanker (1994)* and *PUCL v Union of India, (1997)*.

In *Gobind v State of Madhya Pradesh, (1975)*, the Court quoted Justice Brandeis' dissent in *Olmstead (1928)* to conclude that the framers of the Constitution "must be deemed to have conferred upon the individual as against the government a sphere where he should be let alone." Similarly, in *Auto Shanker*, the Court clarified that the right to privacy was "implicit" in the right to life and personal liberty under Article 21 of the Constitution and was the "right to be let alone" to safeguard the individual's privacy and that of his *family, marriage, procreation, motherhood, child-bearing and education* among others. Importantly, in *PUCL v Union of India, (1997)*, the Supreme Court held that "prior judicial scrutiny" was not a mandatory requirement for the authorisation of surveillance, and issued a series of guidelines in this regard.

Thus, as argued by Acharya (2015), case law in India has led to four types of privacy claims: (i) protections against press intrusions and the right to information from public sources or about public conduct of officials, (ii) privacy from state surveillance, (iii) privacy as decisional autonomy which gives an expanded interpretation of the ideas of personal liberty and individual sovereignty, which would comprise the ability to freely express one's identity, including sexual identity (and was cited in the Delhi High Courts (overturned) decision in Naz Foundation on s. 377 and decriminalising private consensual homosexual relations) and finally privacy pertaining to the collection, storage, use and sale of personal data of individuals.

However, in 2015, during the hearings defending the challenges to the Unique Identity scheme (Aadhaar) rolled out by the Government, this conflict in the jurisprudence between the decisions of the larger and smaller benches of the Supreme Court was relied upon by them to argue that the right to privacy was not a fundamental right, and was only a "vague" concept. Taking this into consideration, the Court in Justice K.S. Puttaswamy (Retd.) v UOI and Ors, (2015) put into question whether the right to privacy is a fundamental right at all under Part III of the Indian Constitution and referred the following questions to a larger five judge bench.

i. Whether there is any "right to privacy" guaranteed under our Constitution.

ii. If such a right exists, what is the source and what are the contours of such a right as there is no express provision in the Constitution adumbrating the right to privacy.

It is interesting that while the Supreme Court of India has put into question the status and contours of the right to privacy, cases with serious privacy implications and violations are being filed in different High Courts across the country. The Delhi High Court in *Laksh Vir Yadav v UOI and Ors, (2016)* is currently hearing a petition on the right to be forgotten, i.e. on whether the right to privacy includes the right to delink from the internet irrelevant information. In September 2016, the Delhi High Court in *Karmanya Sareen v UOI and Ors, (2016)*, also ruled on the WhatsApp-Facebook data sharing arrangement.[7] The case, once again, also brought to light how the Central Government and the Telecom Regulatory Authority of India regulate the functioning of ISPs, there is no statutory framework for the regulation of internet messaging applications such as WhatsApp.

[7] WhatsApp, having been acquired by Facebook in 2014, put in place a new privacy policy in August 2016 informing its users that their account information would be shared with Facebook and all its group companies, to improve Facebook ads and products experiences. The Court in its judgment, directed that the existing user details up to 25.09.2016 of those who opt to remain with WhatsApp shall not be shared with Facebook. Conversely, if a user opts for deleting their WhatsApp account before 25.09.2016, their details will be completely deleted from the WhatsApp servers and will not be shared with Facebook.

5. The need for a privacy law

The reference by the Supreme Court has, in essence, resulted in overturning a seemingly settled position about the importance of the right to privacy after 60 years. At the same time, the regulatory surveillance architecture in India is heavily weighted in favour of the State. As a result, mass surveillance can be carried out, effectively in a legal vacuum, with little regard for the effect on individuals' rights to privacy.

The Supreme Court may, or may not, eventually consider privacy as a fundamental right. However, that should not stop the State from defining the circumstances in which it may intervene with an individual's rights. The right to property is not a fundamental right in India. Nevertheless, India has still enacted the Land Acquisition Act and there is heated debate about the circumstances in which the State may take away land and the due process for this. Why should privacy be any different?

Undoubtedly, privacy is not an absolute right and will always have to be considered against competing rights such as the public interest, public order, and national security. However, in absence of any foundational and constitutional basis, and devoid of theoretical clarity, the right of privacy of an individual will most likely be subordinated in favour of public or State interest when decisions regarding surveillance arise.

As argued earlier, the advent of big data has also meant that data collection, and use are carried out on an unprecedented scale by the private sector. The problem is compounded by 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, Bolsover, and Dubois, 2014). Their self-disclosure of information is not related to their concern or knowledge about the inadequacy of privacy controls, but rather is based on the social relevance of the app or the peer usage.

Competition in the market place, thus, may be inadequate to protect user rights for two reasons, necessitating the intervention of the State:

Information asymmetry: Big data technologies, in our increasingly networked and digitised world, work to increase the asymmetry of information between the individual consumer and the firm/data provider in three ways.

i. They enable data collection that is more ubiquitous, invasive, and valuable.

ii. They enable efficient data mining to combine multiple aspects of a single individual's data and correlate it with different users' data.

iii. They limit users' ability to protect or delete their information, once shared.

The interest in the industry is accompanied by an increasing under-estimation by consumers about the value of their personal data and ignorance about the scale and precision

of data collection and its associated uses. The fact that data, almost inevitably, involves secondary use for purposes not originally envisioned and involves multiple participants (for collection, storage, aggregation, analytics, and sale), increases the information asymmetry.

Another factor contributing to the rising information asymmetry is that web platforms can covertly or overtly change their privacy policies or information-sharing rules after consumers have signed up. A good example may be that of the popular photo-sharing app Snapchat, where photos are said to disappear or self-destruct in a couple of seconds after they are sent and received. However, subsequent features on the app, such as "Snapchat Stories" or "Our Story" or "Snapchat Discover" now retain the pictures from up to 24 hours to a couple of days. In fact, it has also been discovered that the photos do not actually get deleted, and are only buried deep inside the device (Shontell, 2013).

The above instances demonstrate the market failure in creating time-consistent conditions to enable consumers to make privacy decisions under perfect information. The complexity of requiring consumers to consider multiple outcomes and associated probabilities, instead of purely linear transactions, leads them to "highly imprecise estimates of the likelihood and consequences of adverse events, and altogether ignore privacy threats and modes of protection" (Acquisti and Grossklags, 2007).

Bounded rationality: Under rational choice theory, individuals make time consistent decisions, using all available information to maximise their utility over time. However, studies have shown that the actual decisions taken by individuals, when faced with decisions concerning disclosure of their personal data, do not fall within this pattern. A part of the problem arises from the inability to read and comprehend the fine print of privacy policies and part from bounded rationality, causing a failure to process how personal information is being traded further in secondary markets (Acquistion and Grossklags, 2007; Newman, 2014).

A related cognitive bias is what Brandimarte, Acquisti, and Loewenstein, (2010) term "the control paradox". Here, merely by making individuals *feel* in control over information dissemination, irrespective of their actual control, firms encourage data subjects to reveal more personal information. Similarly, it has been shown that the phrase "privacy policy" has acquired certain normative value, such that simply on seeing the phrase (without reading the policy), users are more willing to believe that their data will be safe and not shared forward (Turow et al., 2007).

These examples challenge the assumption that the market can solve the problem by making concerned rational individuals pay more to protect their privacy. Apart from failing to understand the fine print of privacy policies, we see that individuals often view such policies as guarantees of data protection, instead of liability disclaimers for firms (Tene and Polonetsky, 2012).

Thus, privacy protections are required not only from the State but also from the private

sector. In fact, a recent Nasscom-DSCI survey showed that inadequate data protection frameworks were causing losses worth billions of dollars to the Indian IT-BPO sector, in part because India's data protection regime was not considered 'adequate' by the EU (Nasscom, 2013; Alawadhi, 2015).

In the face of ambiguity regarding the status of the right to privacy as a fundamental right, the absence of any statutory privacy code, ineffective mechanisms to safeguard against the violation of one's privacy, outdated applicability of the PUCL surveillance safeguards, and the inability of the market to provide privacy protections, it is necessary to enact a privacy law.

Such a law would provide an authoritative guidance on privacy rights in an era of surveillance and electronic communication. It would define key terms, govern the rights of users, detail the obligations of the State, lay down privacy principles and exceptions, provide guidance on resolving privacy-security conflicts (for instance, by applying a European proportionality test)[8] and would delineate various redress and compensation mechanisms.

However, before proposing a framework for the proposed privacy law, it is important to understand the privacy principles that would underlie such a law.

[8] The European Court of Human Rights and the European Court of Justice evolved the proportionality test in the context of the right to private and family life under Article 8 of the ECHR. Article 8 is not an absolute right and has to be considered against competing rights such as security. Thus, in determining whether the processing of certain data or an interference with an individual's right to privacy is permissible, the Court evaluates whether it is proportional - i.e. whether the interference is for a legitimate aim, is in accordance with law, and is necessary in a democratic society (or the least restrictive means available). See *Handyside v United Kingdom*, Appl. No. 5493/72 (ECtHR 7 December 1976).

6. Principles

There is a general consensus amongst countries on internationally accepted privacy principles, whether it is the OECD, (2013) Privacy Principles, the APEC, (2005) Privacy Framework, the European Directives on Privacy (European Commission, 2012; Boillat and Kjaerum, 2014) or the data protection laws in countries such as the Canadian Personal Information Protection of Electronic Documents Act 2000 (as amended by the Digital Privacy Act of 2015), the English Data Protection Act of 1998, and the American Consumer Privacy Bill of Rights (White House, 2015).

These principles were relied upon by the 2012 Committee Report of the Group of Experts on Privacy chaired by Justice Shah ["**Justice Shah Report**"] to recommend the following nine principles to form the foundation of a proposed Privacy Act in India. In this paper, we use these nine principles of the Justice Shah Report, (2012), as understood by us, as the basis for a national privacy legislation in India. The privacy principles are enumerated below:

Notice: This implies that a data controller[9] should give all its users notice of its information practices and data processing activities, prior to their registration on its website or services. Such a notice should be simple and concise, so as to enable users to understand the practices followed by the data controller in respect of their personal information and then decide whether to give informed consent about the same.

One of the most common examples of the principle of notice are the terms of service or privacy policy encountered by users when signing up to different online services such as Facebook, Gmail, Snapchat or Twitter. For instance, the Twitter Privacy Policy *"*describes how and when Twitter collects, uses and shares your information when you use our Services.*"* (Twitter, 2016a)

Choice and Consent: This principle requires a data controller to give its users the choice, through opt-in/opt-out provisions, of whether to provide their personal information to sign up on its website. After that, the data controller needs to take the consent of its users for the collection, use, and processing of such personal information.

