Use of personal data by intelligence and law enforcement agencies

Rishab Bailey Vrinda Bhandari Smriti Parsheera Faiza Rahman[*]

August 1, 2018

[*]Rishab Bailey, Smriti Parsheera and Faiza Rahman are Technology Policy researchers at the National Institute of Public Finance and Policy (NIPFP). Vrinda Bhandari is a practicing advocate.

[†]We thank Ajay Shah for valuable discussions. An earlier version of this paper dated 27 June, 2018 was referred to in the Report of the Committee of Experts under the Chairmanship of Justice B.N. Srikrishna ('Fair and Free Digital Economy: Protecting Privacy, Empowering Indians' published on 27 July, 2018). This version has been updated following the release of the Committee's report.

Contents

1 Introduction

Ensuring safety and security of the nation, prevention and investigation of crimes and maintenance of law and order are among the key functions of the state. In the course of performing these functions intelligence bodies and law enforcement agencies (**LEAs**) often encounter the need to access and make use of the personal data of individuals. While the legitimacy of these functions cannot be denied, it is equally important to acknowledge that the authority to conduct surveillance constitutes a powerful tool in the hands of the state and its exercise needs to be circumscribed through sound legal processes. This is in line with the observations made by the nine judges of the Hon'ble Supreme Court in *Justice K.S. Puttaswamy (Retd.)* v. *Union of India*[1] (**Puttaswamy**). While recognising the right to privacy as a fundamental right the court held that like other fundamental rights, the right to privacy is not absolute. It can be restricted by laws pursuing other legitimate aims (such as protecting national security and preventing and investigating crimes) provided that such aims are pursued through a procedure that is just, fair and reasonable.

The widespread adoption of modern technologies and reduced storage and computing costs have made it easier for the state to carry out both physical and electronic surveillance. In many instances, this has led to a shift in the nature of surveillance – from a targeted activity to be carried out in a narrow set of circumstances to broad based surveillance over a larger set of the population. The United States (US) Supreme Court recently noted in *Carpenter* v. *United States* that there have been seismic shifts in digital technology that make it possible to continuously track the location of multiple persons, not just for short periods, but for years on end.[2]

Recent debates around surveillance in India have also centered around the spread of digital technologies, particularly in the context of the Aadhaar project, and the enhanced potential for monitoring of individuals using those means. In July, 2017, the Government had constituted a Committee of Experts under the Chairmanship of Justice B.N. Srikrishna (**Srikishna Com-**

[1](2017) 10 SCC 1. Also see Vrinda Bhandari, Amba Kak, Smriti Parsheera and Faiza Rahman, An analysis of Puttaswamy: the Supreme Court's privacy verdict, September 20, 2017, available at https://ajayshahblog.blogspot.com/2017/09/an-analysis-of-puttaswamy-supreme.html.

[2]Supreme Court of the United States, decided on 22 June, 2018, No. 16-402, 585 US –. The case related to the acquisition of cell-site records by the Government. The Court held that this amounted to a search under the Fourth Amendment of the US Constitution, which would require a warrant supported by probable cause.

mittee) to propose a data protection framework for India. The White Paper released by the Srikrishna Committee in November, 2017 recognised that the use of data for counter-terrorism and intelligence gathering functions in India lacked sufficient legal backing. The Committee has since released its report titled "A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians" along with the draft of a Personal Data Protection Bill, 2018.

Sections 42 and 43 of the draft law proposed by the Srikrishna Committee incorporate the *Puttaswamy* tests of legality, necessity and proportionality while exempting the processing of personal data in the *interests of the security* or for *prevention, detection, investigation and prosecution of any offence or any other contravention of law*. The Committee's report contains a broader set of recommendations relating to structural reforms in the intelligence gathering framework, which have unfortunately not found a place in the draft law.

The paper is structured as follows. The next section reviews the existing legal framework on surveillance in India. In the third section we map some elements of this existing framework against the tests of legality, legitimate aim, proportionality and procedural safeguards identified in the *Puttaswamy case*. The fourth section contains a discussion of the principles and best practices from other jurisdictions, with a focus on countries that have attempted to strike a balance between the civil liberties of individuals and the state's requirement to pursue certain surveillance activities. Drawing from these discussions, the fifth section sets out our recommendations on the way forward for India in terms of building appropriate protections relating to access and use of personal data by intelligence agencies and LEAs. In the concluding section of this paper we analyse how the Srikrishna Committee's report and draft law fare in terms of implementing a sound legal framework on surveillance, based on the normative framework elucidated in the previous section.

