PRIVACY IN INDIA IN THE AGE OF BIG DATA

Buddhadeb Halder

Privacy in India in the age of big data

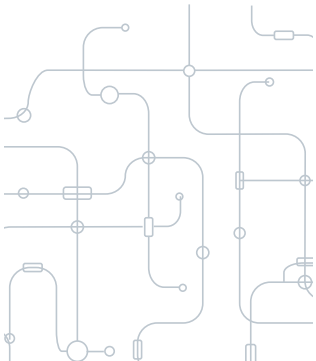
Written by Buddhadeb Halder
Edited by Ritu Srivastava, Rajen Varada & Gulshan Banas
Reviewed by Osama Manzar and Rajen Varada
Cover designed by Bhawana Mahariya
Design & layout by Shaifali Chikermane and Bhawana Mahariya

Published & distributed by Digital Empowerment Foundation

You can read the online copy at www.defindia.org/publication-2

Contact
Digital Empowerment Foundation
House No. 44, 2nd & 3rd Floor (Next to Naraina IIT Academy)
Kalu Sarai, (Near IIT Flyover), New Delhi – 110016
Tel: 91-11-422-33-100 / Fax: 91-11-26532787
Email: def@defindia.net | URL: www.defindia.org

CONTENTS



1

Introduction

Privacy is a human right recognised by the United Nations (UN). It is difficult to define succinctly and precisely what this right entails. Privacy has a dual aspect—it is concerned with information or personal data and the extent to which that is shared with other parties. The understanding of privacy has been shaped by technologies available at the time, starting from literacy, to book keeping to newspapers, and the current times we live in, the Internet. The Internet and the advent of mass data collection and retention have reshaped the concept of privacy in the modern world. The current discourse around privacy revolves around the ways in which third parties deal with the information they hold—whether it is secured, safeguarded, who has access, and under what conditions.

The 'right to privacy' is a fundamental human right recognized in the Universal Declaration of Human Rights (UDHR), the International Covenant on Civil and Political Rights (ICCPR), the UN Convention on

Migrant Workers[1] and the UN Convention on Protection of the Child[2] and in many other international and regional treaties. Numerous international human rights covenants, conventions, and human rights courts[3] give specific reference to privacy as a right.

The UN Special Rapporteur made reference to the right to privacy in his first report on 8th March 2016. Two principles underpin his report – 1. Privacy safeguards must be available regardless of national borders; and 2. Remedies for violations of privacy likewise must be available across these borders[4]. In order to facilitate the Principles, the Special Rapporteur has also outlined a Ten Point Action plan[5].

The right to privacy underpins other rights and freedoms like the freedom of expression, association, and belief. However, in the age of big data, the right to privacy has become a pivotal issue as personal data is routinely collected and traded in the new economy. Data researchers and analysts are now trying to reclaim privacy concerns and ensure that any data collected remains secure.

Edward Snowden[6] expose of the National Security Agency and the Five Eyes Intelligence Alliance's global surveillance program[7] along with the cooperation of telecommunication companies and European

1. *See A/RES/45/158 25 February 1991, Article 14.*
2. *See UNGA Doc A/RES/44/25 (12 December 1989) with Annex, Article 16.*
3. *For example, the 1950 Convention for the Protection of Human Rights and Fundamental Freedoms, the European Convention on Human Rights, the American Convention on Human Rights, and the American Declaration of the Rights and Duties of Man. Several Courts of Human Rights have also begun to address privacy issues in their hearings.*
4. *Report of the United Nations Special Rapporteur on the right to privacy, (A/HRC/31/64). 8th March 2016.*
5. *Ten Point Action Plan will be discussed later in the sub-section 1.1. under 'Privacy Safeguards at the International Level'.*
6. *An American computer professional, former Central Intelligence Agency (CIA) employee, and former contractor for the United States government who copied and leaked classified information from the National Security Agency (NSA) in 2013.*
7. *The US, the United Kingdom (UK), Australia, Canada, and New Zealand are the Five Eyes Intelligence Alliance. See: Nyst, C and Crowe, A. Unmasking the Five Eyes' global surveillance practices. Association for Progressive Communications (APc) & Humanist Institute for cooperation with developing countries (Hivos). APC-201408-CIPP-R-EN-DIGITAL-207.*

governments, revealed the extent of risks that big data brings to consumers and citizens the world over.

Using big data analytics, the 'communications surveillance' by state and non-state actors including private entities is becoming inescapable and highly aggressive. In the present age 'communications surveillance' encompasses the "monitoring, intercepting, collecting, obtaining, analysing, using, preserving, retaining, interfering with, accessing or similar actions taken with regard to information that includes, reflects, arises from or is about a person's communications in the past, present, or future" (Necessary and Proportionate Coalition, 2014).

The 'big' in big data refers not just to volume, but also the velocity and variety of data elements and sources. These large databases are collected, created and owned by government and private stakeholders. Most of these huge datasets are either collected by government to provide welfare services but managed or stored by private stakeholders or collected by private technology corporations. For example, in India, Unique Identification Authority of India (UIDAI)[8], Census of India[9], Stock Exchange[10], the Ministry of Rural Development for the Mahatma Gandhi National Rural Employment Guarantee (MGNREGA)[11], Income Tax Department[12] among others hold huge datasets. Apart from these, other programmes of Indian government like Central Monitoring System, Human DNA Profiling, Smart Cities Mission, and Digital India programme also retain big data. Besides the government, non-state actors including telecom providers, online travel agencies, and online retail stores use big data analytics to promote their businesses. Though there are positive characteristics of big data and most of these big-data oriented programmes have a clearly laid down privacy policy, there is a lack of properly articulated access control mechanism and doubts over important issues such as data ownership owing to most projects involving public private partnership which involves private organisations collecting, processing, and retaining large amounts of data.

Therefore, the human rights implications of collection, storage, and use of big data in the Indian context need to be investigated. This paper explores the issue of privacy in the present big data age, and how big data gathered through ICT tools and social media platforms can be used against citizens. This paper will also analyse the importance of privacy and describe the technologies that put citizens' data most at risk on the net. Finally, this paper will identify possible ways to protect citizens' private data on the Internet in India.

---

8. *See more at https://uidai.gov.in/*
9. *See more at http://www.censusindia.net/*
10. *See more at http://www.bseindia.com/*
11. *See more at http://www.nrega.nic.in/netnrega/home.aspx*
12. *See more at http://www.incometaxindia.gov.in/Pages/default.aspx*

2

Research Objective

The objectives of the paper are to define big data in the Indian context, to further improve the understanding of big data, and help initiate public discourse around issues of privacy in the big data age. Expectations remain that this public discourse would potentially pave the way for developing the law in India to enable citizens to gain from big data, while limiting the potential violations and also ensuring the human rights of citizens.

2.1 Research Questions

The following questions guided the present research:

1. What are the different privacy issues related to collection, storage, and use of big data?
2. How can big data gathered through ICT tools and platforms, including social media be used against users?
3. What are the possible ways to protect users' privacy in the age of big data?

2.2 Research Methodology

To achieve the above-mentioned objectives and research questions, we analysed and used different research studies and academic lectures to identify the relation between right to privacy and collection, storage, and use of big data. We adopted both methodologies— desk review and case studies collection.

Under desk review, we identified emerging trends of right to privacy violations by state and non-state actors. We used media reports, news, briefing, research papers, and academic reports as sources for tracking official responses and analysis of right to privacy. We further attempted to look at some of the legal precedents in the exercise of right to privacy. To make the research paper more informative[1], we used some case studies of different governance initiatives that collect big data to explore the right to privacy issues related to those initiatives and tried to identify privacy violations in India. We used purposive sampling to identify case studies.

1. *The case studies are: Aadhaar platform, Central Monitoring System, Human DNA Profiling, Smart Cities Mission, and Digital India Programme*

3

Defining big data

Big data has been defined in various ways. The report by META Group (now Gartner) in 2001 defined big data using three vs—volume, velocity and variety (Laney, 2001). Big data is high-volume, high velocity, and/or high-variety information assets that demand cost-effective and innovative forms of information processing to enable enhanced decision-making and automation processing. Other characteristics of big data are articulated by different features such as scalability (Marz & Warren, 2015), veracity (Marr, 2014), value, variability (McNulty, 2014) and granularity. It is rare for datasets to satisfy all characteristics. Thus, most of the time, big data agencies determine the permutation and combination of these characteristics, and classify them as 'big data.'