For this principle to be effective, it is necessary to give users proper notice of the data controller's practices. Thus, continuing with the example above, the Twitter (2016a) Privacy Policy states that "when using any of our Services you consent to the collection, transfer, storage, disclosure, and use of your information as described in

[9] A data controller is an organisation, institution or a person who determines the purposes and the manner in which personal data is processed. The term is widely used and defined, both in European law, specifically Regulation (EC) 45/2001, and in the UK Data Protection Act.

this Privacy Policy".

However, for consent to be truly informed, the notice should be easy to read and understand. Notice and consent are the bedrock of all privacy regulation today (although this is changing), since they function on the premise that users have knowingly parted with their personal information after understanding and consenting to the data controller's collection, storage, and use of their information.

Collection Limitation: As a principle, this is intended to limit the amount of personal information collected by the data controller only to what is necessary for the purposes identified for such collection. This is premised on the idea that even after users consent to share their data, the data controller does not have an unrestricted right to collect their personally identifiable information, *unless* such collection is necessary, fair, and collected through lawful means.

For instance, Twitter, and other apps such as Google Maps and Facebook, collect the location of its users, using information from its users' devices "such as precise location information from GPS, information about *wire*less networks or cell towers near your mobile device, or your IP address" (Twitter, 2016a). This is considered to be consistent with the principles of collection limitation since users are expressly notified about the nature of information being collected, the modes of collection, and the purpose for which location information is being used.

Purpose Limitation: This principle, also termed as 'Use Limitation', requires data controllers to use the personal data only for the specified purpose for which it was collected, and not for any further purpose. Thus, if Twitter collects the credit card information of its users for a specified commerce transaction on its server, it cannot then share that payment information with a third party, since that was not the original purpose of the collection of data. It is on account of such a principle that Twitter, (2016a) makes it clear that "we consider your Payment Information and shipping address private and do not make such information public".

The 'Purpose Limitation' principle also requires that after the information has been used, it should be deleted and that any change in the purpose for which the data was originally collected has to be notified to the users, so that they can determine whether to continue their consent. Combined with the principle of Disclosure, it protect users, and notifies them for instance, when their credit card information entered online is shared with third parties. With the advent of big data and ease of collection and storage of information, there has been a shift in the emphasis from Collection Limitation to Use Limitation.

Access and Correction: This privacy principle grants users the right to access their personal information, held by data controllers, and correct them if necessary. By allowing users to access and correct their personal information, such as address,

account details, or social security number, this principle ensures the veracity of the personal data stored (and shared) by the data controllers. Since the data stored in such databases forms the basis of multiple onward transactions whether for targeted advertisements or to determine an individual's credit rating it is important to ensure the accuracy of the information.

Disclosure of information: The Disclosure principle applies in the context of the data controller sharing the personal information of its users with third parties. It requires the data controller to provide notice of such disclosure to its users, and obtain their informed consent to the onward sharing of their personal data. The third party is then required to abide by these privacy principles, even after consent has been withdrawn, and cannot de-anonymise information that was anonymised for the transfer.

Part of the increasing popularity of data controllers such as Google, Amazon, Facebook and Twitter with other companies and advertisers is the vast swathes of data continuously collected and mined by them. It is thus important to require these data controllers to disclose their practices of sharing this data with such third parties for commercial gain.

Companies try and get around this principle by incorporating vague statements in their privacy policies. For example, the Twitter, (2016a) privacy policy stipulates that *"*Third-party service providers may collect information sent by your device as part of a web page request, such as cookies or your IP address. Third-party ad partners may *share* information with us, like a browser cookie ID, website URL visited, mobile device ID, or cryptographic hash of a common account identifier (such as an email address), to help us measure and tailor ads.*"* The wording of this disclosure clause and the use of the word "may" is indicative of the manner in which data controllers try and retain the maximum possible flexibility in sharing the data of their users with third parties.

Security: This principle deals with the technical, physical, administrative, and technological measures put in place by data controllers to safeguard against the unauthorised access, use, modification, de-anonymisation, or disclosure of any personally identifiable information of its users. It thus functions as a preventive measure since the security practices of data controllers should be able to prevent any deliberate, negligent, or accidental unauthorised use or disclosure of information.

Openness: This principle focuses on making the internal privacy policies and practices of data controllers accessible, and available in a transparent and easy to understand manner. It pushes data controllers to fully disclose their information practices and any change of terms, so that users can decide whether to continue their consent, as in the case of Snapchat above.

Data controllers are encouraged to refrain from making vague statements about their privacy policies. Thus, Twitter (2016a) states that "if we make a change to this policy

that, in our sole discretion, is material, we will notify you via an @Twitter update or email to the email address associated with your account." It is thus clear that Twitter wants to be the final arbiter of whether any change in their terms of service is "material" enough to warrant notifying their users, which undermines the Openness principle.

Accountability: The Accountability principle is possibly the foundational privacy principle, since it ensures the data controller's compliance with the remaining privacy principles, often through the means of the law or regulations. For instance, data controllers can be required to implement privacy policies, have external and internal audits, and even conduct the requisite training sessions to spread awareness about the governing legal regime.

While the Security principle functions as a preventive measure, the 'Accountability' principle serves a curative purpose, although its success is predicated on an effective enforcement mechanism and self regulation.

These principles also seem to have been accepted by the Government in a draft 2014 leaked version of the Privacy Bill, although, notably, this draft has not been made available online for public comments (Hickok, 2014).

Apart from these principles, which should underlie any national privacy law, we believe that the ideas of "data minimisation" (limiting the collection and retention of data), "privacy by design" (incorporating data protection requirements in the design of information systems), and "data breach notification" (informing users/public about data breaches), should become part of the legal framework. Before moving to a framework for the proposed privacy law, it is important to consider how privacy has been understood globally.

7. Framework of the proposed privacy law

A privacy law has to inevitably deal with two competing concerns. The first is that of national security vis-a-vis privacy. The second is that of the big data's multitude of benefits vis-a-vis privacy. The design of a law, therefore, is a not a simple question of enacting a law where privacy trumps every other consideration be it security or big data benefits every time. The proposed privacy law has to recognise and be able to resolve such conflicts. To that end, we propose certain design elements that can be a part of a national privacy legislation.

7.1. Objective of the privacy law

A privacy law must begin with the objective that the law seeks to achieve. It must provide for ways of dealing with inevitable conflicts between privacy and security. To this end, the law should contain Privacy Principles that would guide the interpretation of specific provisions.

7.2. Value of personal data

The law is shaped by the value we place on personal data. Value in this context does not mean the market value of the data or how it can be commoditised. Rather, this question refers to the importance we give to the privacy of our personal data and how such an underlying philosophy informs the provisions of the law. For instance, Article 8 of the ECHR recognises an individual's *right to the protection of personal data concerning him or her*. The underlying premise of the Charter is that privacy is a comprehensive fundamental right.

Since the Supreme Court of India is currently deciding whether privacy is a fundamental right in *Justice K.S. Puttaswamy (Retd.) v UOI and Ors, (2015)*, it becomes all the more important to express the value of privacy and personal data in the proposed law and connect it to Article 21 of our Constitution. The law should address, either explicitly or implicitly, the value of personal data and the importance of privacy.

However, it is important to recognise that while the right to privacy should include authority over personal data, it should not be limited to it. The right to privacy must be understood by using frameworks of dignity and liberty, touched upon above, to extend it to the right to be left alone. It is our belief that such an understanding will help provide the requisite theoretical underpinning of the law.

7.3. Scope and ambit of the law

The law needs to address the question of what constitutes personal or sensitive data to which it would apply. This definition should be wide enough to ensure the broad applicability of the law, and should be able to account for technological changes that enable re-

identification or indirect identification of an individual.

Section 1 and Section 2 of the Data Protection Act in England differentiate between personal data and sensitive data respectively. Section 1 defines "personal data" widely to mean *data which relate to a living individual who can be identified -*

a) from those data or b) from those data and other information which is in the possession or, is likely to come into the possession of, the data controller and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Section 2 defines "sensitive personal data or information" as personal data consisting of information relating to the data subjects political opinions, racial/ethnic origins, religious beliefs, physical/mental health conditions, commission oralleged commission of any offence and membership to a Trade Union.

Schedule 3 of the Act imposes additional conditions on the processing of sensitive personal data. For instance, personal data can be processed (unlike sensitive data) if data controllers can show it is necessary for the performance of a contract to which the data subject is a party. However, for sensitive personal data, the processing should be necessary to exercise or perform *any right or obligation which is conferred or imposed by law on the data controller in connection with employment* or for example, where the information contained in the personal data has been made public as a result of steps deliberately taken by the data subject.

The US, on the contrary, takes a slightly more restrictive approach, with very few Federal or State privacy laws defining personal information to include information that on its own does not actually identify a person (Halper, Kashatus, and Lucente, 2016).

In an environment such as India with high possibility of discrimination based on caste, religion, health outcomes (for example, having HIV), as well as sexual preferences (for example, homosexuality has still not been decriminalised), we propose that the law treat personal and sensitive data separately, as in the UK. Another reason is that in the US, different sectors have their own privacy frameworks, making it possible to have differential levels of protection given the area in question, whereas in India, these pertain to one comprehensive law.

Sensitive personal data should be defined in an exhaustive and narrow manner and extend to passwords, financial and biometric information, medical records, political opinion, ethnicity/caste, sexual orientation, and religious beliefs. It should have stronger protections in terms of collection, use and consent, especially because it has a higher chance of being used in a discriminatory manner whether knowingly, for instance HIV discrimination, or unknowingly, for instance, Google's alt.suicide.methods discussion group. Thus, even though having additional safeguards for sensitive personal data increases transaction and

compliance costs for the data controller, the benefits of avoiding profiling and discrimination make it worth it. Pertinently, although "sensitive personal data or information" has been defined under the IT Act in India, as we shall see in Section 8, the definition is fairly limited and has been criticised.

The proposed Act should also make clear that it applies to data controllers (both body corporates and non-profits) and government intelligence agencies. Although security considerations may result in the Privacy Principles applying separately to government collection and use of personal information, there should not be a blanket exemption (as in the proposed Aadhaar Bill). This is consistent with our general framework that privacy inheres as a right to all individuals, regardless of whether the entity in control of the personal data is a non-profit or the government, since the ramifications of their unauthorised use of personal data remains the same.

