Privacy and National Security: The Balancing Act?

Divyanshu Dembi[1]

The tussle between law enforcement agencies (LEAs) and technology companies over the power to access communications, either in real time or post facto is not new. However with the advent of accessible technologies and the internet, the issue of balancing privacy and surveillance for national security concerns has entered the mainstream conversation. This paper aims to elucidate the contemporary debates around the 'balancing act' between national security surveillance (both pre and post facto) and the civil liberties of people, and traces the development of privacy as it is understand now. This paper analyses the legal development of a right to privacy in India and USA, and finally aims to find framing for a good privacy legislation.

Conceptualizing Privacy:

People often confuse privacy, intimacy and secrecy with each other. What is intimate is private but what is private need not be intimate such as one's bank account details. What is secret is not what is illegal. It could simply be something that one doesn't want to share with others.[2] The earliest conception of privacy was articulated in the now legendary paper titled 'The right to privacy'[3] by Warren and Brandeis in which they built up on the idea of 'right to be left alone'. They argued this right to be arising out of 'inviolate personality' rather than private property which was a commonly accepted argument in common law till then in form of the castle doctrine. Privacy as understood now does not have a hard and fast definition, and is evaluated on a case to case basis but it is now largely accepted that it majorly has three components to it, namely:

[1] L.L.B. candidate, Jindal Global Law School, 2020-2023. I would like to thank Asst. Prof. Soumya Singh Chauhan for her valuable guidance and comments on this paper.
[2] Bhairav Acharya, *The Four Parts of Privacy in India*, 50 Economic & Political Weekly 32-38 (2015).
[3] Samuel D. Warren & Loius D. Brandeis, *The Right to Privacy*, 4 H.L.R. 193-220 (1890).

a) Spatial control – right against un-warranted searches and seizures[4], and a 'reasonable expectation' of privacy in one's home.
b) Informational control – according to Alan Westin, the right to privacy has its essence in the ability of an individual to control information about one that is available to others.
c) Decisional autonomy – the right to control one's body and take intimate decisions. This jurisprudence of privacy was used in *Griswold v. Connecticut*[5] and *Roe v. Wade*[6] and was later affirmed in *Justice K. S. Puttuswamy (Retd.) and Anr. V UOI and Ors.*[7]

A brief history of privacy: India and USA

USA:

The American jurisprudence on privacy started in a case regarding the legality of evidence obtained against a bootlegger by the police using a hearing device that was fitted in a public telephone booth.[8] The defendant argued that the 4th amendment barred the police from listening to his private conversations as he had the 'right to be left alone', and thus the evidence should be inadmissible.[9] The bench decided in favor of the police and said that the fourth amendment only protects un-warranted searches in one's home and does not mandate a warrant if the act is done outside one's home. It attached the right to privacy to the place instead of the person. Brandeis J. dissented against the majority and opined that the right to be left alone was one of the most fundamental of rights given under the US constitution. *Olmstead* was overturned by *Katz v. United States*[10] in which the court now recognized that the right to privacy (even though not explicitly mentioned under the US constitution) travels with the person and is not attached to a static place. The bench in Katz devised a two-fold test for evaluating whether a right to privacy existed or not.[11] First was that if there was a 'reasonable expectation' of privacy or not, and second if that reasonability is something that is societally recognized. Later in *Griswold*

[4] 4th amendment of the US Constitution.
[5] 381 U.S. 479.
[6] 410 U.S. 113.
[7] AIR 2017 SC 4161.
[8] Olmstead v. United States 277 US 438.
[9] Abraham R. Wagner & Paul Finkelman, *Security, Privacy, and Technology Development: The Impact on National Security*, 2 TEX. A&M L. REV. 597 (2015).
[10] 389 US 347.
[11] Supra Note 10.

the court clarified that the right to privacy was 'embedded in the amendments and easily emanates from them, thus creating as zone of privacy".[12]