2 Current framework in India

Present surveillance systems in India suffer from two main limitations. The first relates to the design of the legal framework, which gives a broad mandate to intelligence agencies and LEAs, without affording sufficient legal and procedural safeguards to for protecting civil liberties. The second issue relates to the limitations of state capacity in carrying out surveillance functions. This problem is exacerbated by the tendency to gather large amounts of surveil-

lance data, which comes with the burden to process and analyse that data and extract relevant information from it.

In the context of delivery of public services, it has been noted that activities that are highly *"discretionary"* – requiring decisions that cannot be easily mechanised – and *"transaction-intensive"* – involving a large number of transactions – are particularly challenging to deliver.[3] Similar logic can be extended to the exercise of surveillance powers by state agencies. The function in question is clearly discretionary in nature, requiring specific application of mind in every case, and transaction-intensive, in terms of the volume of surveillance requests.[4] It is therefore important to devise mechanisms that can support narrowly tailored surveillance activities, that simultaneously satisfy the pursuit of civil liberties and optimum utilisation of limited state capacity. We discuss this idea further in the subsequent sections of the paper. The present section restricts itself to providing an overview of the legal provisions relating to surveillance in India, the agencies carrying out these functions, and the key judicial decisions on this issue.

2.1 Relevant legal provisions

The legal framework governing surveillance in India stems mainly from the Telegraph Act, 1885 (**Telegraph Act**), the Information Technology Act, 2000 (**IT Act**) and the Code of Criminal Procedure, 1973 (**CrPC**).

The interception of post and telegraph/telephone is governed by the provisions of the Telegraph Act.[5]

[3] Lant Pritchett and Michael Woolcock, "Solutions when the Solution is the Problem: Arraying the Disarray in Development", *Center for Global Development Working Paper No. 10*, September, 2002, available at https://www.cgdev.org/sites/default/files/2780_file_cgd_wp010.pdf.

[4] See Suyash Rai, "A Pragmatic Approach to Data Protection", Ajay Shah's blog, 9 February 2018, available at https://ajayshahblog.blogspot.com/2018/02/a-pragmatic-approach-to-data-protection.html for a discussion on the state capacity constraints that need to be taken into account while devising a data protection framework for India.

[5] The definition of "telegraph" under section 3(1AA) of the Act has been interpreted by the Supreme Court in *Delhi Science Forum v Union of India*, (1996) 2 SCC 405 to cover telephones and telecommunication services. The Court in *Bharti Airtel Ltd. v Union of India*, (2015) 12 SCC 1 also clarified that all electromagnetic wave based services fell within the definition of telegraph under section 3(1AA). The TDSAT in *Total Telefilms Pvt Ltd. v Prasar Bharati*, (2008) TDSAT 127 interpreted "telegraph" to mean broadcasting, which would require a license under the Telegraph Act. Recently, the Madras High Court in *Tata Communications Ltd v TRAI*, (2018) SCC Online Mad 1991 held that the Cable Landing

Section 5(2) of the Telegraph Act envisages a two-tiered threshold test that needs to be satisfied for the Central or State Government to authorise the interception of messages. *First*, there should be a condition of a public emergency or interest of public safety. *Second*, the concerned official needs to be satisfied that the interception is necessary or expedient in the interests of the sovereignty and integrity of India, the security of the state, friendly relations with foreign states or public order or for preventing incitement to the commission of an offence. While the Telegraph Act establishes the substantive framework for lawful interception, the Indian Telegraph Rules, 1951 (particularly Rule 419A, which was introduced in 2007) provide the procedural framework for the same. Rule 419A details the process to be followed prior to, during, and subsequent to the interception, including the relevant sanctioning authority that can issue such an order; the review process; and the total duration of the interception order.