7.4. Coverage

The scope of the national privacy law should make absolutely clear its territorial applicability and personal jurisdiction.

Under EU law, the fundamental right of privacy covers all persons targeted by the State (through law enforcement/surveillance), irrespective of their nationality or domicile. However, under American law, foreign intelligence surveillance whether under the Foreign Intelligence Surveillance Act, the Patriot Act or the Freedom Act differentiates between US and non-US citizens, unlike American law governing ordinary criminal investigations (Boehm, 2015).

In India, the draft 2014 Privacy Bill seems to have extended the right to privacy to all residents of India, unlike the 2011 draft, which limited its scope to Indian citizens (Hickok, 2014). This expansive scope is consistent with the idea of privacy being a fundamental right emanating from Article 21 of the Constitution (which applies to all persons), and should be a part of the proposed privacy law. Even otherwise, given the interconnected nature of most transactions and existing supply chains, it makes business sense if foreigners residing in India are entitled to the same privacy protections as Indian citizens.

7.5. Principles governing collection and retention of personal data

A national privacy law should include a separate chapter on the responsibilities of the data controller, including the government, while collecting, retaining, processing, and sharing data. This helps regulate and limit the scope of their seemingly unrestricted powers.

7.5.1. Collection of data

The principles surrounding the collection of data revolve around two aspects, *first*, the Collection Limitation principle, which is the idea that data controllers should only collect that

information about an individual as is necessary for a certain specified purpose. *Second*, even this collection of information should be regulated by principles of consent and choice, whereby data subjects have the chance to agree or disagree with the terms of service, and leave if required.

Schedule 2 of the UK Data Protection Act incorporates the Privacy Principles of Collection Limitation and Consent, which limit the collection of personal information and require the consent of the data subject. The EU further incorporates data minimisation principles through Article 4.1(b) and (c) of Regulation 45/2001/EC of the European Parliament and Council and Articles 25 and 47 of the European Commission, (2016) Regulation (EU) 2016/679. This limits the collection of information to only what is relevant and necessary to accomplish a specified legitimate purpose. In India, the proposed privacy law should similarly incorporate such principles of collection.

Similarly, the opt-in/opt-out provisions relating to consent are also helpful in determining the scope of the principles governing the collection of personal data. Such a provision should be added in the proposed Indian privacy law. It should also explicitly provide users with the right to withdraw consent, after which their data should be deleted from the system.

Guidance can be taken from the EU to introduce the idea of proportionality and narrow tailoring of exceptions while balancing rights, and data minimisation principles. These are premised on the idea that personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected, so as to limit the scope of any potential misuse (European Commission, 1996).

While notice and consent are the bedrock of all privacy laws, they do not take into account the prevailing market failures of asymmetric information, imperfect competition and cognitive biases discussed above. Thus, users with cognitive biases in understanding complex privacy notices are faced with an all-or-nothing choice to stay or leave the platform. As the PCAST Report notes, "Only in some fantasy world do users actually *read* these notices and understand their implications before clicking to indicate their consent." (White House, 2014).

Nor do they consider consent in the context of changed privacy policies, as in the case of Snapchat, which in 2015 updated its terms of service to clarify that it had the right to "store, use, display, reproduce, modify, adapt, edit, publish, and distribute" content provided by its users (French, 2015; Snapchat, 2016). Consequently, our privacy law should focus on context and use frameworks, discussed below, that makes privacy policies easier to read and accessible, and should deal with cases of changed privacy policies.

7.5.2. Retention of data

With respect to the retention of data, different countries and companies adopt different time limits. However, the EU's 2015 Data Protection Reform has now added the "right to be forgotten", which permits the deletion of data relating to an individual under specific circumstances such as when the individual no longer wants her data to be processed and there are no legitimate grounds for retaining it (European Commission, 2015b).

In India too, the proposed privacy law should provide a time limit for retention or should require data controllers to specify the same. The law should also specify the manner and format of preserving data. Specific provisions should deal with requests from law enforcement agencies, especially in the context of the recent Apple vs FBI debate, which has lessons for India where internet companies based abroad have to deal with Indian data protection and interception standards, which are lower than the US (Sukumar, 2016).

Currently, under the Indian IT Act, data controllers are not obliged to retain data for any period of time and many privacy policies only seek to comply with US law (of the parent entities). For instance, Twitter, (2016b)'s policy is to preserve data, such as account records, for 90 days for use as potentially relevant evidence in legal proceedings.

7.6. Use and processing of data

With the rise in big data, data is collected both actively (e.g. when we provide it to use an app) and passively (e.g. our GPS tracking our location on Google Maps even without the internet), and can be stored easily and cheaply. In fact, big data also facilitates the tracking and storing of keystrokes. Thus, it was recently revealed that even half-typed posts/comments/status updates are stored as metadata by Facebook, even if it was deleted before pressing "Enter" (Golbeck, 2013). This has made it almost impossible in practical terms to regulate access control and limit the collection and retention of personal data (Kagal and Abelson, 2010; Jerome, 2013).

As a consequence, there is a shift in the focus of the Privacy Principles from *Collection* to *Purpose/Use* Limitation (Mundie, 2014) and support for the "Context and Use Framework" to apply to the *data and with the code that operates on the data* (White House, 2014).

The EU (Danezis et al., 2014; European Commission, 2015b) and Canada (Cavoukian and Jonas, 2012) are attempting to tackle this problem by emphasising "data protection by design" and "data protection by default", which rely on in-built data protection safeguards as companies' default privacy settings, instead of trying to achieve the same through compliance with regulatory frameworks. There have also been calls in India to incorporate privacy principles into the design of data systems, especially due to the perception that Indians may have fewer privacy considerations than their Western counterparts (Wright et al., 2011).

Along with incentivising such design-oriented solutions, the proposed Indian privacy law should incorporate the Privacy Principle of *Purpose Limitation* in favour of its prior focus on the *Collection Limitation* principle. This will help transfer some control with the data subjects, especially when they indicate their desire to delete their account or personal information.

Although different rules may apply to private entities and the government intelligence apparatus, we do not endorse the draft 2014 Privacy Bill and the Aadhaar Act's seemingly complete exemption of the government agencies when they act in the interest of sovereignty, integrity, security or the strategic, scientific oreconomic interest of India (Hickok, 2014). Such a blanket exemption undermines the right to privacy and precludes a judicial determination of balancing privacy with security concerns based on the facts of the case, which is especially dangerous given the government's extensive surveillance abilities.

7.7. Sharing and transferring of data

Along with regulating the collection, use, and retention of users' data, a national privacy law should also regulate how such data is shared with third parties, including those that are across national borders.

European data protection measures function on the premise that every instance of data transfer to other agencies violates fundamental rights, and thus requires special justification. Article 45 of Regulation (EU) 2016/679 permits cross-border transfer of personal data only if the other country or international organisation *ensures an adequate level of [its] protection* (European Commission, 2016). Conversely, there seems to be largely unrestricted data sharing between law enforcement and intelligence agencies in the US (Boehm, 2015). It was in this background that the "Safe Harbour Agreement" between the EU and US where US companies had to voluntarily undertake to protect EU citizens' personal data when transferred to the US was declared illegal by the European Court of Justice in October 2015 (*Maximillian Schemes versus Data Protection Commissioner, 2015*)[10].

Indian privacy law should follow a similar rule of only permitting transfer of personal or sensitive personal data if the other body corporate or person adheres to the same level of data protection, and if the transfer is necessary or the user has consented to it. This will assure data subjects of the privacy of their personal data, regardless of whether the data controller holds it in India or transfers it to its servers across the world. The 2014 Privacy Bill seems to have a similar provision (H. Subramaniam and A. Subramaniam, 2016), which should be a part of the proposed national privacy law.

[10] The ECJ ruled that the Agreement was not valid, focusing on the fact that US public authorities were not subject to its terms and that US undertakings had to disregard the rules under the Safe Agreement on considerations of national security, law enforcement and public interest. The ECJ also relied on the fact that users had no administrative or judicial means of redress enabling access and correction.

7.8. Rights of data subjects?

The proposed privacy law should also separately cover the rights of the data subjects, who are other important stakeholders in the privacy debate. Rights of data subjects should largely adhere to the Privacy Principles, and apart from those discussed above, should include data quality and integrity (along with concomitant rights of access and correction); data protection (to prevent unauthorised collection or use); and notification principles (of requests for accessing data, or regarding data breach). We specifically focus on three rights that are absent in the Indian context but should be part of our national privacy law.

i. The first relates idea of "data portability", introduced in the 2015 EC Directive, to allow users to transmit their personal data across various service providers, as part of improving their access and control over their own data (European Commission, 2015b). This has the dual advantage of giving users flexibility and control while encouraging competition amongst service providers to introduce privacy-friendly policies.

ii. The second right relates to the "data breach notification", also introduced in the 2015 EC Directive. This gives data subjects the right to know when their data has been hacked through notification by the data controller to the user or the national supervisory authority. This allows data subjects to take immediate action to limit the damage and also seeks to prevent data controllers from covering up their mistakes.

iii. The third right relates to the "right of access to, and correction of, personal data", which is meant to empower data subjects by keeping them informed about where and how their personal data is being used. This is expressly provided in Section 7 of the UK Data Protection Act, which stipulates that after giving a request in writing, users' are entitled to be informed whether their personal data is being processed. If so, they are entitled to the data in question; the reason for the processing; the recipient of the information; the source of the data; and in cases where the processing is to evaluate the users' *performance at work, his creditworthiness, his reliability or his conduct* for taking a decision, the logic involved in such decision taking.

The access and correction right also enables the confirmation of the veracity of the contents of the data and subsequent correction. In fact, access and correction are especially important when we consider that apart from being processed by the particular data controller, the user's data is also being shared with third parties, and will thus enter multiple data systems. There are serious implications of incorrect data of, for e.g. financial records on creditworthiness and ability to secure a loan and the law needs to provide methods of access and correction.

7.9. Supervision and redress mechanisms

The enforcement and impact of a privacy law will depend on having proper safeguards to prevent unauthorised access/misuse/deletion etc. of data and a grievance mechanism to provide adequate remedies. This is part of the *Security* and *Accountability* Principles and should be incorporated into Indian privacy law.

In UK, supervision occurs through the Information Commissioner's Office under Section 17 of the Data Protection Act, which ensures that no personal data is processed without an entry in a register. In America, the Federal Trade Commission regulates industries within its jurisdiction, along with other sector-specific regulators such as the U.S. Department of Health and Human Services, (2016), which examines complaints filed under HIPAA.