3.1 Big Data and its Relationship with Privacy

Big data is a new paradigm of data-driven decisions. The quantity of data that is being generated by smartphones, televisions, social media networks, sensor-driven devices, and many other such networks that we constantly use in our daily life. Big data looks

for correlation rather than the causation, the 'what' rather than the 'why'. Big data comprises a variety of data types including text, imagery, and video. Different sources of such data types are mainstream news articles, social media platforms, images on Instagram, professional photographs, satellite imagery and aerial imagery captured by Unmanned Aerial Vehicles (UAVs), and videos from TV channels, YouTube, Vimeo and other channels. This is not limited to the developed world, with the developing world producing huge amounts of big data as well Rapid ICT developments and users' engagement with platforms like social media, micro blogging sites, among others enable unprecedented gathering, retention, and analysis of big data. The analytics of data collected from social media, websites, mobile GPS, and more could help to address various socio-economic problems (Morrison, 2016) and help in evolving effective solutions and measures (Coulton, Goerge, Putnam-Hornstein & de Haan, 2015). Thus, big data is being considered as an extraordinary resource that could potentially offer unique opportunities for all. Along with big data, metadata[1] also has the potential to reveal sensitive information about people's lives, political preferences, religion, sexual orientation, etc. Metadata can reveal information like the time at which a particular webpage was accessed, IP address, location, etc. There have been cases of governments collecting metadata (Blaze, 2013)[2]. The business model of many internet companies relies on the collection of metadata, in order to improve their services and to infer user-behaviour to further improve their products. However, gathering, accessing, and using such data carry significant threats to fundamental freedoms and human rights. Both—big data and metadata have the potential to seriously threaten individuals' rights to keep their personal and sensitive information private and to have control over how their information is used.

Since the 1970s, US industry in particular has been keen to accumulate

1. *Data that gives a description of data.*
2. *Metadata summarizes basic information about data, which can make finding and working with particular instances of data easier*

large amounts of information on consumers and run algorithms against that data, but over the past twenty years this form of data mining and automated decision-making has seen a rapid increase (Privacy International, n.d.). Privacy International has identified that this type of data analysis has expanded to passenger profiling, anti-terrorist systems, border management (i.e., automated-targeting system), and money laundering (i.e., suspicious transaction reporting and analysis). The ability of emerging technologies to transfer data over a network without requiring human-to-human or human-to-computer interaction is potentially another threat to privacy contributed by the so called 'Internet of Things' (IoT). IoT inter-relates "computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers" (Rouse, 2016). Most importantly, there is now an industry around big data, "selling solutions to governments and companies, while there are new opportunities for data collection—whether it is through mass communications surveillance, the merging of data sets, the deployment of new sensor technologies, and the emerging 'internet of things'" (Privacy International, n.d.). Governments are introducing bills, policies, laws and etc. to collect enormous personal data[3] and sensitive data[4] and initiating programmes to offer different types of services to the citizens and residents of the country.

In recent years, political leaders and businesses are proclaiming big data as a solution for diverse range of problems from corruption, providing government services and entitlements, fighting against diseases, etc.

---

3 . "Personal data" means data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller'. See: https://www.dataprotection.ie/docs/What-is-Personal-Data-/210.htm

4. 'Sensitive data encompasses a wide range of information and can include: your ethnic or racial origin; political opinion; religious or other similar beliefs; memberships; physical or mental health details; personal life; or criminal or civil offences. These examples of information are protected by your civil rights.' See: http://web.mit.edu/infoprotect/docs/protectingdata.pdf

It has been noted that in the name of public services, better delivery of citizen centric services, better user experience and providing safety and security of citizens, governments and private stakeholders are Cllecting, storing and analysing huge amount of citizens' data. However, concerns over the lack of transparency and accountability around the design of algorithms used to process the data, dubious security measures used in storage and maintenance of large datasets and over-reliance of big data as opposed to traditional forms of analysis, and the creation of new digital divides have grown. In the next section we are going to discuss how governments and different companies are collecting, storing, using, transferring, and reusing collected data for different purposes and how the right to privacy is being threatened and infringed upon in the present age of Big Data.

Finally, based on the 'Ten Point Action Plan' proposed by the UN special rapporteur for the right to privacy, this paper proposes a framework to be followed in India to protect citizens' personal and sensitive data on the Internet. At the end, the paper outlines some opportunities for making progress.

3.2 Privacy Safeguards at the International Level

Several countries have privacy safeguards for their own citizens. Privacy is a fundamental human right recognized in the Universal Declaration of Human Rights (UDHR), the International Covenant on Civil and Political Rights (ICCPR), the UN Convention on Migrant Workers[5] and the UN Convention on Protection of the Child[6], and in several other international and regional treaties. Numerous international human rights covenants, conventions and human rights courts[7] give specific reference to privacy as a right.

5. *See A/RES/45/158 25 February 1991, Article 14.*
6. *See UNGA Doc A/RES/44/25 (12 December 1989) with Annex, Article 16.*
7. *For example, The 1950 Convention for the Protection of Human Rights and Fundamental Freedoms, the Convention created the European Commission of Human Rights, the American Convention on Human Rights, the American Declaration of the Rights and Duties of Man. Also different Courts of Human Rights have also begun to addresses privacy issues in its cases.*

Article 12 of the UDHR provides that

"no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks[8]."

The ICCPR to date ratified by 167 States, provides in Article 17 that

"no one shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation."

It also states "everyone has the right to the protection of the law against such interference or attacks.[9]" The United Nations General Assembly (UNGA) in its resolution 68/167, international human rights law provides the universal framework against which any interference in individual privacy rights must be assessed. Other regional bodies such as the EU, recognise the right to privacy as a fundamental human right in Article 8 of the Charter of Fundamental Rights of the European Union.

The Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression mentioned that without the full guarantee of the right to privacy of all individuals, the right to freedom of opinion and expression cannot be fully enjoyed[10]. During the 13th Session in December 2009, the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms, Frank La Rue, also emphasized that, "surveillance systems require effective

8. *See the Article 12 of the Universal Declaration of Human Rights (UDHR), 1948.*
9. *See A/HRC/27/37 also available at http://www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx*
10. *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. (A/HRC/23/40). Human Rights Council. Twenty-third session. Agenda item 3. Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development Frank La Rue.*

oversight to minimize harm and abuses[11]" including by requiring a warrant issued by a judge on a case-by-case basis.

One of the previous UN High Commissioners for Human Rights, Navi Pillay published her detailed report on 'The Right to Privacy in the Digital Age' in July 2014. In the report, Ms. Pillay stated that internal procedural safeguards without an independent external monitoring body are not adequate for the protection of rights. The report also mentioned that effective protection of the law could only be attained if all the branches of government as well as an independent civilian oversight agency are built into the procedural safeguards[12].

Finally, on 8th March 2016, the UN Special Rapporteur for the right to privacy, Joseph Cannataci, in his first report laid out an ambitious agenda for addressing the growing concern about protection of privacy in the trans-border digital environment. In his report he stressed on two main principles. First, in a world that benefits greatly from an Internet without borders, privacy safeguards must be available regardless of national borders. Second, remedies for violations of privacy likewise must be available across these borders.
In order to facilitate the process, the Special Rapporteur has developed an outline 'Ten Point Action Plan'[13].

---

11. *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin. Human Rights CouncilThirteenth session. Agenda item 3 (A/HRC/13/37).*
12. *See The right to privacy in the digital age. Report of the Office of the United Nations High Commissioner for Human Rights (A/HRC/27/37).*
13. *Report of the United Nations Special Rapporteur on the right to privacy, (A/HRC/31/64). 8th March 2016.*

1. Going beyond the existing legal framework to a deeper understanding of what it is that we have pledged to protect
2. Increasing awareness
3. The creation of a structured, on-going dialogue about privacy
4. A comprehensive approach to legal, procedural and operational safeguards and remedies
5. A renewed emphasis on technical safeguards
6. A specially focused dialogue with the corporate world
7. Promoting national and regional developments in privacy-protection mechanisms
8. Harnessing the energy and influence of civil society.
9. Cyberspace, Cyber-privacy, Cyber-espionage, Cyberwar and Cyberpeace
10. Investing further in International Law.