Technology disrupted not just financial markets, but also the US constitution. The 'reasonable expectation' test is more difficult to evaluate when individuals interact with other individuals online, through emails, social media and other ways. Questions such as is there a reasonable expectation of privacy when an individual sends an email to other or even when someone sends an E2E encrypted message to others are open to judicial interpretations. In *Smith v Maryland*[13], the court held that accessing the meta-data of phone calls would not require a warrant under the fourth amendment. The court used the third party doctrine and interpreted the meta-data as business records and not personal records. A further analysis of how the right to privacy has evolved in America is beyond the scope of this paper, but it is important to see how the right evolved in lines of the interpretation of different facets of the right as understood now.

India:

Merely four years after the constitution had come into force, *M. P. Sharma v Satish Chandra*[14] saw the Supreme court giving an off the cuff remark on existence and validity of a right to privacy under the constitution. The question was whether the search conducted by the government in the course of investigation violated an individual's right against self-incrimination. The court stated that since the constitution framers had not explicitly recognized the right to privacy analogous to US fourth amendment, the courts had no justification to import this right into a totally different right. This formed the part of the apex court's early positivist reading of law.[15]

Arguably the first case of state surveillance in India was *Kharak Singh v. State of UP*[16] in which the question was regarding the constitutionality of certain police regulations that granted the police the right to conduct 'domiciliary visits' to known offenders or 'history-sheeters'. The bench in *Kharak Singh* declined to read right to privacy in the Indian constitution under article 21 as a fundamental right and based its decision on the common law right to privacy while holding the provisions unconstitutional. The now prevalent understanding of right to privacy

[12] Id.
[13] 442 U.S. 735.
[14] 1954 AIR 300.
[15] S.P Sathe, *Judicial Activism: The Indian Experience,* 6 Washington Journal of Law and Policy 29-107 (2001).
[16] AIR 1963 1295.

as a fundamental right was first articulated in *Govind v. State of MP*[17] in which the bench held that the right indeed existed in part III of the constitution but was not absolute and had to be balanced against 'compelling state interests'. Right to privacy since then has been weighed against different rights and the courts have mostly upheld the idea of right to privacy as guaranteed under the constitution. However, it was in *Puttuswamy*, that the 9 judge bench finally set the record straight. The bench clearly established the right to privacy as a fundamental right under part III of the constitution arising out of article 21. However the judgment recognized that it is not an absolute right and has to be weighed against the state interests. To that effect the three pronged test as to when the right to privacy can be restricted was laid down:

a) Legality of what is sought to be done
b) Need, in terms of a legitimate state aim
c) Proportionality which ensures a rational nexus between the legitimate state aim and least restrictive means adopted to achieve it.

Why privacy matters: In search of the mythical balance

Privacy is an essential prerequisite to the exercise of individual freedom, and its erosion weakens the constitutional foundations on which democracy and good governance have traditionally been based.[18] As outlined above, there is a rich jurisprudence of different facets of right to privacy held under both the Indian and US legal systems, however this right often comes up in contrast with other rights. One area where the right to privacy is most commonly restricted is when it comes to national security. Different legislations throughout the years have given power to LEAs over wiretapping, email surveillance, mobile device access etc. In the US, post 9/11 there was a culture of secrecy over statute[19] that was followed by intelligence agencies and law enforcement agencies in which many surveillance programs were either strengthened by executive access or were de novo created such as the Patriot Act. Thus the 'need' for surveillance over-rode the concern for 'civil liberties'.

[17] AIR 1975 1378.
[18] Charles D. Raab, *Security, Privacy and Overreach*, Security in a small nation (2017).
[19] Brittany Adams, *Striking a Balance: Privacy and National Security in Section 702 U.S. Person Queries*, 94 Wash. L. REV. 401 (2019).