In the EU, under the 2015 reforms a single supervisory authority will replace national level Data Protection Commissioners (who monitor the application of EC Directives in their jurisdiction) to facilitate the ease of business across countries. Data protection authorities will be empowered to fine companies for failure to comply with EU rules (European Commission, 2015).

India currently lacks any such strong regulator, privacy or data Commissioner or Ombudsman. Aggrieved users only have the option of approaching the consumer courts (which are usually time consuming and expensive) or proceeding under sector-specific laws such as the IT Act (which have a limited scope and weak enforceability as discussed in the next section).

A strong supervision and enforcement system is necessary to make the guarantees of the national privacy law a reality and to ensure compliance. The 2014 Bill seems to focus on self-regulation and appointment of industry ombudsmen (Hickok, 2014). We believe that such a law needs to be supplemented with a distinct redress mechanism system. The focus should be on strengthening civil remedies in the form of compensation to the data subjects for loss and fines imposed on the data controller for contravention of the law.

At the same time, the role of such Ombudsmen or Information Commissioners should not be monopolised by retired civil servants or judges. There should be cross-sector representation from civil society, academics, industry representatives and experts. The law should also be more narrowly tailored in its exceptions and should remove the complete exemption of government intelligence agencies, since that might only encourage mass surveillance in the ostensible name of security.

Having outlined the privacy principles and the design elements of the proposed law above, it is useful to evaluate the privacy protections in an existing Indian law against such a framework. This will help understand how theoretical principles are translated on the ground in practice.

8. Evaluating the Indian IT Act

Currently, the most comprehensive law in India around privacy and data protection are the provisions of the IT Act and the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules 2011 (IT Rules, 2011). The Act applies to the State, to private corporate entities, and to individuals. In this section, we evaluate the IT Act provisions against the design elements sketched out in the section above. Such an evaluation will help us think about the amendments for the Aadhaar Act of 2016, which would strengthen privacy; understand the flaws in the IT Act and Rules which need to be fixed; and help us think about the future legislative journey of the Privacy Bill of 2014.

8.1 Objective of the law

While the IT Act does not exclusively deal with the right to privacy, the 2011 Rules lay out a framework to govern the collection, management, use, and sharing of personal data or sensitive personal data or information (SPDI). Currently, these are the most detailed provisions relating to personal data in India, although, as we will discuss in this chapter, there are many shortfalls.

8.2 Value of personal data

A well-designed privacy law should indicate the value it places on privacy and personal data. The 2011 Rules under the IT Act do not recognise that a right to privacy applies to every individual. They also do not articulate the value of the right itself. What this implies is that when there is a security-privacy conflict, as is inevitable, the government can easily disregard the privacy of individuals by citing public interest or security considerations.

One of the main reasons behind the recent Apple vs FBI standoff in the US is that the FBI's law enforcement arguments are being countered by referring to the importance of the right to privacy in American law and jurisprudence, and how accessing mobile phones is equivalent to accessing an individual's "innermost thoughts and private affairs" (Apple Press Info, 2016). In India, however, it is likely that in such a similar situation, law enforcement priorities would prevail.

8.3 Scope and ambit of the law

Good design principles require a privacy law to properly define personal data and SPDI, and treat them both separately.

Section 43A of the IT Act, introduced in 2009, deals with security practices and procedures relating to possessing, dealing or handling of any SPDI by body corporates. It thus only seems to apply to SPDI, and not personal information more generally. A conjoint

reading of the IT Act and the 2011 IT Rules, however, creates a slight ambiguity.

While Section 43A only mentions sensitive personal data, the Rules drafted there under define both "personal information" (Rule 2(1)(i)) and "sensitive personal data or information" (Rule 3) separately. However, the Rules seem to use these terms interchangeably thus, Rule 4 mandates body corporates to provide a privacy policy for both types of information, whereas Rules 5(1) and (4) on the collection of information and Rule 6 on disclosure only focus on sensitive personal data.

Moreover, clarifications issued by the Government of India in May and August 2011 through a Press Note stipulate that the intent of the Rules is to "protect sensitive personal information" (Press Information Bureau, 2011). Thus, the law does not clearly indicate whether, and if so, how, it treats personal and sensitive personal information separately.

The definition of SPDI is also fairly limited - while extending to passwords, financial and biometric information, medical records etc., it excludes email/home addresses, electronic communication records, political opinion, ethnicity/caste, religious beliefs, and user details (the last was included in a previous draft) (Department of Information Technology, 2011). Even the terms it includes, such as "biometric information" are left undefined. In fact, Rule 2(1)(b) defines "biometrics" in terms of technologies analysing human body characteristics, but is silent on what constitutes biometric information.

8.4 Coverage

A well-designed privacy law should extend to all residents of India and should be enforceable against the public and private sector. Section 43A (and the 2011 IT Rules) apply to "body corporates", requiring them to maintain reasonable security practices and procedures while possessing, dealing or handling any SPDI in a computer resource.

Section 43A defines "body corporate" in a manner that excludes any government agencies or non-profits. Such a blanket exemption is unwelcome, especially in the backdrop of the Aadhaar Act of 2016, whose privacy protections, as discussed below, are inadequate to ensure the accountability of the government, even though it is in charge of the largest personal data collection effort in human history. Governments and charities should also be covered under the ambit of the IT Act.

8.5 Collection and retention of personal data

The proposed privacy law should incorporate principles relating to consent and specify time limits and methods for retention and preservation of data.

Rules 4 and 5 of the 2011 IT Rules incorporate the *Choice* and *Consent* principles, allowing users to opt-in/opt-out and even withdraw consent. However, there is currently no statutory definition or guidance dealing with data minimisation and proportionality (when there

are conflicting rights). Further, since Rule 5 only governs the collection of SPDI, there is seemingly no requirement of consent for the collection of personal information, which is information capable of identifying any individual.

Retention of data is governed under Section 67C of the IT Act, which requires intermediaries (such as Facebook or Twitter) to preserve and retain certain information for certain duration and in a certain manner, as prescribed by the Central Government. Unfortunately, the government has failed to notify any Rules in this regard, and thus time limits for retention of data are currently completely voluntary in India.

Further, Rule 5(4) of the 2011 IT Rules only directs body corporates to not retain sensitive personal data for "longer than is required", and does not extend to the retention of "personal information". Thus, all data controllers are permitted to retain personal information regarding the data subjects for long after the specified purpose for which they were collected end. This undermines the importance of the right to privacy.

8.6 Use and processing of data

A well-designed privacy law should indicate a shift to context and use frameworks and incorporate the idea of privacy by design.

The 2011 IT Rules contain this principle of *Purpose Limitation* through Rule 5(5), which only permits using the information for the purpose for which it was collected. However, Rule 5(5) does not require a company to notify the data subjects if it changes its purpose, nor does it require destruction of data/personal information after the specified purpose is over. On the whole, the Act and the Rules seem to emphasise the importance of collection limitation more than use limitation.

8.7 Sharing and transferring of data

Another important design principle involves the regulation of sharing (disclosure) and transfer of personal and sensitive personal data to third parties and across borders. Like much else, Rule 6 of the 2011 Rules only governs the disclosure of SPDI and requires prior permission from the "provider of information". However, this is an undefined term, which can include either the original data subject, the intermediary, or a third party who is selling the SPDI further, thus introducing ambiguity in the law.

Rule 7 of the 2011 Rules allows transfer of SPDI within or outside India only if that body corporate or person adheres to the same level of data protection, if the transfer is necessary for the performance of a lawful contract or country or the user has consented to such transfer. This is consistent with international privacy principles and is welcome.

8.8 Rights of data subjects

The IT Act does not confer data subjects with the rights of data portability and data breach notification. However, Rule 5(6) of the IT Rules permits the (undefined) "providers of information" to review and correct any personal information or SPDI. This lack of definition becomes problematic when one considers that if the phrase is interpreted to include an intermediary or third party, the data subject will be unable to exercise this valuable right of access and correction.

8.9 Supervision and redress mechanisms

Security, *Openness* and *Accountability* principles require a privacy law to have proper supervision and redress mechanisms. India currently lacks any such strong regulator, privacy or data Commissioner or Ombudsman. Aggrieved users only have the option of approaching the consumer courts or proceeding under Section 43A of the IT Act (for negligent security practices causing wrongful loss or gain to a third party) before an Adjudicating Officer. This Officer, under Section 46 of the IT Act, can only hear disputes less than Rs. 5 crore. Rule 5(9) of the 2011 IT Rules also envisage the appointment of a Grievance Officer by body corporates.

However, in reality such an officer is an "invisible man" (Mohanty, 2012), considering that the Rules are silent about his minimum qualifications, duration, tenure, powers, and manner of reaching a decision, and no right of appeal is prescribed. Even the civil remedies prescribed under the IT Act are not easily enforceable. For instance, Section 48 provides for the establishment of multiple Cyber Appellate Tribunals, for appeals against the order of an Adjudicating Officer. Currently, only one Cyber Appellate Tribunal has been set up in Delhi and even that has been defunct since 2011, when the previous Chairperson retired (Soibam Singh, 2014). In fact, the last decided case seems to be of 30th June 2011, bringing to light the stark inefficiencies of the functioning of the IT Act (Tribunal, 2016).

Despite probably being the most comprehensive legislation currently in India regulating personal data and SPDI, the provisions of the IT Act and the IT Rules are seriously inadequate. The only other law, which has direct privacy implications, is the 2016 Aadhaar Act, even though it does not deal with concepts such as SPDI or context and use frameworks. However, in the absence of any development with respect to the 2014 draft Privacy Bill, it is instructive to evaluate the Aadhaar Act to understand where the law relating to privacy is heading.

9. Evaluating the Aadhaar Act

On 23rd March 2016, the Government of India enacted the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 [Aadhaar Act] touted as India's biggest welfare legislation. The Act, aimed at targeted delivery of subsidies, benefits and services by providing unique identity numbers based on an individual's demographic and biometric information, has been controversial. This section evaluates the Aadhaar Act using the same principles and components of privacy law as described above.

9.1 Objective of the law

By virtue of the large-scale and centralised collection, storage and use of an individual's demographic (e.g. name, date of birth, address) and biometric (e.g. iris scan, fingerprint, photograph etc.) information, the Aadhaar Act has great privacy implications. However, the Act does not consider privacy as one of its objectives. The word privacy does not even find mention in the Act. In fact, even the government's arguments in the Supreme Court during the challenge to Aadhaar, make it clear that it (and therefore, the Aadhaar Act) does not view privacy as a fundamental right (Moglen and Choudhary, 2015). Thus, while the text of this law is better than the UPA's 2010 draft, it is weak on privacy (Firstpost, 2016).