3.3 Indian Constitution and Privacy

The Supreme Court of India has in a number of decisions recognized the right to privacy as a subset of the larger right to life and personal liberty under Article 21 of the Constitution of India[14] . The Article states, "no person shall be deprived of his life or personal liberty except according to procedure established by law". The Supreme Court of India has asserted that Article 21 of the Indian Constitution is the core of the Fundamental Rights. The extension in the dimensions of Article 21 has been made possible by giving an extended meaning to the words 'life' and 'liberty' in Article 21 (Iliyas, 2014).

The scope of this right first came up for consideration in Kharak Singh V. State of Uttar Pradesh case (Uppal, 2015)[15] , which was concerned with the validity of certain regulations that permitted the surveillance of suspects. In

14. *Kharak Singh v State of UP, AIR 1963 SC 1295; People's Union of Civil Liberties v. the Union of India, (1997) 1 SCC 318*
15. *Kharak Singh v. State of Uttar Pradesh, cited at: (1964) SCR (1) 332.*

the context of Article 19(1) (d), the right to privacy was again considered by the Supreme Court in 1975. The Supreme Court while deciding the case of Govind v. State of Madhya Pradesh[16] laid down that "a number of fundamental rights of citizens can be described as contributing to the right to privacy." However, the Supreme Court also stated that the right to privacy would have to go through a process of case-by-case development. The Supreme Court in the case of R. Rajagopal v. State of Tamil Nadu, for the first time directly linked the right to privacy to Article 21 of the Constitution and laid down thus:

"The right to privacy is implicit in the right to life and liberty guaranteed to the citizens of this country by Article 21. It is a 'right to be let alone'. A citizen has a right to safeguard the privacy of his own, his family, marriage, procreation, motherhood, child bearing, and education among other matters. None can publish anything concerning the above matters without his consent whether truthful or otherwise and whether laudatory or critical. If he does so, he would be violating the right to privacy of the person concerned[17] ..."

In the case of PUCL v. Union of India, the Supreme Court observed that telephone tapping would be a "serious invasion of an individual's privacy."[18] In the case of Selvi v. State of Karnataka the Supreme Court told that "an involuntary subjection of a person to narco analysis, polygraph examination and BEAP tests violates the right to privacy."[19] It is noted that even with the enlarged scope of Article 21 of the Constitution covering right to privacy, yet any individual's privacy is still limited due to the lack of proper policy and framework.

The ideas of privacy and data management that are prevalent can be traced to the Fair Information Practice Principles (FIPP). These principles are also

---

16. *Govind v. StateofMadhyaPradesh, cited at: AIR 1975 SC 1378.*
17. *R. Rajagopal v. State of Tamil Nadu, cited at: 1994 SCC (6) 632.*
18. *PUCL v. Union of India, cited at: (1997) 1 SCC 30.*
19. *Selvi v. State of Karnataka, cited at: AIR 2010 SC 1974.*

followed in international regimes such as the OCED Privacy Guidelines, APEC Framework or the nine National Privacy Principles articulated by the Justice A.P Shah Committee Report. In 2012, the Justice A. P. Shah panel recommended an over-arching law to protect privacy and personal data in the private and public spheres. The report also suggested setting up privacy commissioners, both at the Central and State levels. It has spelt out nine national privacy principles that could be followed while framing the law[20].

The Supreme Court observed that the right to privacy may be restricted for prevention of crime, disorder or protection of health or morals or protections of rights and freedom of others (Verma, 2015). Unfortunately, during the hearing of a batch of petitions seeking to stop the implementation of the Aadhaar Scheme in July 2015, the Centre replied in the Supreme Court, that privacy was not a fundamental right in India. Attorney-General Mukul Rohatgi said the right to privacy had been a "vague" concept all these years, a subject of varying conclusions from the Supreme Court (Kumar, 2015).

These frameworks give the power of consent to individuals so that they should be notified if their personal data is used.

3.4 Business, Big Data Bank, and Personal Privacy

The predictive power of big data has enormous potential in our lives. For example— receiving 95 per cent accurate weather information prior to 48 hours gives individuals the power to decide whether to carry a raincoat or not. But at the same time, the collection of huge amount of data by state and non-state actors has raised concern among users and the consequence of their every

20. *See Report of the Group of Experts on Privacy (Chaired by Justice A P Shah, Former Chief Justice, Delhi High Court) http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf*

move online being monitored. A survey carried out by Pew Research Center found that nine out of 10 respondents in USA said they felt consumers had lost control over how companies collect and use their personal information[21]. In another example, IBM's Personality Insight service can build a detailed user profile, moving beyond their basic demography or location information to their personal habits, which can reveal any individual's identity, opinions, social behaviour, and political behaviour. With 400 million users, Alibaba—the world's biggest online shopping platform is using its unique database of consumer information to compile individual "social credit" [22] scores. The Centre for Internet and Society (CIS) conducted a study 'Evaluating Safety Buttons on Mobile Devices: Technological Interventions, Personal Safety, and Women's Agency'[23] evaluating the privacy policies of 26 mobile safety apps and the end user agreements on their websites. The study identified 24 safety apps that send user data to the developer's server and access contacts and location information, 22 of them access all media files on the phone and four applications have permission to record and send audio files, even remotely.

The collection of users' personal data by mobile apps, websites, social networking websites, insurance companies or by any other commercial entity is smartly analysed by sophisticated software, and used or sold primarily for marketing purposes. This data is never forgotten, which violates the right to be forgotten

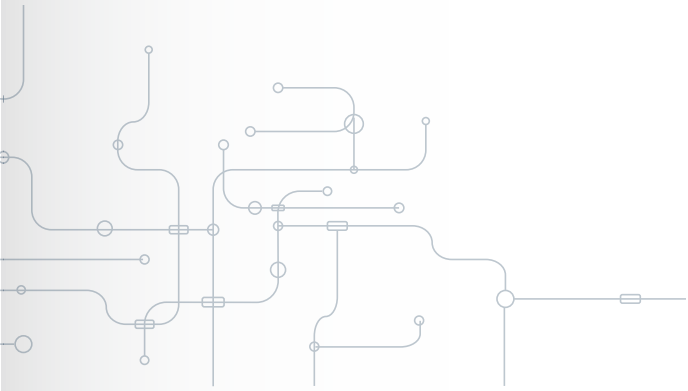
---

21. *The survey was conducted by the Pew Research Center. It is a nonpartisan American think tank which is based in Washington, D.C. It provides information on social issues, public opinion, and demographic trends shaping the United States and the world. See: http://www.pewresearch.org/topics/privacy-and-safety/*
22. *Social Credit comprises interlocking concepts of economics and politics which deal with the just relationship between man and the Society in which he lives.*
23. *See: https://cis-india.org/raw/evaluating-safety-buttons-on-mobile-devices-preview*

3.5 Public Service, Big Data Banks, and Personal Privacy

Another aspect of big data is the unethical access of personal data by the state. Many countries are collecting and updating their citizen databases i.e. Big Data Bank to include biometric identifiers that verify identity based on physical characteristics such as fingerprints, iris, face and palm prints, religion, ethnicity, sexual orientation, gait, voice, and DNA. Compulsory national identification systems have been implemented in a number of countries including Argentina (Rodriguez, 2012), Belgium, Colombia, Germany, India, Italy, Mexico, Peru, Spain, and Thailand (Electronic Frontier Foundation, n.d.). The Pakistani government is engaged in communications surveillance—of phone and internet protocol (IP) traffic, domestically and internationally and other data like biometrics and device registration information to counter 'internal and external' threats (Rice, 2015). China has set up a biometric data centre with the stated purpose of maintaining public security, but has allowed an online commercial enterprise offering biometric data-matching services access to the data. According to BBC, by 2020, everyone in China will be enrolled in a vast national database that compiles fiscal and government information, including minor traffic violations (Hatton, 2015). The intentions behind implementing these national identification schemes vary by country. In most cases, individuals are normally assigned an ID number with biometric details, which is used for a broad range of identification purposes. Huge amounts of personal and sensitive data of residents such as name, date and place of birth, gender, biometric information[24], current address, photograph, and other