However most scholarship agrees to the idea that any right to privacy is not absolute, and there are genuine concerns of national security that need to be addressed. In that sense these rights are not seen as absolute or unconditional, but rather as *qualified rights*. This qualification — that these rights are in turn subject to other rights — is important if these rights are to be consistent, balanced and mutually reinforcing. Each right must be protected and respected, to the greatest extent possible, but it cannot exist in isolation. There is no privacy without respect for security; there is no liberty without respect for privacy; security requires both certain liberties and privacy. It is therefore unfruitful (indeed misleading) to cast debates about privacy, liberty and security as a matter of choice or 'balancing' between these rights, still less to think of trade-offs between these rights. There is no metric for 'weighing' different rights, or even for comparing the 'weight' of different rights in particular cases.[20] But it is feasible to set out robust standards that must be met in adjusting rights to one another and to devise and establish structures to do so. Stephen Coleman in his paper[21] makes the argument that "while there are some extremely worthwhile points raised in discussions of the legal issues of privacy, discussions have shown that a legally based discussion cannot answer the fundamental ethical questions raised by the issue of privacy and the Internet".[22] Therefore this raises the larger question of whether solely using the framework of law to analyse privacy as a concept is sufficient or not.

Current debate on the ethics and philosophy of surveillance derive a lot from Michel Foucault's 'Panopticism'.[23] The Panopticon was an architectural system of prison in which the prison guard could stand in a tower and see every prisoner while the prisoners could not see the guard. In line with Foucault's idea of how modern society's discipline their subjects and bind them in constraints and restrictions, the system is based on a collective psychology of fear and being constantly monitored. Similarly, wide spread surveillance programs create a psychological fear of always being watched while feeling helpless about protecting one's privacy.[24]

---

[20] Supra Note 19.
[21] Stephen Coleman, *Email, Terrorism & Right to Privacy*, 8 Ethics and Information Technology 17-27 (2006).
[22] Id.
[23] H. Akın Ünver, *Politics of digital surveillance, National Security and Privacy*, 2 Centre for Economics and Foreign Policy Studies 1-21 (2018)
[24] Varsha Bansal, *The Hyderabad model of CCTV Surveillance* (Jan. 9, 2021, 17:25), https://www.livemint.com/news/india/the-hyderabad-model-of-cctv-surveillance-11604926158442.html. The Hyderabad police had planned to deploy around 1 million CCTV cameras by the end of 2020, which roughly amounts to 1 CCTV per 10 citizens.

After the Snowden revelations of the scale of mass state surveillance, the privacy culture in America, and around the world tilted in favour of protection of civil liberties. One very significant step that was taken by technology companies, particularly those that make mobile devices was to encrypt their devices. Against the wishes of the state and law enforcements, companies like Apple and Google encrypted their mobiles with such technology that made even the companies themselves unable to decrypt those devices. These fears of LEAs came true in Paris and San Bernardino, California shootings where the attacker's devices were encrypted. The law enforcement agencies argue that it hampers their ability to solve crimes. Given the fact that these companies are themselves unable to decrypt these messages, a court warrant in such cases is worthless. The LEAs term this gap as 'going dark'. The famous case of *DOJ v Apple Inc.*[25] serves as an example of this. In order to not be bound by such encryptions, governments around the world have been demanding tech companies to include 'backdoors' in their code for access by the LEAs in cases of national security. India recently joined US, UK, Canada and Japan in issuing letters to major tech companies asking them to build backdoors in their E2E encrypted system for them to access.[26]

However there is a pertinent issue that often goes un-noticed in national security v civil liberties debates, which is the way in which intelligence communities and LEAs understand the effects of their performance upon individuals and society, with respect to the values of security (or safety), privacy, and the exercise of freedoms. There exists an institutional 'mobilization of bias' within these communities that leaves many issues and alternative perspectives out of account, or suppresses them. Which is to say that how these actors think about the debate has a direct bearing on what ends up happening on the ground irrespective of what the law and conventions are. Post 9-11 in USA, and post 26-11 in India, the LEAs and the governments of respective countries went on a surveillance overdrive backed up by popular support of masses. The ripple effects of those policy changes still exist in both countries in the forms of Patriot Act, in US and various national surveillance programs in India as outlined later.