The objective of the law has to be understood in the context of whether the Act is voluntary or mandatory. Although, the government has repeatedly claimed that it is voluntary, this is belied by their practice in requiring Aadhaar numbers in nearly every area of life (Anand, 2016; Srivas, 2016; Yadav and Rao, 2016).

9.2 Value of personal data

While the Aadhaar Act, on first blush, seems to understand the value of the information it collects, it is not underpinned by an understanding of the right to privacy. As discussed before, laws are shaped by the value we place on personal data, and function on an underlying premise of privacy being valuable in and of itself. However, the Act lacks understanding or articulation of the importance of privacy of personal data. Privacy considerations in the Act appear to be a minor afterthought, especially when juxtaposed with the needs of 'national security' which is given prominence in the Act. The government has tried to remedy this by notifying various regulations pertaining to enrolment, authentication, and sharing of information in September 2016, although these only have the status of delegated legislation.

9.3 Scope and ambit of the law

The scope of the Aadhaar Act is a bit unclear since the working of key provisions have been left to regulations that have only recently been notified in September 2016.

For instance, Section 2(g) of the Act defines 'biometric information' to mean photograph, finger print, Iris scan, or such other biological attributes of an individual as may be specified by regulations. It is thus possible that DNA can be included under this definition, and become part of a centralised government database. The consequences of DNA-based profiling and its potential misuse are terrifying.

Another example of the lack of clarity is found in Section 23(2)(k), which permits the Unique Identification Authority of India ("UIDAI") to share information about individuals in such manner as may be specified by regulations.

Similarly, Section 29(2) permits the sharing of identity information, other than core biometric information, in such manner as may be specified by regulations. Even more worryingly, Section 29(4) permits the publication and display of an individual's core biometric information or Aadhaar number for purposes as may be specified by regulations.

Together, these examples undermine the idea of a watertight database that will be used exclusively by the government for the purposes of giving subsidies, benefits or services. Worse still, the regulations notified by the government continue to remain vague in part for instance, the phrase "as may be specified" by the UIDAI occurs 27 times over the four sets of regulations. Thus, the Aadhaar (Enrolment and Update) Regulations 2016 provide for the standard of demographic information (Regulation 4), the procedure for enrolling residents unable to provide biometric information (Regulation 6), the specification of biometric devices (Regulation 8), the collection of information at enrolment centres (Regulation 11), rectification action (Regulation 31) and the grievance redress mechanism (Regulation 32) to be specified in the future. Even the Code of Conduct for Service Providers requires them to follow confidentiality, privacy, and security protocols that will be specified by UIDAI.

While the government has drafted regulations with a view to improve the scope and coverage of the Act, it is unfortunate that significant changes have been sought to be made by bypassing parliamentary procedure and debate, that would have been necessitated by amendments to the law. Instead, the government has relied on executive notification, that can be changed anytime in the future without parliamentary involvement.

9.4 Coverage

The Aadhaar Act justifies the collection, storage, and use of personal data on the premise that it is a "condition for receipt of a subsidy, benefit or service", as stipulated under Section 7 of the Act. Thus, the Act is projected as covering (or regulating) only the interactions between the State and its residents.

However, a closer look reveals that under Section 57, the Act also facilitates interactions between private parties and residents of India by allowing body corporates to use the Aadhaar number for their own purpose. This raises concerns about violations of privacy when UIDAI shares data with private entities.

For instance, TrustID[11] is an app that allows the user to verify any individual using their Aadhaar number, and offers a range of services including pre-employment, credit background, tenants, business partners, employers, and property owners' verification. It is not clear that the information access by TrustID is taking place in ways that protect the privacy of individuals. As Ramanathan, (2016a) notes, many private companies have begun the process of trying to expand and leverage the uses of Aadhaar. The use of Aadhaar by a large number of private persons has long been touted as a contribution of the Aadhaar system to the Indian economy. There may be many conflicts about privacy in this process of expansion.

These applications suggest that the Aadhaar system will not be narrowly limited to the applications described in Section 7. The Act potentially covers everyone. It can include all the transactions conducted between an individual and the State in relation to benefits and subsidies; and the transactions between an individual and a corporate entity, where the private entity uses the Aadhaar number for identification and authentication.

The expanded scope of coverage, along with the absence of protection privacy, implies that this Act has reduced the overall privacy protections enjoyed by residents in India whether in their interactions with the State to access subsidies/benefits or in their interactions with corporate entities.

9.5 Collection and retention of personal data?

With regard to data collection and its retention, it is important to provide an opt-in/opt-out clause to users, as this is consistent with the Choice and Consent principle. This is particularly important in the Aadhaar Act, given our ownership over our own personal (demographic and biometric) data and the pervasiveness of our biometric data (e.g. we leave our fingerprints wherever we go).

The Aadhaar Act does not provide an opt-out clause, wherein Aadhaar number holders can choose to leave the system (and forego all its benefits) and ensure that their identity information is permanently removed from the Central Identities Data Repository.

In fact, Member of Parliament, Mr. Jairam Ramesh, proposed an amendment to Clause 3 of the Bill in the Rajya Sabha, allowing a person to opt out even if they had already enrolled, with the consequence that their authentication, biometric, and demographic information would be deleted from the system within 15 days. Although passed by the Rajya

[11] www.trustid.in

Sabha, the amendment was rejected by the Lok Sabha.

The absence of an opt-out clause is closely related to the issue of retention of personal information in as much as there are no time limits for the retention of data. This is unwelcome in light of the inherent non-revocability of biometric information and the fact that traces of our biometric data, for instance fingerprints, are left everywhere.

9.6 Use and processing of data

The principle of Purpose/Use Limitation is lacking in the Act. For instance, Section 33(2) carves out an express exception to Section 29(1)(b)'s stipulation of "using" core biometric information for any purpose other than generation of Aadhaar numbers and authentication under this Act if it is in the interest of [undefined] "national security".

Section 3(2) and Sections 8(2) (b) and 8(3) of the Act require the enrolling agencies to inform the individual about the manner in which their information shall be used and shared and ensure that their identity information is only used for submission to the Central Identities Data Repository.

At first blush, thus, the Act seems to incorporate principles of Purpose Limitation, especially since Section 41 imposes a penalty on the requesting entity for non-compliance. However, the lack of an effective enforcement mechanism, as discussed later, undermines these provisions. For instance, the Act does not detail how an Aadhaar number holder can escalate the issue (since only the UIDAI can file a complaint) or what standard will be used to determine whether the requesting entity has provided the information in a clear and suitable manner.

Further, the Aadhaar number holder's identity information can be used both by the State and body corporates, without any further regulation governing the use by third parties.

9.7 Sharing and transferring of data

This component of privacy design focuses on the Disclosure principle, namely the sharing of personal data with third parties. In the case of Aadhaar, this entails the identity information of the Aadhaar number holder. One of the most controversial sections of the Aadhaar Act is Section 33, which provides for the disclosure of information, including identity information or authentication records, under certain circumstances.

Section 33(2) makes an exception to the security, confidentiality and disclosure provisions on the direction of the Joint Secretary in the interest of national security. Such a direction has to be reviewed by a three member Oversight Committee, consisting of the Cabinet Secretary, the Secretary of the Department of Legal Affairs and the Secretary of the Department of Electronics and Information Technology. The second proviso further provides that such a direction shall be valid for three months, after which it can be reviewed and extended every three months. This is problematic for various reasons.

i. As Members of Parliament, Mr. Jairam Ramesh and Mr. Sitaram Yechury noted while moving an amendment to Section 33(2), "national security" is an undefined term, and thus, there is no transparency concerning covert surveillance. Consequently, the Rajya Sabha passed an amendment to replace the phrase "national security" with "public emergency or in the interest of public safety" (as is present in the Telegraph Act dealing with wiretapping). Unfortunately, this amendment was rejected by the Lok Sabha, and Section 33 remained as is.

ii. The scope of Section 33 is vague and it seemingly permits, and even facilitates, the furnishing of personal information to any third party, if it is in the interest of national security.

iii. The Oversight Committee is basically a committee of three Executive nominees. Thus, the possibility of effective oversight remains low.

9.8 Rights of users

The right to access and correct one's own information, the right to data breach notification, and the right to data portability are extremely important from the perspective of the user.

Unfortunately, the Aadhaar Act does not grant these rights to the Aadhaar number holder. With respect to the right of access, it is instructive to examine the proviso to Section 28(5) of the Act, which states that an Aadhaar number holder may "request" (not demand) the UIDAI to provide access to her identity information. Nevertheless, the proviso excludes requests for her core biometric information.

It is unclear what the powers of the UIDAI are to accept or deny such a request or why a carve out has been made to restrict access to one's own finger print/iris scan, especially considering they can be wrongly entered in the system, as has been documented in Rajasthan (where the biometric information of potential food ration beneficiaries did not match the data stored on the Aadhaar servers).

Correction or change of demographic information (e.g. on getting married) or biometric information is governed by Section 31 of the Act, which requires the Aadhaar number holder to "request" (not demand) the UIDAI to alter such information in their records. The section states that the UIDAI, on the receipt of such a request, "may, if it is satisfied" make such changes. It is unclear what the standard for such "satisfaction" is, and the Act does not prescribe any statutory penalty or means for judicial redress for the delay/failure to act. Given the centrality of the Aadhaar number in linking various databases and services, such truncated rights of access and correction are worrying.

The Aadhaar Act also fails to prescribe 'data breach notification' requirements, mandating the UIDAI to inform an individual, the Aadhaar number holder, that their identity (biometric and demographic) information has been shared or used without their knowledge or consent. Similarly, there is no concept of 'data portability' since information cannot freely be transferred amongst different service providers, since there are no alternatives to the UIDAI.

9.9 Supervision and redress mechanisms

Effective supervision and redress mechanisms require individuals to be informed when there is a breach of confidentiality or disclosure of their personal information.

Section 47 of the Act prescribes that only the UIDAI or its authorised officer can file a criminal complaint under the Act. Thus, all the criminal penalties prescribed under the Act (e.g. for disclosing identity information under Section 37 or for unauthorised access to the Central Identities Data Repository under Section 38) can only be initiated by the UIDAI, and not the aggrieved Aadhaar number holder.

Consequently, even though the Act prescribes civil and criminal remedies for unauthorised access, use, or disclosure by the prescribed authority, the criminal remedy is not available to the aggrieved Aadhaar number holder. Such a person only has recourse to civil law, and the fines prescribed under the Act.