24. Biometric verification is any means by which a person can be uniquely identified by evaluating one or more distinguishing biological traits. Unique identifiers include



information like family members is linked to this ID number and stored in a centralized database (Electronic Frontier Foundation, n.d.). Governments mainly create Big Data Banks for the range of purposes, including national identification systems (Privacy International, n.d.)[25] , electoral registers and supporting democratisation - Philippines (Jaracz, 2013), Ghana (Darkwa, 2013) and Kenya (Kisiangani & Lewela, 2012), aid delivery and social protection programmes (Garcia & Moore, 2012)[26], border management[27], and delivery of social services[28] . While supporters claim that biometric identifiers are an effective way to accurately recognize people, they are expensive and prone to error and most importantly, violate privacy and other human rights, putting citizens at risk of serious data breaches and the misuse of their personal data. Further, the growing concern is that big data technologies can potentially be used to discriminate against vulnerable groups and manipulate information. Biometric identifiers present extreme risks to individual's privacy and can create an alarming effect on right to privacy, freedom of expression, and freedom of assembly and association online and offline. For example, Aadhaar project of India collects all residents' biometric information. It has become a

---

fingerprints, hand geometry, earlobe geometry, retina and iris patterns, voice waves, DNA, and signatures.

25. *This is to prevent identity fraud and theft: governments in Mexico, India, and Argentina are all developing Biometric national identification systems and Thailand has launched a smart ID card that is believed to be the largest integrated circuit chip ID card project in the world.*
26. *UNHCR (http://bit.ly/1THlwlH) uses biometric technologies to process enrolment in refugee camps, the World Bank () to ensure effective targeting of beneficiaries, by funding biometric systems for registration of the urban poor in Benin and Kenya.*
27. *vMauritania is implementing a biometric entry-exit border control system as part of its security and counter-terrorism strategy and Senegal (http://www.snedai.sn/fr/) recently implemented a biometric visa process upon entry for nationals of certain countries.*
28. *WHO is running e-health programmes in collaboration with national partners across the world, other examples include TeleDoctor in Pakistan or E-Health Point in India which enable access to health care professionals, Nacer in Peru which uses telephone and internet technology to allow data management (collect, access, sharing, analysis) or m-Health (mobile - health) programmes such as Vida Net, the HIV patient reminder and information system in Mexico.*

tool for targeted surveillance and mass surveillance to surreptitiously identify and track citizens. Aadhaar has become the de-facto identity document accepted at private banks, schools, hospitals, telecom operators to buy SIM cards, medical insurance or any other utility services. The document is being linked to a number of social schemes as well. Besides, Aadhaar, there are other such 'so called initiatives' such as Central Monitoring System (CMS), Smart Cities Mission, and Digital India Programme that are using technologies and provisions that undermine individual privacy. Thus, if any individual wants to form an assembly or associate with like-minded people or groups, the state is likely already tracking their movements through social media, insurance companies, mobile phones, etc.

3.6 The Indian Big Data Bank - Aadhaar Platform, and the Right to Privacy

The Aadhaar programme, launched in 2009 is an initiative of Unique Identification Authority of India (UIDAI)[29] that aims to give universal identity to every Indian resident. This would help government provide services to intended beneficiaries by assigning them unique identity numbers in the form of the biometric Aadhaar card (Express News Service, 2016). Aadhaar is the world's largest biometric identity platform. As of May 2015, a total of 101,39,87,895 Aadhaar numbers[30] have been issued. Now, let us take a look at the technical and legal aspects of Aadhaar.

Technology systems have a major role across the UIDAI infrastructure. The Aadhaar database is stored on a central server. Enrolment of the residents is computerised, and information exchange between Registrars and the Central

29. *See more: Features of the UIDAI Model. Accessed from http://bit.ly/1R7YmDo on 29/04/2016.*
30. *The real-time statistics gathered at 13:12 (Indian Standard Time) on 15/05/2016. Source: https://uidai.gov.in/*

Identities Data Repository (CIDR)[31] takes place over a network. Authentication of the residents is done online. The Authority also claims that they put systems in place for the security and safety of information.

Aadhaar has some unique "data challenges that exhibit all characteristics of big data like data volume, data variety, and data velocity" (Balasubramanian, 2012). A number of technologies have been used to handle massive parallel processing, streaming data reads, data locality computing, low latency reads, data integrity and challenges of dealing with distributed data. In a nutshell, in this biometric identity platform,

1. 200 trillion biometric matches per day;
2. 2 peta byte of raw data stored;
3. 100 million authentication requests per day;
4. Tera byte scale data warehouse of 200 million records;
5. 50 million messages move per day and
6. 100 million database transactions per day.

After a very short debate, on 11th March 2016, the Lok Sabha i.e., Lower House passed the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Bill, 2016, with a voice vote (Sflc, 2016). Aadhaar plan has faced a number of controversies and it has been challenged before the Supreme Court of India. In Justice K. S. Puttaswamy (Retd) Vs Union of India, activists found potential human rights violation mechanisms present within the Aadhaar framework. However, the Attorney General has argued that people have no 'right to privacy.' While placing the bill in the Rajya Sabha, it was labelled as a Money Bill, making it more suspicious than usual. There are extensive threats to privacy contained within this legislation, which seeks to institutionalise an extensive, pervasive database that links multiple databases containing personal information (Arun, 2016). The rights to liberty and freedom of expression will be violated if the right to privacy is compromised since the former hinges on the latter.

---

31. Central Identities Data Repository (CIDR) is a government agency in India that stores and manages data for the country's Aadhaar project.

On its website the UIDAI declares, "we want to expose all publishable public information via a 'Data Portal' where all data is exposed in machine-readable formats. This portal allows third party developers to develop Web 2.0 applications based on this data."[32] Thus, the technology of Aadhaar platform allows "third party developers to develop Web 2.0 applications." Allowing third party to avail residents' data is a potentially risky step. Further, the government wants to expose "publishable public information". However, it is not clear what authorities mean by "publishable public information." It is not clear what is publishable and what is not? In terms of the partnership model, it states, "the UIDAI approach leverages the existing infrastructure of government and private agencies across India." Again the UIDAI is allowing 'private agencies' to develop mechanisms to "leverage existing infrastructure of government." "In addition, the Authority will partner with agencies such as central and state departments and private sector agencies, who will be 'Registrars' for the UIDAI. Registrars will process Aadhaar applications, and connect to the CIDR to de-duplicate resident information and receive Aadhaar. The Authority will also partner with service providers for authentication of identity."

The private company, Swabhimaan has developed a mobile app, TrustID that performs Aadhaar authentication. Any individual who has TrustID mobile app can send Aadhaar number of class III technicians (including plumber, electrician, etc) and the app then discloses their personal information like name, gender, age, address, and biometric scans. This information is held in a

32. *'Aadhaar Technology : See more at https://uidai.gov.in/aadhaar-technology.html Accessed on 05/05/2016.*

database maintained by the UID authority[33]. Similarly, Samsung's Iris Galaxy Tab can access personal information when the users' irises are scanned. These efforts clearly show that the use of Aadhaar will go beyond delivery of welfare schemes, subsidies and services such as availing LPG subsidy under the PAHAL scheme, MGNREGS payments, scholarships and pensions. Over time, such Aadhaar authentication for private services in companies, hospitals, or hotels will "help the government gather granular data on citizens".

UIDAI states that "biometric information will not be shared with anyone, nor it will be displayed publicly, except for purposes specified by regulations".[34] Further the statement elaborates that the Authority also makes sure that they envision a balance between privacy and purpose "when it comes to the information it collects on residents. The Authority will also enter into contracts with Registrars to ensure the confidentiality of the information they collect and store."[35] Here, the statement and the elaboration of the statement are contradictory. Secondly, the question is how the Authority is going to make a balance between 'privacy and purpose' that is not clear at all. Further it says, "the agencies may store information of the residents if they are authorised to do to enrol citizens for Aadhaar number." Thus, 'private agencies' can store and access sensitive personal data and information.