At the heart of the debate lies the question of consent and knowledge on the part of the actor's whose data is being collected and stored, and the kind of benefits that are generated as a result of that. Surveillance is not just a national issue but also an international issue as no country wants to lose the intelligence race by reducing its powers to conduct surveillance and collect

[25] 952 F. Supp. 2d 638.
[26] Shubham Singh, *Internet Freedom Foundation raises alarm over India's move for backdoor access to encrypted data*, Inc. 42 (Jan. 9, 2021, 17:38), https://inc42.com/buzz/iff-alarmed-over-indias-move-for-backdoor-access-to-encrypted-data/.

information and data. The logic is that if a single intelligence agency has the ability to process and store overwhelmingly large volumes of data compared to other agencies, this enables the monopoly agency to weaponize that data in the form of digital espionage or diplomatic strong-arming against other countries.[27] The rhetoric of conducting surveillance for ensuring 'better security' is not just a legitimate concern for the state, it is also a good electoral promise and strategy.

Another worrying trend is that of 'profiling' that takes place due to mass surveillance both online and offline. The GDPR contains a jargon-free definition[28] of profiling which is easier to comprehend: 'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. The worst practice for a democracy seems to be over-centralizing information, intelligence and national security decisions into a small group of decision-makers, without establishing accountability mechanisms. In 2002, American department of defence had sanctioned a profiling program titled 'Total Informational Awareness' whose goal was to extensively gather all kinds of data and locate any 'suspicious' behaviour. After this information was made public, public outcry lead to its shut down. Similar profiling programs are extensively run in India, examples of which are given later.

Privacy as boundary management

Anja Kovacks of the Internet democracy project, argues that the most important aspect of privacy is privacy as boundary management.[29] She argues that the information that we reveal about ourselves to various people helps us retain control over our identity and is an integral part of our dignity. Furthermore she says that the binary idea of privacy as there, or not there is a false spatial construct whereas privacy as boundary management is always dynamic, because it is contextual. She argues that the trend of collecting all around data in the hope that it will be valuable later if not today, leave the individuals with little to no choice of constructing

[27] Supra Note 24.
[28] 'Profiling' under Article 4, Chapter 1, General Data Protection Regulation (Jan. 9, 2021, 17:42), https://gdpr-info.eu/.
[29] Anja Kovacks, *When our bodies become data where does that leave us* (Jan. 9, 2021, 15:30), https://deepdives.in/when-our-bodies-become-data-where-does-that-leave-us-906674f6a969.

their identity vis-à-vis the state and other people. She also critiques the idea of 'data-fication of bodies' a process by which data is collected around a person to make their virtual profile in order to gain insights by state and non-state actors. She argues that "the truth is that neither bodies nor data exist outside of the social world — and so neither do bodies-as-data" and thus such data which is collected outside the social context of the individual whose data is being collected is not objective and is itself riddled in social biases and contexts.

I've got nothing to hide

When it comes to articulating the real issues at hand that lack of privacy facilitated by surveillance risks bring about, Daniel J. Solove's paper[30] is a shining beacon. Solove writes that the nothing to hide argument in its most formidable sense is as follows, "The NSA surveillance, data mining, or other government information-gathering programs will result in the disclosure of particular pieces of information to a few government officials, or perhaps only to government computers. This very limited disclosure of the particular information involved is not likely to be threatening to the privacy of law-abiding citizens. Only those who are engaged in illegal activities have a reason to hide this information. Although there may be some cases in which the information might be sensitive or embarrassing to law-abiding citizens, the limited disclosure lessens the threat to privacy. Moreover, the security interest in detecting, investigating, and preventing terrorist attacks is very high and outweighs whatever minimal or moderate privacy interests law-abiding citizens may have in these particular pieces of information." Solove argues that since most of the data collected isn't very sensitive (bank records, travel history, call stamps) the correct way to look at the data asymmetry between the state and the individual is more on the lines of Franz Kafka's 'The Trial' than the popular Orwellian narrative of big brother. In the book Kafka portrays a world where a bureaucracy with inscrutable purposes uses people's information to make important decisions about them, yet denies the people the ability to participate in how their information is used. What we're seeing in the world right now, with unprecedented advances in 'digitising' identity and government programs such as Aadhar, is an example of building this data asymmetry. Solove argues that the point captured by the Kafka metaphor is a certain sense of helplessness in how the data is collected, stored and used. Not only does that lead to a chilling effect, but also fundamentally alters the relationship of an individual with the state. Constitutional scholar Gautam Bhatia argues that the constitution is fundamentally about power and how it's