Unfortunately, a conjoint reading of Sections 28 and 47 of the Act disclose the possibility of conflict of interest since it may be in UIDAI's interest to cover up breaches of privacy. Without the UIDAI's proactive action, an individual Aadhaar number holder is left without remedy.

Regulation 32 of the Aadhaar (Enrolment and Update) Regulations 2016 envisage a contact centre to serve as a grievance redress mechanism for the resolution of queries through calls and emails, although its procedures and processes, and even its binding nature, have been left unspecified. Given that the Regulations aim to bring about substantive changes in the working of the Act, such lack of enforceability is unfortunate. For instance, the Aadhaar (Sharing of Information) Regulations, 2016, states that if the identity information of the Aadhaar number holder is published or shared contrary to the Act or the regulations, the person has recourse to the grievance redress mechanism above.

Section 30 of the Act treats biometric information as "sensitive personal data or information", as understood in Section 43A of the Information Technology Act. The treatment of such information under the IT Act has been dealt with in detail in our previous post. The IT Act itself fails to handle sensitive personal data or information in ways that embed privacy concerns.

Finally, as discussed in the sections above, the supervision mechanism for one of the Aadhaar Act's most controversial sections (Section 33), is the constitution of an Oversight Committee. This Committee is tasked with reviewing the disclosures made in the interest of national security, and thus serves to fulfill the Accountability and Security principles of privacy law. However, this three member Committee comprises of three government bureaucrats, especially after the Lok Sabha rejected the Rajya Sabha amendment to include either the CVC or the CAG as part of the Committee.

10. Conclusion

Consider the new world of electronic communications. It is impossible for us to even know that our privacy is being infringed, or to know what information is being held about us. The Snowden revelations have proved that data collection, retention and analysis by the State is an immutable reality and that we have literally sleepwalked into a surveillance society. This has compelled governments in the US, UK and Europe, which have a far greater recognition of the right to privacy than India, to evaluate and revise their legal framework.

In India, in the absence of an over-arching law, our regulatory surveillance architecture is heavily weighted in favour of the State. This is extremely problematic as mass surveillance is being carried out in a legal vacuum, with little regard for the effect on individuals' rights to privacy. In such a situation, regardless of whether the Supreme Court of India considers privacy as a fundamental right, the State must define the circumstances in which it may intervene with an individual's rights. Similarly, law must define how private sector entities deal with user data.

In this paper, we make a case for India to enact a privacy law. Such a law would define key terms, govern the rights of users, detail the obligations of the State, lay down privacy principles and exceptions, provide guidance on resolving privacy security conflicts (for instance, by applying a European proportionality test) and would delineate various redress and compensation mechanisms.

India is a fledgling democracy. In the best of countries, there is an under-supply of criticism. In India, our ability to improve the working of the Republic requires more fearless people who will criticise the status quo. Privacy law should be a priority. Once greater privacy is secured, the processes of democracy in all other areas would work better.

References

Abraham, Sunil. (2015). Surveillance Project. *Frontline.* Accessed on 10 October 2016.

Acharya, Bhairav. (2015). The Four Parts of Privacy in India, *Economic and Political Weekly,* 50(22), 32–38.

Acquisti, Alessandro and Jens Grossklags (2007). What Can Behavioral Economics Teach Us About Privacy. In (eds.) Alessandro Acquisti and Sabrina De Capitani di Vimercati, *Digital Privacy: Theory, Technologies and Practices*, Auerbach Publications (Taylor and Francis Group). 363–377.

Alawadhi, Neha (2015). Ruling on Data Flow between EU and US may Impact India's IT sector. *The Economic Times.* Retrieved from: **https://goo.gl/xkvx0Y**.

Altman, Irwin. (1977). Privacy Regulation: Culturally Universal or Culturally Specific? *Journal of Social Science,* 33(3), 66–84.

Altman, Micah et al. (2016). Towards a Modern Approach to Privacy-Aware Government Data Releases. Research Publication 2016-9. Berkman Center.

Anand, Utkarsh (2016). Supreme Court reminds Govt.: Aadhaar cannot be Mandatory. *Indian Express.* Retrieved from: **https://goo.gl/BZy0Hx**.

APEC (2005). The APEC Privacy Framework. Tech. rep. *The Asia-Pacific Economic Cooperation.*

Apple Press Info (2016). Amicus Briefs in Support of Apple. Retrieved from: **https://goo.gl/omQLxL.** Accessed on 12 July 2016.

Artavia Murillo et al. (2012). ("In Vitro Fertilization") v Costa Rica (2012). Judgment of November 28. Preliminary Objections, Merits, Reparations and Costs, Inter American Court of Human Rights.

Barocas, Solon and Andrew Selbst (2016). Big Data's Disparate Impact. In Calif. L. Rev. 104, 671–732.

Bhargava, Yuthika (2015). India Tops Facebook's List of Content Restriction Requests. *The Hindu*. Retrieved from: **https://goo.gl/JIyzB8**.

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

Boehm, Dr. Franziska (2015). A Comparison between US and EU Data Protection Legislation for Law Enforcement: Study for the LIBE Committee. Tech. rep. Policy Department C, Citizens' Rights and Constitutional Affairs, Directorate General for Internal Policies, European Parliament.

Boillat, Philippe and Morten Kjaerum (2014). Handbook on European Data Protection Law. Tech. rep. European Union Agency for Fundamental Rights and Council of Europe.

Booth, Jenny (2004). UK 'Sleepwalking into Stasi State'. *The Guardian*. Accessed on 17 July 2016.

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

Cavoukian, Ann and Jeff Jonas (2012). *Privacy by Design in the Age of Big Data*. Tech. rep. Privacy by Design, Canada.

CFR (2000). Charter of Fundamental Rights of the European Union, 2000/C 364/01. Tech. rep. *Official Journal of the European Communities*, C 364/1, 18.12.2000.

Chernichaw, Adam and Brandon Freeman (2015). *White House Re-introduces Consumer Privacy Bill of Rights*. White and Case, Retrieved from: http://goo.gl/yVVGGY. Accessed on 19 July 2016.

CIPPIC (2007). *Identity Theft: Introduction and Background*. Tech. rep. Canadian Internet Policy and Public Interest Clinic (CIPPIC) Working Paper No. 1 (ID Theft Series), Ottawa.

CIS (2011). *Privacy in India - Country Report*. Tech. rep. Centre for Internet Society, Privacy India, Privacy International, Society in Action Group.

_____, (2013). *Privacy (Protection) Bill, 2013: Updated Third Draft*. Centre for Internet and Society. Retrieved from: https://goo.gl/gUhonR. Accessed on 12 October 2016.

Citron, Danielle Keats and Frank Pasquale (2014). The Scored Society: Due Process for Automated Predictions. In *Wash. L. Rev.* 89, 1–33.

Clarke, Richard et al. (2013). *Report and Recommendations of The President s Review Group on Intelligence and Communications Technologies*. Tech. rep. White House. White House.

Cohen, Julie (2012). What Privacy is For. In *Harv. L. Rev.* 126, pp. 1904–1933. Congress.gov (2015). *Data Security and Breach Notification Act of 2015*. S. 177 - 114th Congress (2015-2016), Retrieved from: https://goo.gl/hKUQyP. Accessed on 22 July 2016.

Cooley, Thomas (1871). A Treatise on the Constitutional Limitations Which Rest Upon the Legislative Power of the States of the American Union. Little, Brown and Co.

CRID, University of Namur (2006). First Analysis of the Personal Data protection Law in India. Tech. rep. Report delivered in the framework of contract JLS/C4/2005/15 between CRID, the EU Directorate General Justice, Freedom, and Security.

Danezis, George et al. (2014). Privacy and Data Protection by Design: From Policy to Engineering. Tech. rep. European Union Agency for Network and Information Security (ENISA).

Department of Information Technology (2011). Draft Rules - Reasonable Security Practices and Procedures and Sensitive Personal Information. Ministry of Communications and Information Technology, Government of India. Retrieved from: http://goo.gl/kiJPg1. Accessed on 12 July 2016.

Dreze, Jean (2016). The Aadhaar Coup. *The Hindu.* Retrieved from: https://goo.gl/gbLqY3. Accessed on 11 October 2016.

European Commission (2015a). Press Release: Agreement on Commission's EU data Protection Reform will Boost Digital Single Market. Retrieved from: http://goo.gl/KvbKRZ. Accessed 10 July 2016.

_____, (2015b). Fact Sheet, Questions and Answers - Data Protection Reform. Accessed on 10 July 2016.

_____, (1996). Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals With Regard to the Processing of Personal Data and on the Free Movement of Such Data. *Tech. rep. Official Journal* L(281/31); 23.11.1995.

_____, (2012). Proposal for a Directive of the European Parliament and of the Council on the Protection of Individuals with regard to the Processing of Personal Data by Competent Authorities for the Purposes of Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and the Free Movement of such Data. Tech. rep. Brussels, COM (2012) 10 final, 2012/0010 (COD).

_____, (2016). Regulation (EU) 2016/679 on the Protection of Natural Persons With Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation). *Tech. rep. Official Journal* L(119/1): 27.04.2016.

Firstpost (2016). UPA vs NDA: Check Out How Aadhaar Act 2016 Differs from the 2010 Bill. Retrieved from: http://goo.gl/qE2rcR. Accessed on 08 August 2016.

French, Sally (2015). Snapchat's New 'Scary Privacy Policy has Left Users Outraged. MarketWatch. Retrieved from: http://goo.gl/bLLA1a. Accessed 12 July 2016.

Gartner (2001). IT Glossary. Retrieved from: http://www.gartner.com/it-glossary/big-data/. Accessed on 28 December 2015.

Gobind v State of Madhya Pradesh (1975). SCR (3) 946.

Golbeck, Jennifer (2013). On Second Thought...: Facebook Wants to Know Why You Didn't

Publish that Status Update You Started. The Slate. Accessed on 10 July 2016.

Google (2015). Google Transparency Report: India. Retrieved from: http://tinyurl.com/zsgajqu. Accessed on 10 April 2016.

Google Spain SL, Google Inc. v Agencie Espanola de Protection de Datos (AEPD) (2014). Case No. C-131/12, European Court of Justice.

Government of Australia (2015). Australian Public Service Better Practice Guide for Big Data. Tech. rep. Data Analytics Centre of Excellence and the Big Data Working Group.

Green, Leon (1934). "Relational Interests". In: *Illinois* L.R. 29; 460–490.

Hafetz, Jonathan (2002). A Man's Home is His Castle?: Reflections on the Home, the Family, and Privacy During the Late Nineteenth and Early Twentieth Centuries. In: William and Mary J. of Women and L. 8.2; 175–242.