The government also wants to link mobile SIM with the Unique Identification (UID) number or Aadhaar. The main stated objective of linking SIM with Aadhaar Card is to remove fake users and control the misuse of mobile

33. *See 'How the government gains when private companies use Aadhaar' at: https://scroll.in/article/805467/how-the-government-gains-when-private-companies-use-aadhaar*
34. *See:http://www.prsindia.org/billtrack/the-aadhaar-targeted-delivery-of-financial-and-other-subsidies-benefits-and-services-bill-2016-4202/*
35. *Features of Aadhaar, accessed on 05/05/2016 and accessed from https://www.developer.uidai.gov.in/site/*

phones for anti-social activities (IANS, 2014). Since there is no detailed privacy framework, therefore there are possibilities that the Authority may use Aadhaar Card data against citizens. For example, during a protest, law enforcement agencies can record the videos of protesters, scan the iris data, and easily access information about protesters. Access to sensitive data of this nature gives unfair advantage to repressive governments and protesters are vulnerable to threats (Ghosh, 2016). The Aadhaar Database could be misused by government agencies and third parties via unauthorized access. Therefore, it is important to take measures to protect human rights and freedoms while developing any new technology. So far, the authority has not taken effective measures to protect the privacy of citizens concerning the Aadhaar database. It is also suggested that the authority take full responsibility for the consequences of a data breach. In spite of several assurances of safety, the authority offers citizens and residents "no guarantee of compensation or recompense if its poor choices endanger them." (Arun, 2016). Highly sensitive and personal data of more than 100 million Indians are being stored in two data centres located at Bangalore, Karnataka, and Manesar, Haryana (PTI, 2016). The crucial question is what would happen if even one of the data centre locations is compromised. It would be a privacy disaster for millions of Indian residents. The important question of the hour is whether or not the government can assure citizens that these initiatives/programmes and data that will be collected whether it be biometric, biological, iris scans, finger prints, human DNA structure, personal communications, everything put together—will not be misused.

As mentioned in earlier sections that the government is claiming the noble goal of creating such a database is to have a functional Public Distribution System. According to Section 7 of the Aadhaar Act 2016,

"The Central Government or, as the case may be, the State Government may, for the purpose of establishing identity of an individual as a condition for receipt of a subsidy, benefit or service for which the expenditure is incurred from, or the receipt therefrom forms part of, the Consolidated Fund of India, require that such individual undergo authentication, or furnish proof of possession of Aadhaar number or in the case of an individual to whom no Aadhaar number has been assigned, such individual makes an application."

On the one hand, citizens are being told that the objective of Aadhaar initiative is smooth delivery of government benefit schemes. However, analysing Section 33(2), one can see that law enforcement agencies may be given permission to access the 'Big Data Bank' through Aadhaar platform. It is not clear why law enforcement agencies need to be granted access to the database if the objective is to aid in the smooth delivery government benefit schemes.

Citizens have also been told that sensitive personal data in the database is secured and inaccessible for any purpose other than authentication. In the part 'protection of information' under the 'security and confidentiality of information' in the legislation, it states, "The Authority shall ensure the security of identity information and authentication records of individuals."[36] Later, in Section 29(2), the legislation makes significant exceptions and permits the authority to easily dip into Aadhaar data. It says, "The identity information, other than core biometric information, collected or created under this Act may be shared only in accordance with the provisions of this Act and in such manner as may be specified by regulations."

---

36. See: Chapter VI, Protection of Information. Section 28(1) of The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Bill, 2016

The Section 33 (1) of the Aadhaar Act 2016 says, 'Nothing contained in sub-section (2) or sub-section (5) of section 28 or sub-section (2) of section 29 shall apply in respect of any disclosure of information, including identity information or authentication records, made pursuant to an order of a court not inferior to that of a District Judge."

Lawyer Chinmayi Arun stated in an interview that the country does not have adequate trained district judges who can understand implications of databases like Aadhaar. Thus, there will be a possibility that district judges will authorise mass blocking of online content and gag orders and these judges can now authorise access to Aadhaar data without any disclosure or discussion with the citizen affected—only the Aadhaar authority will have the right to contest the order if it is so inclined. The Section 33 (2) of the Act states,

"nothing contained in sub-section (2) or sub-section (5) of section 28 and clause (b) of sub-section (1), sub-section (2) or sub-section (3) of section 29 shall apply in respect of any disclosure of information, including identity information or authentication records, made in the interest of national security in pursuance of a direction of an officer not below the rank of Joint Secretary to the Government of India specially authorised in this behalf by an order of the Central Government. One way is if a district judge orders disclosure of information." According to this Section, a Joint Secretary authorised by the government can direct disclosure of information "in the interests of national security".

This order will be reviewed by a committee consisting of the Cabinet Secretary and the Secretaries to the Government of India in the Department of Legal Affairs and the Department of Electronics and Information Technology. The Act offers no space where the affected party may appeal if his/her rights are affected. Thus, it creates a space for misusing Aadhaar database, which further leads to a threat to anyone's right to privacy.

3.7 Central Monitoring System and the Right to Privacy

The Central Monitoring System (CMS) came into media coverage in 2013; however, it was actually approved by the Cabinet Committee on Security (CCS) on 16th June 2011 and the pilot project was completed by 30th September 2011. The idea of having such a system to monitor all communications in India and centrally storing such data was first proposed in 2009 following the 2008 Mumbai terrorist attacks. CMS started off as a project run by the Centre for Communication Security Research and Monitoring (CCSRM), along with the Telecom Testing and Security Certification (TTSC) (Xynou, 2014). Ever since, India's Telecom Enforcement Resource and Monitoring (TERM) cell is operating the CMS to automate the process of lawful interception and monitoring of telecommunications. In order to require Telecom Service Providers (TSPs) to intercept all telecommunications as part of the CMS, the Clause 41.10 of the Unified Access Services (UAS) License Agreement was amended in June 2013. The amended clause states,

"But, in case of Centralized Monitoring System (CMS), Licensee shall provide the connectivity upto the nearest point of presence of MPLS (Multi Protocol Label Switching) network of the CMS at its own cost in the form of dark fibre with redundancy. If dark fibre connectivity is not readily available, the connectivity may be extended in the form of 10 Mbps bandwidth upgradeable upto 45 Mbps or higher as conveyed by the Governemnt, till such time the dark fibre connectivity is established. However, LICENSEE shall endeavour to establish connectivity by dark optical fibre at the earliest. From the point of presence of MPLS network of CMS onwards traffic will be handled by the Government at its own cost."

Moreover, draft Rule 419B under Section 5(2) of the Indian Telegraph Act, 1885, allows for the disclosure of "message related information" / Call Data Records (CDR) to Indian authorities. Call Data Records, otherwise known as Call Detail Records, contain metadata (data about data) that describe a telecommunication transaction, but not the content of that transaction. This means that 'Call Data Records' will include data such as phone number of caller and receiver, time duration of the call, date and time of the call, etc. This kind of data can only be issued on a national level through orders by the Secretary to the Government of India in the Ministry of Home Affairs, while on the state level, orders can only be issued by the Secretary to the state government in charge of the home department.

Unfortunately, Section 5(2) fails to regulate the details of CMS functioning. The government has released very little information about names of agencies that will have access to the system, which may allow surveillance,

and the legal standards that must be met to intercept various kinds of data or communications. Telecom Minister Ravi Shankar Prasad stated that in order to "...take care of the privacy of citizens, there is oversight mechanism in the form of review committee under chairmanship of the Cabinet Secretary at central government level and Chief Secretary at the state government level". (Bhargava, 2015). However, it is not yet clear what the nature of oversight mechanism may be or who the members of review committee are or when the review committee will submit the first review report.

It also remains unclear how users' data that is monitored and gathered through the CMS is being used. Going by this, CMS appears to be 'mass surveillance tool' that collects huge amounts of data every day. This raises many questions regarding its potential misuse and subsequent violation of India's right to privacy and other human rights. Prior to the implementation of CMS system, security agencies were required to approach the telecom operators to intercept calls or messages of suspected 'anti-national' and 'anti-social elements' but now it is built in to the licensing process itself. Since CMS was created without parliamentary approval, or without any public consultation the government should convene a full public debate about the intended use of the system before proceeding.