[30] Daniel J. Solove, *'I've Got Nothing to Hide' And Other misunderstandings about Privacy*, 44 San Diego Law Review 745-772 (2007).

distributed.[31] Petitioners in the constitutional challenge to Aadhar had argued that the program alters the relationship between the individual and the state. They argued that a citizen's right to identity, personhood and all other rights derived from being recognised as a person were made subject to the assertions and claims made by the database system. And that the citizen had no reasonable control over such a database due to asymmetry of power and information.[32] It gives the state immense power over the person due to possible data seeding, but most importantly in a Focauldian manner trap their bodies in a system of constraints and thus discipline them by chilling effects. Senior advocate Shyam Divan in the constitutional challenge to Aadhar famously said that '*the constitution is not a charter of servitude'*.[33]

Types of privacy harms:

Solove divides privacy harms into four major criteria, and includes sub topics:

a) Information Collection – Surveillance, interrogation
b) Information processing – Aggregation, Identification, Insecurity, Secondary Use, Exclusion
c) Information dissemination – Breach of confidentiality, disclosure, exposure, increased accessibility, blackmail, appropriation, distortion
d) Invasion – Intrusion, decisional interference

Privacy needs to be understood as an umbrella term for a lot of related things, and not a definitive thing. Privacy has for most of its conception, understood to be an individual right. Right from Brandeis' conception of 'right to be left alone' to the modern understanding of informational privacy and decisional autonomy – it is the individual who is theorised to exercise these rights. To that effect, one of the reason why the privacy argument seems weak against the national security argument is because it's seen through a false utilitarian lens of one versus many. Solove argues that the characterisation of individual rights as being antithetical to social interests in false. He uses John Dewey's argument about how as social beings we cannot isolate the idea of our good from the society's good. Dewey contended that the value of protecting individual rights emerges from their contribution to society, and thus society makes way for individual rights for the benefit that this space provides. Because otherwise, in a

[31] Code, technology & Law, a lecture delivered by Gautam Bhatia accessible at https://www.youtube.com/watch?v=YqUZokjvSTc&list=PL_wMv9o9KGI7OxNylgAzhqfKikvYUA_x8&index=1&t=1039s.
[32] Reetika khera, Dissent against Aadhar (1st ed. 2019).
[33] Vidyut, *The Constitution is not a charter of servitude*, Aam Janta – Intellectual Anarchy! (Jan. 9, 2021, 17:51), https://aamjanata.com/democracy/the-constitution-is-not-a-charter-of-servitude/.

utilitarian sense, there is no place for individual rights. Solove argues that only those societies will attract people to live which do not suffocate their members by their intrusiveness. Thus privacy is not to be protected just for the individual, but for the society too as it has a societal value as well.