Halper, Jim, Jennider Kashatus, and Kate Lucente (2016). Data Protection Laws of the World: United States. Tech. rep. DLA Piper.

Hetcher, Steven (2001). Changing the Social Meaning of Privacy in Cyberspace. In *Harvard J. of L. and Tech.* 15.1, 149–209.

Hickok, Elonnai (2014). Leaked Privacy Bill: 2014 vs. 2011. The Centre for Internet and Society. Retrieved from: http://goo.gl/kPAGnS. Accessed on 12 July 2016.

Human Rights Council (2011). Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue. Tech. rep. United Nations General Assembly, A/HRC/17/27.

Introna, Lucal (1974). Privacy and the Computer: Why we need Privacy in the Information Society. In *Metaphilosophy.* 28.3, 259–275.

Jerome, Joseph (2013). Buying and Selling Privacy: Big Data's Different Burdens and Benefits. In Stan. L. Rev. Online. 66, 47–53.

Justice K.S. Puttaswamy (Retd.) v UOI and Ors (2015). W.P. (Civil) No. 494 of 2012, Supreme Court of India.

Justice Shah Report (2012). Report of the Group of Experts on Privacy. Tech. rep. Government of India, Planning Commission.

Kagal, Lalana and Hal Abelson (2010). Access Control is an Inadequate Framework for Privacy Protection". In W3C Privacy Workshop.

Karmanya Sareen v UOI and Ors (2016). W.P. (Civil) No. 7663 of 2016, High Court of Delhi.

Kharak Singh v State of Uttar Pradesh (1964). SCR 1 332.

Khedekar, Naina (2013). India second in Government Requests for User Data: Google

Transparency Report. First Post. Retrieved from: http://tinyurl.com/hfw4ncc.

Kosinski, Michal, David Stillwell, and Thore Graepel (2013). Private Traits and Attributes are Predictable from Digital Records of Human Behavior. In Proc. of the Nat. Acad. of Sciences 110.15; 5802–5806.

Laksh Vir Yadav v UOI and Ors (2016). W.P. (Civil) No. 1021 of 2016, High Court of Delhi.

Moglen, Eben and Mishi Choudhary (2015). Aadhaar and the Right to Privacy. *The Hindu.* Retrieved from: http://goo.gl/9nb420. Accessed on 08 August 2016.

Mohanty, Amlan (2012). Grievance Officer in the IT Rules - An Invisible Man? Spicy IP, Retrieved from: http://goo.gl/NaarbQ. Accessed on 11 July, 2016.

Montjoye, Yves-Alexandre de et al. (2015). Unique in the Shopping Mall: On the Reidentifiability of Credit Card Metadata. In *Science* 347.6221; 536–539.

Moore, Adam (2008). Defining Privacy. In *J. of Soc. Phil.* 39.3; 411–428.

M.P. Sharma v Satish Chandra (1954). SCR 1077.

Mundie, Craig (2014). Privacy Pragmatism: Focus on Data Use, Not Data Collection. Foreign Affairs. Retrieved from: https://goo.gl/X1zv2Z. Accessed on 10 March 2016.

Narayanan, Arvind and Vitaly Shmatikov (2008). Robust De-anonymization of Large Sparse Datasets. In Proceedings of the 2008 IEEE Symposium on Security and Privacy; 111–125.

Nasscom (2013). NASSCOM Update on EU Data Protection Regime.

Newman, Nathan (2014). Search, Antitrust and the Economics of the Control of User Data. In Yale J. of Reg. 31(2); 401–454.

Routray, Bibhu (2012). Making a Case for Futuristic Predictive Policing in India. New Indian Express. Retrieved from: http://goo.gl/cYjasQ. Accessed on 10 July 2016.

OECD (2013). The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Tech. rep. The Organisation for Economic Cooperation and Development.

Ohm, Paul (2010). Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. In UCLA L. Rev. 57; 1701–1777.

Parent, William (1983). Privacy, Morality and the Law. In Phil. and Pub. Affairs 12.4; 269–288.

Parker, Richard (1974). A Definition of Privacy. In Rutgers L.R. 27; 275– 296.

Patel, Nipun and Susan Conners (2008). Outsourcing: Data Security and Privacy Issues in India. In *Issues in Info. Sys. J.* 9.2; 14–20.

Perry, Walter et al. (2013). Predictive Policing: The Role of Crime Forecasting in Law

Enforcement Operations. Tech. rep. RAND Corporation.

Podesta, John et al. (2014). Big Data: Seizing Opportunities, Preserving Values Tech. rep. Executive Office of the President, White House.

Press Information Bureau (2011). Clarification on Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 under Section 43A of the Information Technology Act, 2000. Ministry of Communications and Information Technology, Government of India, Retrieved from: http://goo.gl/4lf8qq. Accessed on 12 July 2016.

_____, (2015). Status of NATGRID. Ministry of Home Affairs, Government of India. Retrieved from: http://goo.gl/lTg2O8. Accessed on 12 July 2016.

PTI (2014), Government to Launch Internet Spy System 'Netra' Soon. Times of India, Retrieved from: http://goo.gl/ti6rsM. Accessed on 12 July 2016.

PUCL v Union of India (1997). 1 SCC 301.

Rachels, James (1975). Why Privacy is Important. In *Phil. and Public Affairs* 4.4, 323–333.

Ramanathan, Usha (2016a). The Future is Here: A Private Company Claims it can Use Aadhaar to Profile People. Scroll Retrieved from: http://goo.gl/Fru5Z1. Accessed 11 July 2016.

_____, (2016b). The Law Needs to Catch Up With Aadhaar, But Not in the Way Jaitley is Promising. *The Wire*. Retrieved from: http://goo.gl/3E8CLC. Accessed on 17 July 2016.

Rockelmann, Andreas, Joshua Budd, and Michael Vorisek (2011). Data Breach Notifications in the EU. Tech. rep. European Union Agency for Network and Information Security (ENISA).

Rossler, Beate (2005). The Value of Privacy. Polity Press.

Sacharoff, Laurent (2012). The Relational Nature of Privacy. In: Lewis and Clark L. Rev. 16.4; 1249–1303.

Scanlon, Thomas (1975). Thomson on Privacy. In *Phil. and Pub. Affairs* 4.4; 315–322.

Scott, Mark (2015). Europe Approves Tough New Data Protection Rules. New York Times, Retrieved from: http://goo.gl/3E5u5r. Accessed on 18 July 2016.

SFLC (2014). India's Surveillance State: Communications Surveillance in India. Tech. rep. SLFC.in, Software Freedom Law Centre.

Shekhar, Raj (2015). Police Plan Tech to Predict Crime. Times of India. Accessed on 12 July 2016.

Shontell, Alyson (2013). Actually, Snapchat Doesn't Delete Your Private Pictures And

Someone Found A Way To Resurface Them. Business Insider. Accessed on 11 July 2016.

Singh, Soibam (2014). India's Only Cyber Appellate Tribunal Defunct Since 2011. Hindustan Times. Accessed on 11 July 2016.

Singh, Sumit (2015). Delhi Police Launches into Space. New Indian Express. Accessed on 10 July 2016.

Snapchat (2016). Terms of Service. Retrieved from: https://www.snapchat.com/terms. Accessed on 12 July 2016.

Solove, Daniel (2008). Understanding Privacy. Harvard University Press.

Srivas, Anuj (2016). Aadhaar Moves Forward As Ministries Navigate SC Order and Public Backlash. *The Wire*, Retrieved from: https://goo.gl/ZFxW1X.

Subramaniam, Hari and Aditi Subramaniam (2016). India: Data Protection 2016. International Comparative Legal Guide, Retrieved from: http://goo.gl/vYd7uJ. Accessed on 10 July 2016.

Sukumar, Arun Mohan (2016). What Apple versus FBI Means for India. The Hindu, Retrieved from: http://goo.gl/Lv14Ih. Accessed on 11 July 2016.

Sweeney, Latanya (2000). Simple Demographics Often Identify People Uniquely. In Data Privacy Working Paper 3. Carnegie Mellon University, 1–34.

Tene, Omer and Jules Polonetsky (2012). Privacy in the Age of Big Data: A Time for Big Decisions. In Stan. L. Rev. Online 64; 63–69.

_____, (2013). Big Data for All: Privacy and User Control in the Age of Analytics. In:*Northwestern J. of Tech. and Intell. Prop.* 11.5; 239–273.

TFEU (2012). Consolidated Version of the Treaty on the Functioning of the European Union. Tech. rep. *Official Journal* C(326), 26.10.2012.

Times, Economic (2011). India Ranks Third in Snooping through Google. Tribunal, Cyber Appellate (2016). Judgment. Government of India. Accessed on 12 July 2016.

Turow, Joseph et al. (2007). The Federal Trade Commission and Consumer Privacy in the Coming Decade. In *J. of L. and Policy for the Information Soc.* 3.3, 723–749.

Twitter (2016a). Privacy Policy. https://twitter.com/privacy?lang=en. Accessed on 17 July 2016.

_____, (2016b). Guidelines for Law Enforcement. Accessed on 10 July 2016.

U.S. Department of Health and Human Services (2016). Health Information Privacy: Filing a Complaint. HIPAA, Retrieved from: http://goo.gl/yzaw5M. Accessed on 12 July 2016.

Volker and Markus Schecke GbR and Hartmut Eifert v Land Hessen (2010). Joined Case, Case No. C-92/09 and C-93/09, European Court of Justice.

Von Hannover v Germany (No. 2) (2012). 55 EHRR 15, European Court of Human Rights.

Warren, Samuel and Louis Brandeis (1890). "The Right to Privacy". In: Harv. L. Rev. 4; 193–220.

Westin, A. (1967). Privacy and Freedom. Atheneum Publishers.

White House (2014). Big Data and Privacy: A Technological Perspective. Tech. rep. President's Council of Advisors on Science and Technology (PCAST), Executive Office of the President, White House.

_____, (2015). Administrative Discussion Draft: Consumer Privacy Bill of Rights Act of 2015. Tech. rep. The Office of the President of the United States of America. Wright, Glover et al. (2011). Report on Open Government Data in India. Tech. rep. Centre for Internet and Society, Bangalore.

Walker, Joseph (2013). Data Mining to Recruit Sick People. *Wall Street Journal,* Retrieved from: http://goo.gl/s0JvBD. Accessed on 10 July 2016.

Yadav, Anumeha and Menaka Rao (2016). Despite Glitches, Government Plans to Introduce Aadhaar authentication at Health Centers. Scroll.in, Retrieved from: https://goo.gl/o1i5Rv.