3.8 Smart Cities Mission, Big Data, and the Right to Privacy

While there's no single definition, the term 'smart city' generally refers to cities using information technology to solve numerous urban problems. A 'smart city' is an urban region, which is highly advanced in terms of overall infrastructure, sustainable real estate, communications, essential public service, and market feasibility (Internet Desk, 2016a). In the year 2014, the Indian government had announced plans to build 100 smart cities across the country in light of the shift towards urban transformation due to massive inflow of migrants from villages (Tolan, 2014). In July 2015, the Government of India published the 'Smart City Mission Statement and Guidelines'. The vision of Smart Cities Mission is to "drive comprehensive physical, institutional,

social, and economic infrastructure development"[37] and the government wants to develop all 100 smart cities in five years (Internet Desk, 2016b).

Exploring ICTs, smart cities offer sensors monitoring water system, use of clean energy, monitors traffic flows, and installs security cameras to make residents' life easier. Each smart city generates huge amounts of data, and stores and sends that data directly to city administrators. Apps that help residents navigate traffic, report potholes, and vote will be developed to complement services offered. Garbage collection will be totally automated (Tolan, 2014). The city administrators would store, analyse, and transfer data to other departments or third parties to monitor services and avail different services. Thus, big data and data analytics will certainly play a huge role in such a transformation, in which case different ICT tools will act as mediators to gather and store data.

The list of 20 smart cities out of the 98 shortlisted for the 'Smart Cities Mission' was released in January 2016 (Internet Desk, 2016c). As these 20 cities will be the first to receive funds, they will start developing infrastructure very soon. It is believed that authorities will install a number of sensors around these cities. This will be done by collecting and analysing large amounts of data—ranging from information about available parking spaces, emergency systems, naming streets, roads with low traffic, water and electricity usage and even refuse levels etc., finding problems and taking decisions to rectify them. Thus, leveraging the data and using Geographical Information Systems (GIS) to collect valuable information are some common techniques that are being used to make cities smarter. The other sources of data would be from fire alarms, disaster management situations, and energy saving mechanisms etc., which would sense, communicate, analyse, and combine information across platforms to generate big data to facilitate decision making processes and manage services in smart cities. It is a city where information technology is the principal infrastructure for providing essential services to residents. There are many technological platforms involved, including but not limited to automated sensor networks and data centres.

According to the Government of India's Department of Electronics and Information Technology, the plan to develop smart cities in the country could lead to a massive expansion of an Internet of Things (IoT) ecosystem within the country (Draft Policy on Internet of Things, 2015). The draft IoT policy aims to develop IoT products in this domain by using big data for government decision-making processes. In India, a key opportunity of using big data analytics in smart cities is with regard to traffic management and congestion. Collecting data during peak hours, processing information in real time and using GIS data and also using GPS history from mobile phones can give insight into the routes taken and modes of transportation preferred by commuters to deal with huge traffic (Singh, n.d.).

---

37. Smart City: Mission Statements and Guidelines Accessed on 29/04/2016 from http://bit.ly/1hHBqBq

The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011[38] deal with the accountability regarding personal and sensitive data security and protection; and as it applies to 'body corporates'[39] and digital data. Therefore, it can be established that anyone collecting and using big data for the smart cities in India would be excluded from the scope of these rules. This highlights the lack of a suitable regulatory framework to deal with potential privacy challenges in smart cities[40].

3.9 Digital India Programme, Big Data, and the Right to Privacy

The Digital India programme is a flagship programme of the Government of India with a vision to transform India into a digitally empowered society and knowledge economy[41]. The programme was launched on July 1, 2015 to ensure availability of government services to citizens electronically by improving online infrastructure and increasing Internet connectivity.

---

38. *Please find details about the The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 at http://bit.ly/1KXFuqN*
39. *A 'body corporate' is "any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities" under the IT Act 2008.*
40. *Rakesh. V, (2016). Too Clever By Half: Strengthening India's Smart Cities Plan with Human Rights Protection. http://bit.ly/1RuV0B1*
41. *See: 'About the Digital India Programme' retrieved on May 12, 2016 from http://www.digitalindia.gov.in/content/about-programme.*

The programme has nine different pillars[42]. Out of these nine pillars and 19 schemes, two of them i.e., e-Governance and e-Kranti are directly linked with Aadhaar platform and present huge potential to use big data analytics. These two pillars intend to reform governance through technology and enable electronic delivery of services. In the Digital India programme, "use of integrated & interoperable systems and deployment of emerging technologies like cloud & mobile would be undertaken to enhance the delivery of Government services to citizens".

According to the Digital India programme, "adoption of Unique ID would be promoted to facilitate identification, authentication, and delivery of benefits". Out of 19 schemes, 11 schemes that do not have a specific privacy policy laid down have been made available to the public. While general regulations may be followed in each scheme, no specific privacy guidelines are followed universally through these schemes. These schemes fail to recognize the breach of privacy that users are subjected to. There is a complete vacuum of security measures in seven schemes, while the remaining ones have undertaken limited measures. For example, in the CCTNS project, in some states the NCRB has reported that steps are being taken for data privacy, confidentiality and access control. But agencies have not rolled out any privacy principles. The NRHM Smart Card rolled out under the RSBY encrypts and duplicates data to protect the large amount of medical information collected, but no specific privacy protection provision has been made available[43]. Though, the four schemes have comprehensive privacy policies, measures are taken by the UIDAI[44] in the case of electronic health records[45]

---

42. *The nine pillars are: Broadband Highways, 2. Universal Access to Mobile Connectivity, 3. Public Internet Access Programme, 4. e-Governance- Reforming Government through Technology, 5. eKranti- Electronic delivery of services, 6. Information for All, 7. Electronic Manufacturing, 8. IT for Jobs and Early Harvest Programmes*

43 *. See:'Chhattisgarh RFP, Implementation of CCTNS Project in Chhattisgarh, Vol. I',available at http://ncrb.nic.in/BureauDivisions/CCTNS/All%20State%20RFP/Chhattisgarh/CG_CCTNS_RFP_Vol-I%20Functional%20&%20Technical%20Specifications.pdf.*

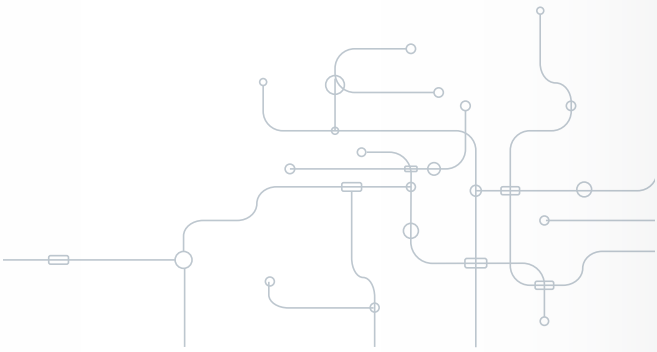
44. *The Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016.*

45. *See: 'Circular on Electronic Health Records Standards for India', Ministry of Health and Family Welfare (August 2013) available at http://www.mohfw.nic.in/showfile.php?lid=1672*

and the eSign framework for Aadhaar[46]. There is no specific policy laid down to account for subsequent protection of data after access to data has been granted to UIDAI or any other external agency. This means large scale digitisation, electronic collection of data from residents and processing common standards for interoperability between schemes, and potential sharing of data will be involved heavily in this programme.

---

46. See: 'eSign-Online Digital Signature Service', Ministry of Electronics and Information Technology (Controller at Certifying Authorities) available at http://www.cca.gov.in/cca/?q=eSign.html .



4

Discussion: Government Initiatives, Big Data, and the Right to Privacy

All these government initiatives and projects demand attention due to use of big data, which raises questions about the public dialogue in the context of big data, rights, and governance, status and role of India's data protection instruments impacted by big data, and the legal hurdles posed by it. Moreover, the absence of properly articulated access control and data ownership mechanisms in collecting, processing, and retaining large amounts of data using PPP (public private partnership) model make the whole privacy debate more complicated. All digital initiatives have been showcased as tools exclusively meant for disbursement of subsidies, protection of citizens, safety and security of the country, etc. However, most of the citizens of India do not realize that they can also be used for mass surveillance.