Privacy is often misunderstood as concealment of illegal acts, which is why the nothing to hide argument seems formidable when weighed on a utilitarian scale. Solove argues that privacy when understood as a family of issues is a better way to approach the debate. This *Dataveillence* can deter people from engaging in legal activities as well, thus creating a chilling effect. The harm is that it reduces the range of viewpoints expressed and engaged with, and these views are most likely to be directly in contrast to populist/state ideals which in turn further reduces the chances of dissent which was recently characterised as the 'functioning valve' of a democracy by Chandrachud J.[34] The illegal use of facial recognition systems by Delhi Police during the CAA-NRC protests is the perfect example as to how such data collection deters dissent and creates a chilling effect. However it is very difficult to show evidence of deterred behaviour in courts, and the larger harm in strict sense in such privacy violations. The Kafkaesque problem is that of "indifference, errors, abuses, frustration, and lack of transparency and accountability" by the data collecting institutions whether state or non-state.

The larger issue of data correlations leading to profiling of a person by de-anonymizing even anonymised data has been raised in the recent Indian Non personal data framework as well.[35] Solove argues that the real asymmetry arises from the sheer lack of knowledge on people's part as to how their data is collected and used by the state and private entities. This exclusion introduces an imbalance in power as Bhatia argues. The question is not about whether one has done something illegal, but is the power concomitant with such mass surveillance programs justified in the hands of the executive?

As is agreed in most scholarship, the issue with arguing for privacy is that privacy harms lack dead bodies. There is no visceral reaction as opposed to other torts, and thus is it difficult to convince either the people or the policymakers about the seriousness of the issue. He argues that "privacy problems resemble certain environmental harms which occur over time through

[34] PTI, *Dissent is the safety valve of democracy: Justice Chandrachud*, Hindustan Times (Jan. 9, 2021, 17:55), https://www.hindustantimes.com/india-news/dissent-is-the-safety-valve-of-a-democracy-justice-chandrachud/story-1vOft3QfRvszjGuBBWSuLI.html.

[35] Report by the committee of Experts on the Non Personal Data Governance Framework, Ministry of Electronics & Information Technology, Government of India (Jan. 9, 2021, 17:57), https://static.mygov.in/rest/s3fs-public/mygov_160922880751553221.pdf.

a series of small acts by different actors". The real question is not if there should be any surveillance or not, but what kind of oversight and accountability should be established. To that effect the need of the hour is to have a robust legal framework that guards individual liberty but also gives room for acting on national security threats. That demands a commitment to due process, something that is opposite to most agencies modus operandi when it comes to surveillance. Thus what we need is a cultural shift within these agencies and in popular culture as well, so that people don't keep falling for the national security rhetoric and as a result keep giving up their civil liberties one by one.

What makes for a good privacy law?

In India the only 'privacy law' in effect is Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.[36] The Rules only deals with protection of "Sensitive personal data or information of a person". The rules provide the reasonable security practices and procedures, which the body corporate or any person who on behalf of body corporate collects, receives, possess, store, deals or handle information is required to follow while dealing with "Personal sensitive data or information". Under section 72A of the (Indian) Information Technology Act, 2000[37], disclosure of information, knowingly and intentionally, without the consent of the person concerned and in breach of the lawful contract has been also made punishable with imprisonment for a term extending to three years and fine. However section 69 of the Act, which is an exception to the general rule of maintenance of privacy and secrecy of the information, provides that where the Government is satisfied that it is necessary in the interest of the sovereignty or integrity of India or, defence of India or, security of the State or, friendly relations with foreign States or, public order or, for preventing incitement to the commission of any cognizable offence relating to above or, for investigation of any offence - it may by order, direct any agency of the appropriate Government to *intercept*, *monitor* or *decrypt* or cause to be intercepted or monitored or decrypted any information generated, transmitted, received or stored in any computer resource. This section empowers the Government to intercept, monitor or decrypt any information including *information of personal nature* in any computer resource. The scope of section 69 of

[36] Available at https://www.wipo.int/edocs/lexdocs/laws/en/in/in098en.pdf.
[37] Available at https://www.indiacode.nic.in/bitstream/123456789/1999/3/A2000-21.pdf.

the IT Act includes both interception and monitoring along with decryption for the purpose of investigation of cyber-crimes.[38]

The grassroots movement save our privacy[39] created Indian Privacy Code, 2018 - a civil society initiative built by using the best practices around the world in data privacy and data protection to model a privacy code. It is based on seven key principles which form the litmus test for strength and robustness of any privacy law. The principles are stated as:

Firstly, individual rights should be at the centre of privacy and data protection. Any such law or protocol must be in consonance with best global practices and be guided by the apex court's *right to privacy*[40] judgement, while making reference to the European GDPR.