Appendix

1. European Union

The EU has one of the most progressive privacy protection norms in place, starting with the value it places on privacy and personal data by treating privacy as a fundamental right.

Article 1(1) of the European Commission, (1996) Data Protection Directive, 95/46/EC, directs Member States to *"*protect the fundamental rights and freedoms of natu*ral* persons, and in particular their right to privacy, with *respect* to the *processing* of personal data.*"* This Directive has recently been repealed by European Commission, (2016) Regulation (EU) 2016/679, which came into force in May 2016, and "protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.*"*

*A*rticle 7 of the Charter of Fundamental Rights of the European Union (CFR), 2000/C/364/01, guarantees the right to respect for private and family life, just as Article 8 of the ECHR. Additionally, Article 8 of the CFR guarantees protection of personal data for everyone (CFR, 2000). This is further guaranteed by Article 16 of the Treaty on the Functioning of the European Union (TFEU), which recognises the right of everyone to the protection of personal data concerning them (TFEU, 2012).

These rights are, however, not absolute and the restrictions on the right to privacy and personal data are subject to principles of proportionality (Boillat and Kjaerum, 2014). This has also been recognised by the European Court of Justice in many cases such as *Volker and Markus Schecke GbR and Hartmut Eifert v Land Hessen, (2010)* and by the European Court of Human Rights in *Von Hannover v Germany (No. 2), (2012)*.

Apart from giving pre-eminence to the right to privacy and personal data, the various EU directives also guarantee substantive privacy protections, consistent with internationally accepted principles. Article 8 of the CFR further recognises the principles of Purpose Limitation, Consent and Choice and Access and Correction, which will be discussed in detail later.

Article 12 of the EC Data Protection Directive of 1996 grants the right of access and rectification, erasure, and blocking of one's own personal data. Interestingly, Article 14 of the Directive provides data subjects with the "right to object" in certain situations to the processing of personal data related to them. It also grants them the right to be informed about the disclosure of their personal data for the first time to third parties.

The other principles of data protection found in the 1996 Directive includes the principles relating to "data quality", which comprises of data relevancy (a form of Collection and Purpose Limitation and data minimisation) and "data accuracy".

Finally, Article 28 of the 1996 Directive further requires each Member State to appoint a public authority responsible for monitoring the application of the Directive to enable in proper supervision of the application of the privacy principles.

The data protection regime in Europe has only been strengthened after the General Data Protection Regulation and the Data Protection Directive of 2015 were adopted by the European Parliament and Council (European Commission, 2015a; European Commission, 2015b) through Regulation (EU) 2016/679 and Directive (EU) 2016/680 respectively. Apart from repealing Directive 95/46/EC, Regulation (EU) 2016/679 of the European Commission, (2016) made four broad changes through the addition of new rights and the strengthening of existing rights. These changes, now part of the privacy-regulatory framework in the EU are enumerated below:

1. A right to "data portability", which is connected to the idea of easier access and control of one's own data and is included in Article 20 of Regulation (EU) 2016/679. The right makes it easier for data subjects to transfer personal data between different service providers in an interoperable format, and gives them greater control over how their data is processed and made available. By empowering data subjects and giving them greater control over their personal data, this reform is aimed at reducing problems of monopolies by enabling startups/small firms to attract customers by offering more privacy-friendly solutions.

2. The right to erasure or the right to be forgotten has been included in Article 17 of Regulation (EU) 2016/679, in line with the decision of the European Court of Justice in 2014 in *Google Spain SL, Google Inc. v Agencie Espanola de Proteccion de Datos (AEPD), (2014)* on the point. This right requires the data controller to delete the personal data of an individual or data subject when she no longer wants her data to be processed, the data is no longer necessary for the purpose for which it was collected or processed, and there are no overriding legitimate grounds for retaining it. Article 17(3), however, delineates certain considerations, such as the exercise of free speech or public interest in public health, that limit the exercise of the right to erasure.

3. The right to know when one's data has been compromised, through "data breach notifications" has now been included in Article 33 of Regulation (EU) 2016/679, after being part of the 2015 Directive. The said Article firmly places the burden on the controller to notify the supervisory authority of any personal data breaches as soon as possible, and within 72 hours. Such a notification has to include a description of the likely consequences of the breach and steps taken by the controller in controlling or mitigating the effects of such breach. Article 34 then requires the controller to communicate the personal data breach to the data subject "without undue delay" if such breach is likely to result in a high risk to the rights and freedoms of natural persons. Data breach notifications thus are meant to control the consequences of a data breach, while

informing the data subjects of the breach.

4. Stronger enforcement and supervision have taken priority in the new reforms and find place in Article 83 of the Regulation (EU) 2016/679. Enforcement is sought to be achieved through improved coordination amongst law enforcement authorities across Europe and by imposing fines of up to 4% of worldwide annual turnover on those companies that fail to comply with certain specified EU rules. In view of this provision and the reporting requirement of a data breach notification within 72 hours, some commentators believe that the combined deterrent effects moved far away from the American standard (Scott, 2015).

These rights are accompanied by proposals to boost the Digital Single Market such as "one continent, one law" to facilitate the replacement of a patchy network of inconsistent national laws with a single pan-European law and rules for innovation such as "data protection by design" and "data protection by default" (European Commission, 2015b). These rules envisage that data protection safeguards and improved privacy settings will be inbuilt into various products and services offered online and privacy-friendly techniques such as pseudonomysation will be encouraged, to protect users even if they have not given informed consent.

2. United Kingdom

Pursuant to the passage of the European Commission, (1996) Data Protection Directive, 95/46/EC, the United Kingdom passed the Data Protection Act of 1998 to regulate the *"*processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information*."*

This Act thus governs a large part of the data protection and privacy framework in the United Kingdom. Schedule 1 of the Act define and elaborate on eight "Data Protection Principles", which focus on the lawful and fair processing of data, collection and use limitation, the relevancy, accuracy and regular updating of data, and principles governing transfer of personal data to a country outside the European Economic Area. Schedule 2 expands on some of these principles and require data subjects to give their "consent" to the processing of their personal data, which has to take place in accordance with certain specified stipulations. The Act defines "personal data" and "sensitive personal data" separately, and the Third Schedule lays down the conditions relevant for the processing of sensitive personal data, such as requiring "explicit consent" from the data subject. The Act also lays down the rights of data subjects and the importance of notification by data controllers in detail.

The Information Commissioner's Office is tasked with supervising the implementation of the Act and ensuring that no personal data is processed without an entry in the Register.

3. United States of America

Unlike the EU or the UK, the United States does not have a single comprehensive law dealing with all aspects of privacy and data protection. Instead, it has a combination of federal laws such as the Privacy Act of 1974, the Electronic Communications Privacy Act and sector-specific regulations such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Financial Modernization Act of 1999 (enforced by eight Federal Agencies including the FTC) and the Children's Online Privacy Protection Act (COPPA). Further, as Boehm, (2015) points out, unlike the EU, standards such as effective access, rules limiting exchange with third parties, proportionality considerations, data breach notifications, or independent oversight do not play a role while considering restrictions on data protection in the US.

Of interest, however, is the recent Consumer Privacy Bill of Rights Act of 2015 (CPBR) unveiled by President Obama as an Administrative Discussion Draft on 27th February 2015. This draft bill is intended to "establish baseline protections for individual privacy in the commercial arena" and to foster their timely implementation through "enforceable codes of conduct developed by diverse stakeholders" (White House, 2015). Its focus therefore, is clearly on commercial, and not public, use of personal data. The Report of the President's Council of Advisors on Science and Technology (PCAST) categorised the principles of the (CPBR) into two categories for ease of reference the principles underlying consumer empowerment and the principles underlying the obligations of data holders or commercial users (White House, 2014).

The first category of consumer empowerment focuses on the rights and responsibilities of the data subjects and the application of privacy principles to them. It includes three principles, namely 'Individual Control' (Section 102, CPBR); 'Transparency' (Section 101, CPBR); and 'Access and Accuracy' (Section 106, CPBR).

Under the obligations of data holders and commercial users and analysers, the focus shifts away from the data subject to the data holder. It is meant to function regardless of the user's understanding of the privacy policy or the 'informed' nature of their consent. Under this category, the PCAST Report grouped four principles of the CPBR Draft, namely 'Respect for Context' (Section 103, CPBR); 'Focused Collection and Responsible Use' (Section 104, CPBR); 'Security' (Section 105, CPBR); and 'Accountability' (Section 107, CPBR).

While the PCAST Report endorses these underlying principles of the CPBR, its primary criticism of the CPBR Draft was that it did not account for the complexities of big data and thats instead of focusing on consent and collection limitation, the CPBR should have regulated data use better (White House, 2014). The CPBR Draft of 2015 has also been criticised for its weak enforcement provisions (Chernichaw and Freeman, 2015). Of specific interest is Section 203 dealing with Civil Penalties, which stipulates that these penalties are to be computed by *multiplying the number of days that the covered entity violates the Act by an*

amount not to exceed $35,000. Such a provision is aimed at deterring violations spread out over time but does little to deter large scale violations carried out by data holders in a single day (since the penalty is capped at $35,000).

It is also worthwhile to note that in January 2015, the Data Security and Breach Notification Act of 2015 was introduced in the US Senate in an attempt to reduce instances of identity theft. The Act is aimed at protecting consumers by *"*requiring reasonable security policies and procedures to protect data containing personal information, and to provide for nationwide notice in the event of a breach of security.*"* It has currently been referred to the Committee on Commerce, Science and Transportation (Congress.gov, 2015).

MORE IN THE SERIES

- Pandey, R. Patnaik. I., (2016). "Legislative Strategy for Setting Up an Independent Debt Management Agency" WP. No. 178 (October)
- Kumawat, L., Bhanumurthy, N. R., (2016). "Regime Shifts in India's Monetary Policy Reforms Function" WP. No. 177 (September)
- Sharma, R. S. (2016). "UIDAI's Public Policy Innovations" WP. No. 176 (September)

Vrinda Bhandari, is Practicing Advocate, Delhi

Email: vrinda.bhandari@gmail.com

Renuka Sane, is Visiting Faculty, Indian Statistical Institute, Delhi

Email: renuka@saner.org.in

National Institute of Public Finance and Policy,
18/2, Satsang Vihar Marg,
Special Institutional Area (Near JNU),
New Delhi 110067
Tel. No. 26569303, 26569780, 26569784
Fax: 91-11-26852548
www.nipfp.org.in