These programmes lack clarity and have faced several complications regarding usage, storage and ownership of such data, the actors involved and their accountability, concerns around data security,

privacy, and need for suitable regulatory frameworks. Apart from all debates regarding the right to privacy in India, it has been identified that none of the digital schemes, initiatives, and programmes were accompanied by a Privacy or Data Protection law. Since India does not have privacy law to protect against arbitrary intrusions into privacy, it is very difficult to protect individual privacy. An expert group lead by retired Justice A.P. Shah was created by the Planning Commission of India[1] to develop principles for a privacy law and the expert group submitted their report in October 2012. The report's recommendations identified that two laws were inconsistent on

"permitted grounds for surveillance, the type of interception that is permitted to be undertaken (monitoring, tracking, intercepting etc.), the type and granularity of information that can be intercepted, the degree of assistance that authorized agencies can demand from service providers, and the destruction and retention requirements of intercepted material. These differences have created an unclear regulatory regime that is non-transparent, prone to misuse, and that does not provide remedy for aggrieved individuals." (Report of the Group of Experts on Privacy, 2012).

It also suggested that all such legislation "be in compliance with the National Privacy Principles, the Principles should be used to harmonize the interception regime in India".

However, one expert suggests that until such provisions are established by law, it will be necessary to adopt mechanisms that ensure compliance towards use of Privacy Enhancing Technologies (PET) (Rane, 2016). Privacy-Enhancing

1. *The Planning Commission has been disestablished in 2014.*

Technologies is a system of ICT measures protecting informational privacy by eliminating or minimising personal data thereby preventing unnecessary or unwanted processing of personal data, without the loss of the functionality of the information system (Privacy Enhancing Technology, n.d.). In terms of this technological safeguard to protect individual privacy in India no mechanism has been implemented towards the integration of Privacy Enhancing Technology (PET) in digital tools and platforms to be used for citizens and by citizens. These technologies allow end users to safeguard the privacy of their personally identifiable information that they willingly provide to government agencies and other service providers. However, these technologies place end users in control over the information to share and also with whom to share. Users also get clear information about the recipients of this information.

Privacy Enhancing Technologies can be one of the ways to protect personal privacy in the present big data age. But PETs can never be the only measure to protect privacy. Along with privacy legislation and implementation of PETs mechanism, a multi-stakeholder approach is needed to deal the issue of 'right to privacy'. Different relevant stakeholders must follow some common and independent best practices to share, collect, store, analyse, and handle personal data and information in the age of big data.

5

Recommendations

Based on earlier discussions and analysis on privacy issue in the Big Data Age, it has emerged that different countries have different approaches to these issues. Most of these initiatives do not have clearly laid down privacy policies. It becomes more concerning when governments, and Internet and tech companies join hands to hand over or help to track personal data and sensitive personal data of citizens and customers.

The procedure of mass collection, combination, storage, and analysis of big data, allows for localisation, image, voice-recognition, and biometrics, and the collection and possible misuse of it could be done by state and non-state actors.

The main threat comes from authoritarian administrations. Service providers do not give proper attention to maintaining high level privacy and security for different online platforms. Existing legal instruments in some countries are really very good to protect privacy of citizens in the big data age. However, it is rare to find proper implementation of the 'Rule of Law'.

1. The paper suggests a set of recommendations on the issue of personal privacy in the present

big data era. It is recommended that State should have a set of clear guidelines on the collection, monitoring, storage, and owning of data, for authorities, tech companies and other stakeholders which are in area of collecting user data.

2. It is recommended to have a strong privacy policy and security measures to protect the citizens from potential cybersecurity threats and misuse of power in the hands of the government and private parties. The privacy law should be drafted in such a way that it protects all forms of personal data such as passwords, financial information, health conditions, medical history, biometric information along with a requirement to seek consent of individuals before collecting any personal information. If an app needs the personal information of the user, then that data needs to be destroyed soon after its use.
3. A multi-stakeholder approach needs to be taken to deal with the issue of privacy. Different stakeholders must follow some common and some independent best practices during collection, storage, analysis, and the handling of personal data and information in the age of big data.
4. It is recommended to have a regulatory body like TRAI (Telecom Regulatory Authority of India) regulate how data is being used and captured, and the availability of data in public domain by state and non-state actors.
5. It is recommended to hold public consultations on how to improve the privacy and data protection measures for citizens
6. Seek judicial authorization for access to any information stored in any data centre, if the need arises.
7. Provide proper physical and digital safeguards for different data centres.

8. Develop tools with Privacy Enhancing Technology (PET) integration to allow users control over their location disclosure and give them the choice of remaining anonymous.
9. Immediately end all ongoing mass-surveillance and refrain from collecting data on citizens en masse in the name of national security or public order.
10. In cases of national security or counter-terrorism purpose, obtain prior authorisation.
11. It is recommended that while collecting data from users, there should be informed consent from users on the storing and usage of data.
12. It is recommended that there is need to educate the end user and simplify the language used to write the policy, user agreements, and terms & conditions as much as possible. End user agreements need to be simpler and specific. The exclusions should be highlighted to show which data will be shared and which will not be. The user needs to be specifically informed about where and how his or her data will be used (purpose) and the data collected should be limited to the declared use.

6

Conclusion and Future Work

In the present digital age, good governance is impossible without the proper implementation of digital services and the active support of citizens. However, at the same time, governments need to make sure that citizens are protected from any type of harm while using different digital services and uphold the human rights framework. A common digital platform can gather different sets of data that help to coordinate the governance work properly, smoothly, quickly, and effectively. The potential of having a common digital platform for governance cannot be underestimated, especially in developing countries where mobile networks are growing very rapidly. Thus, digital empowerment is increasingly seen as the new paradigm of good governance.

However, it is important to keep in mind that some real challenges exist and some new challenges are being added to those existing challenges. Governments, some security agencies, terrorist groups, private companies and other unnamed groups are scrutinizing the online world continuously. Thus, the issue of personal privacy, safety, and security must be taken care of properly.

So, an exceptional attention with innovative approach should be taken at the time of developing new digital platforms for public services, as users look for guaranteed quality, anonymity, privacy, and security. It is suggested to use Privacy Enhancing Technologies during the development process of those platforms. This is the time for a new deal on data, and governments need to ensure protection of personal privacy and freedom.

Bibliography

Arun, C. (2016, March 18). Privacy is a fundamental right. The Hindu. Retrieved from ahttp:// www.thehindu.com/opinion/lead/lead-article-on-aadhaar-bill-by-chinmayi-arun-privacy- is-a-fundamental-right/article8366413.ece

Balasubramanian, R. (2012, July 6). Aadhaar - world's largest biometric identity platform (200 trillion biometric matches per day, 2 PB of data) . Retrieved from https://fifthelephant.talkfunnel.com/2012/417-aadhaar-worlds-largest-biometric-identity-platform-200-trillion-biometric-matches-per-day-2-pb-of-data

Bhargava, Y. (2015, December 3). Government's call intercept system to be ready by end of fiscal year. The Hindu. Retrieved March 15, 2016, from http://www.thehindu.com/business/central-monitoring-system-to-be-ready-by-end-of-fiscal-year/article7941946.ece

Blaze, M. (2013, June 19). Phew, NSA Is Just Collecting Metadata. (You Should Still Worry). Retrieved June 14, 2016, from http://www.wired.com/2013/06/phew-it-was-just-metadata-not-think-again/

Coulton, C. J., Goerge, R., Putnam-Hornstein, E., & De Haan, B. (2015). Harnessing Big Data for Social Good: A Grand Challenge for Social Work (Grand Challenges for Social Work Initiative ed., Grand Challenge: Harness Technology for Social Good, Working paper No. 11). American Academy for Social Work and Social Welfare.