Secondly, any law must also give room for certain exceptions, but without clear wording sometimes exceptions swallow up the rule. A three part test for exceptions should be: (a) worded clearly; (b) limited in purpose, necessary and proportionate to the aim; and (c) accompanied by sufficient procedural safeguards.

Thirdly, a strong data protection authority must be created which has the mandate and the jurisdiction to enforce the privacy principles and/or law. The intended DPA must serve as the forum for the redressal of the general public's grievances. The authority should have the ability to investigate, hold hearings and pass orders with directions and fines.

Fourthly, in addition to a strong DPA, the doors of the courts should always be open to the public. While the DPA serves as the forum for redressal, the public should retain the remedies of approaching the civil courts.

Fifthly, the government should protect user privacy. Most of the privacy discourse is centred on private players and their ability to harm our privacy. However, the government has the most amount of power and information on the people of India. It is imperative that the government, its arms, bodies and programmes be compliant with the privacy protection principles through a data protection law.

---

[38] Vijay Pal Dalmia, *Data protection Laws in India*, Mondaq, (Jan. 14, 2021, 9:40), https://www.mondaq.com/india/data-protection/655034/data-protection-laws-in-india--everything-you-must-know#:~:text=The%20Constitution%20of%20India%20does,of%20the%20Constitution%20of%20India.

[39] *7 Principles of the Indian Privacy Code*, Save Our Privacy, (Jan. 11, 2021, 12:40), https://saveourprivacy.in/principles.

[40] Supra Note 8.

Sixthly, the government or the state must not make sharing of data a pre-condition for accessing state welfare. Withholding services on the pretext of requirement of collection of data effectively amounts to extortion of consent. Individuals cannot be forced to trade away their data and citizenship at the altar of being permitted to use government services and access legal entitlements on welfare.

Seventhly, any data protection law must also limit mass or "dragnet" surveillance as it contravenes the principles of necessity, proportionality and purpose limitation.

These principles are built on the twin premises of privacy by design and giving more control to the user that strengthen the core of the legislation without being riddled with exceptions. Any privacy law is only good as its exceptions. As outlined in the paper above, notions of individual privacy when compared to larger utilitarian notions of 'national security' or 'greater good often lead to privacy laws that are vaguely worded and allow the LEAs and the state to work around the very principles of privacy that the legislation aims to establish. An example of such phenomenon at work is in the Personal Data Protection Bill 2019.[41] A detailed analysis of the intended legislation is beyond the scope of the paper, however our argument is that by containing almost blanket and absolute exceptions for the state to bypass privacy protocols on certain vague national security and allied grounds, while at the same time also allowing the state to subject its departments to the same exemptions,[42] the bill does not do enough to restore the power and data asymmetry generated by mass collection of individual data by state. The Bill also missed a historic opportunity to introduce surveillance reforms.

The Indian Surveillance problem

India has had many surveillance laws in form of Indian Telegraph Act, 1885; Indian Telegraph Rules, 1951; and IT Act 2000 among others. The 'national security' argument is quite prevalent in the legislative intent behind such laws.