Darkwa, L. (2013, August 15). Ghana's Elections 2012: Some Observations. Retrieved May 12, 2016, from http://forums.ssrc.org/kujenga-amani/2013/08/15/ghanas-elections-2012-some-observations/#.WZV5wVEjHIV

Electronic Frontier Foundation. (n.d.). Mandatory National IDs and Biometric Databases. Retrieved May 3, 2016, from https://www.eff.org/issues/national-ids

Express News Service. (2016, March 12). Aadhar Bill passed in Lok Sabha, Opposition fears 'surveillance'. The Indian Express. Retrieved March 19, 2016, from http://indianexpress.com/article/india/india-news-india/aadhar-card-uid-bill-lok-sabha-arun-jaitley/#sthash.wpx24XGv.dpuf

Garcia, M., & Moore, C. M. T. (2012). The Cash Dividend: The Rise of Cash Transfer Programs in Sub-Saharan Africa (Human Development ed., Directions in Development, Publication). Washington D.C.: The World Bank.

Ghosh, M. (2016, March 17). Aadhaar Card Bill Will Bring Exceptional Benefits; But, Privacy Remains a Concern. Retrieved April 29, 2016, from http://trak.in/tags/business/2016/03/17/aadhaar-ccard-benefits-privacy-concerns/

Hatton, C. (2015, October 26). China 'social credit': Beijing sets up huge system. BBC News. Retrieved May 10, 2016, from http://www.bbc.com/news/world-asia-china-34592186

IANS. (2014, October 31). Centre to link mobile SIM with Aadhaar number. Hindustan Times. Retrieved May 28, 2016, from http://www.hindustantimes.

com/india/centre-to-link-mobile-sim-with-aadhaar-number/story-iCycKHL8esJ1WwORFZbPYP.html

Iliyas, H. (2014, January 22). Right To Privacy Under Article 21 and the Related Conflicts. Retrieved June 10, 2016, from http://www.legalservicesindia.com/article/article/right-to-privacy-under-article-21-and-the-related-conflicts-1630-1.html

India, Government of India, Planning Commission. (2012, October 16). Report of the Group of Experts on Privacy. Retrieved April 29, 2016, from http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf

India, Ministry of Communication and Information Technology, Government of India, Department of Electronics and Information Technology (DeitY). (2015). Draft Policy on Internet of Things. Retrieved April 24, 2016, from https://www.mygov.in/sites/default/files/master_image/Revised-Draft-IoT-Policy-2.pdf

Internet Desk. (2016a, January 28). Govt. announces list of first 20 smart cities under 'Smart Cities Mission'. The Hindu. Retrieved April 23, 2016, from http://www.thehindu.com/news/national/Govt.-announces-list-of-first-20-smart-cities-under-Smart-Cities-Mission/article14027175.ece

Internet Desk. (2016b, May 11). Live: Parliament proceedings — '100 smart cities will be developed in five years'. The Hindu. Retrieved May 12, 2016, from http://www.thehindu.com/news/national/live-parliament-proceedings-may-11-2016/article8584347.ece

Internet Desk. (2016c, January 28). Govt. announces list of first 20 smart cities under 'Smart Cities Mission'. The Hindu. Retrieved April 23, 2016, from http://www.thehindu.com/news/national/Govt.-announces-list-of-first-20-smart-cities-under-Smart-Cities-Mission/article14027175.ece

Jaracz, J. (2013, March 01). Philippine biometric voter registration becomes law. Retrieved May 03, 2016, from https://www.secureidnews.com/news-item/philippine-biometric-voter-registration-becomes-law/

Kisiangani, E., & Lewela, M. (2012, October 29). Kenya's Biometric Voter Registration: New Solution, New Problems. Retrieved May 4, 2016, from https://issafrica.org/iss-today/kenyas-biometric-voter-registration-new-solution-new-problems

Kumar, A. (2015, August 10). Privacy, a non-negotiable right. The Hindu. Retrieved June 12, 2016, from http://www.thehindu.com/opinion/lead/privacy-a-nonnegotiable-right/article7519148.ece

Laney, D. (2001). 3D data management: Controlling data volume, velocity and variety. META Group Research Note, 6, 70.

Marr, B. (2014, March 6). Big Data: The 5 Vs Everyone Must Know. Retrieved from https://www.linkedin.com/pulse/20140306073407-64875646-big-data-the-5-vs-everyone-must-know

Marz, N., & Warren, J. (2015). Big Data: Principles and Best Practices of Scalable Realtime Data Systems. New York: Manning Publications.

McNulty, E. (2014, May 22). Understanding Big Data: The Seven V's. Retrieved from http://dataconomy.com/2014/05/seven-vs-big-data/

Morrison, A. (2016, February 23). Attention governments: Big Data is a game changer for businesses. Retrieved June 12, 2016, from http://blogs.worldbank.org/opendata/attention-governments-big-data-game-changer-businesses

Necessary and Proportionate Coalition. (2014, May). Necessary & Proportionate: International Principles on the Application of Human Rights to Communications Surveillance. Retrieved June 15, 2016, from https://necessaryandproportionate.org/principles

Privacy Enhancing Technologies. (n.d.). Retrieved May 11, 2016, from http://ictmatters.eu/index.php/privacy-enhancing-technologies

Privacy International. (n.d.). Biometrics: Friend or Foe of Privacy? (Briefing, Rep.). Privacy International.

Privacy International. (n.d.). What is Big data? Retrieved April 29, 2016, from https://www.privacyinternational.org/node/8

PTI. (2016, March 11). Biometric data of 99 crore Indians collected; data encrypted: Government. Economic Times. Retrieved May 7, 2016, from http://tech.economictimes.indiatimes.com/news/technology/biometric-data-of-99-crore-indians-collected-data-encrypted-government/51359480

Rane, R. (2016, January 28). Ensuring privacy in a digital age. Livemint. Retrieved from http://www.livemint.com/Opinion/ucp5me8oXUafwS1kPZSHNK/Ensuring-privacy-in-a-digital-age.html

Rice, M. (2015). Tipping the scales: Security and Surveillance in Pakistan (Special Report, Rep.). Privacy International.

Rodriguez, K. (2012, January 10). Biometrics in Argentina: Mass Surveillance as a State Policy. Retrieved May 5, 2016, from https://www.eff.org/deeplinks/2012/01/biometrics-argentina-mass-surveillance-state-policy

Rouse, M. (2016). Definition: Internet of Things (IoT). Retrieved May 21, 2016, from http://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT

Sflc. (2016, March 19). How Parliament played the Aadhaar Bill, 2016. Retrieved April 23, 2016, from http://www.legallyindia.com/blogs/how-parliament-played-the-aadhaar-bill-2016

Singh, R. P. (n.d.). Smart Traffic Management With Real Time Data Analysis. Retrieved from https://www.cisco.com/c/en_in/about/knowledge-network/smart-traffic.html

Tolan, C. (2014, July 18). Cities of the future? Indian PM pushes plan for 100 'smart cities'.

CNN. Retrieved April 29, 2016, from http://edition.cnn.com/2014/07/18/world/asia/india-modi-smart-cities/

Uppal, A. (2015). Right to Privacy in India. Retrieved June 10, 2016, from http://www.indialawjournal.org/archives/volume7/issue-2/article3.html

Verma, S. K. (2015). Constitutional Protection to Health Care. Retrieved June 10, 2016, from http://14.139.60.114:8080/jspui/bitstream/123456789/716/6/Constitutional%20Protection%20to%20Health%20Care.pdf

Xynou, M. (2014, January 30). India's Central Monitoring System (CMS): Something to Worry About?. Centre for Internet and Society [Web log post]. Retrieved April 29, 2016, from https://cis-india.org/internet-governance/blog/india-central-monitoring-system-something-to-worry-about

This issue paper has been produced as part of the Digital Empowerment Foundation (DEF) project APC-IMPACT (India, Malaysia, Pakistan Advocacy for Change through Technology), which aims to address restrictions on the internet by promoting and protecting Internet rights. This is a three-year project funded by the European Union (EU).

DEF DIGITAL EMPOWERMENT foundation
European Union
APC IMPACT INDIA, MALAYSIA, PAKISTAN ADVOCACY FOR CHANGE THROUGH TECHNOLOGY
Friedrich Naumann STIFTUNG FÜR DIE FREIHEIT