The Aadhar debate is at the very core of the privacy - surveillance debate in India. Scholars such as Reetika Khera and Jean Dreze make the argument[43] that not only does making Aadhar

[41] Personal Data Protection Bill 2019, http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf.
[42] *Save Our Privacy: A public brief and analysis on the PDP Bill 2019*, Internet Freedom Foundation (Jan. 10, 2021, 11:45), https://saveourprivacy.in/media/all/Brief-PDP-Bill-25.12.2020.pdf.
[43] Reetika Khera, *The different ways in which Aadhar infringes on privacy* (Jan. 9, 2021, 12:45), https://thewire.in/government/privacy-aadhaar-supreme-court.

mandatory for public distribution of benefits affect the most downtrodden, but the privacy risks are massive. Since Aadhar is the centralised database that is connected to more and more services and thus more data, it acts as a single point of entry to compromise all of the data accumulated on an individual. Moreover, since data is the new oil, the Aadhar program is 'seeded' into every database and thus becomes the bridge to hitherto un-connected data. Not only will that lead to greater profiling by anyone who has access to that database, it is also a Kafkaesque nightmare Solove talks about. Individuals have no knowledge about how their data is collected and used by state and non-state actors. India has been working on massive surveillance and monitoring systems. Three particular programs are:

Crime and Criminal tracking network system

The CCTNS has been already been rolled out in more than 14,000 police stations across the country. Since the program entails recording and storing information about suspects and convicts, there are profiling concerns especially in the absence of any data protection law.[44]

Central Monitoring system

The program is aimed to lawfully intercept text messages, social media engagements, phone calls on mobile phones and landline etc. It eliminates hurdles that existed before any LEA in order to gain access to such information. Thus without any intermediary in place now, it raises concern of non-transparency. Moreover, the individuals have no knowledge of their data being collected or intercepted and thus can allow for mass surveillance under the 'national security' excuse.

National Intelligence Grid

This is a magnum opus surveillance program in which certain government agencies listed under the program will be able to gain access to almost all of data on an individual that is collected by various sectors such as banking, telecom, service etc. The program will use big data analytics to study huge amount of data generated across various data points in order to profile individuals and analyse patterns.[45] There are rumours of social media accounts being linked to

[44] Internet Freedom Foundation, *Watch the Watchmen Series Part 3: The Crime and Criminal Tracking Network System* (Jan. 9, 2021, 17:59), https://internetfreedom.in/watch-the-watchmen-part-3/.

[45] Internet Freedom Foundation, *Watch the Watchmen Series Part 1: National Intelligence Grid* (Jan. 9, 2021, 17:59), https://internetfreedom.in/watch-the-watchmen-series-part-2-the-centralised-monitoring-system/.

NATGID as well, however there has not been an official announcement on that as of now.[46] The most worrying aspect however is the exemption of NATGRID from the Right to information act, further exacerbating the lack of knowledge on peoples' part about how their data is used.

Conclusion:

In India and world over, the issue of privacy has finally picked up steam and is being talked and debated from conference halls to dinner tables. The recent change in Whatsapp privacy policy[47] surged in a hitherto unprecedented conversation around encryption, privacy, and the power of big tech. With giants such as Elon Musk convincing people to shift to Signal[48], a more private messaging app – the privacy debate is finally breaking the elite spaces that it has been largely confined to. However, in order to conceptualize the privacy – surveillance debate in a way that protects peoples' civil liberties while also allowing the LEAs to nab criminals, what is needed is a robust legal framework and an unwavering commitment to due process and protecting peoples' privacy.

[46] Vijaita Singh, *NATGRID wants to link social media accounts to central database*, The Hindu, https://www.thehindu.com/news/national/natgrid-wants-to-link-social-media-accounts-to-central-database/article29402252.ece

[47] Tech Desk, *WhatsApp updates terms of service and privacy policy: Why you need to accept it*, Indian Express (Jan. 9, 2021, 18:04), https://indianexpress.com/article/technology/social/whatsapp-new-2021-terms-of-service-and-privacy-policy-new-changes-accept-or-delete-7134815/.

[48] Anumeha Chaturvedi, *Signal beeps luder in India as WhatsApp tweaks policy*, The Economics Times (Jan. 9, 2021, 18:05), https://economictimes.indiatimes.com/tech/technology/whatsapp-rival-signal-reports-growing-pains-after-elon-musks-tweet/articleshow/80172451.cms.