In addition to the interception of calls and messages, the law also provides for a mechanism for the Government to authorise access to information contained in computer resources under Section 69 of the IT Act. Although it is modelled along the lines of the Telegraph Act, there are three notable distinctions. *First*, Section 69 of the IT Act permits the appropriate government to "intercept, monitor or decrypt" any information generated, transmitted, received or stored in any computer resource, without the pre-requisites of "public emergency" or "public safety". *Second*, the IT Act widens the second-tier of the test under the Telegraph Act by providing for two additional grounds, namely in the interest of the "defence of India" and the "investigation of any offence". *Third*, Section 69(3) imposes an additional obligation on intermediaries, subscribers and persons in-charge of the computer resource to "extend all facilities and technical assistance" to the intercepting agency.[6]

The government has also notified the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 (**2009 IT Rules**) under Section 69(2) of the IT Act. These rules govern the procedural aspects of interception and decryption, including designation of the competent authority who can issue the interception order, requiring reasons for the direction, providing a duration and review of such orders, clarifying the role of the intermediary, and prohibiting the disclosure

Stations' building, i.e. concrete structure has equipment inside it which will qualify as telegraphic equipment within the meaning of section 3(1AA).

[6] See also Vrinda Bhandari and Renuka Sane, "Towards a privacy framework for India in the age of the internet", Working Paper No. 179, *NIPFP Working Paper Series*, October 2016, available at https://macrofinance.nipfp.org.in/PDF/1LEPCPr_BhandariSane20160926.pdf.

to unauthorised persons.

In addition, Section 69B of the IT Act empowers the Central Government to authorise "any" government agency to monitor and collect "traffic data" under the low threshold of "enhanc[ing] cyber security and for identification, analysis and prevention of any intrusion or spread of computer contaminant in the country". Traffic data has been widely defined in Section 69B(4)(ii) and includes metadata. The Government has also provided a procedural framework for the issuance of directions relating to traffic data under the Information Technology (Procedure and Safeguards for Monitoring and Collecting Traffic Data or Information) Rules, 2009. Apart from this, rules framed under other provisions of the IT Act also facilitate state surveillance for the purpose of identity verification or for prevention, detection investigation, prosecution, and punishment of offences.[7]

Thus, it is clear that provisions flowing from the IT Act considerably widen the government's powers of surveillance as compared to telephone interception under the Telegraph Act. Surveillance by private actors, *to the extent it is regulated*, is, however, prohibited. For instance Section 43 of the IT Act prohibits any unauthorised access, copying of data, damage or disruption of a computer, computer system or network while Section 66 lays down the punishment for the same.

In addition to these laws, Sections 91 and 92 of the CrPC can also be used for targeted surveillance. Section 91 empowers a Court or any officer in charge of a police station to summon "any document or any other thing" from a person, if it is "necessary or desirable" for the purposes of any investigation, inquiry, trial or other proceeding under the Code. This provision is often used by the police to seek information from intermediaries, or otherwise access stored data.[8] Further, Section 92 regulates the interception of a document, parcel or thing in the custody of a postal or telegraph authority.[9]

[7] Rule 6(1) of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 authorise the disclosure of sensitive personal data by body corporates to government agencies. Rule 3(7) of the Information Technology (Intermediaries Guidelines) Rules, 2011 requires intermediaries/ISPs to provide "information or any such assistance" to government agencies on a lawful order. Even cyber cafes have been classified as intermediaries and under Rule 7 of the Information Technology (Guidelines for Cyber Cafe) Rules, 2011, they have to provide "any necessary information" to authorised officers conducting an inspection, which could include search histories. See Software Freedom Law Centre, "India's surveillance state: Other provisions of law that enable collection of user information", 2015, available at https://bit.ly/2yWZXzZ.

[8] *Id.*

[9] An order to this effect may be made by a Magistrate or Court although any other

Besides the different categories of interception and communications surveillance, physical surveillance is also carried out by the police and intelligence agencies. In case of the police, this is supposed to be done in accordance with the processes laid down in local police manuals. The "Model Police Manual" released by the Bureau of Police Research and Development notes that "surveillance and checking of bad characters" is an integral part of the police's duty to reduce crime and for the preservation of peace and security.[10] Rule 1052(1) of this document requires a history sheet to be maintained with the names of all persons within the limits of the police station "who are known or are believe to be *addicted* to or aid or abet, the commission of crime", *regardless* of whether they have been convicted or not. Similarly, Rule 1059(17) of the Karnataka Police Manual states that the station house officer must show photos of "rowdies" to his subordinate officers and instruct them to watch their movements and record their surveillance.[11]

2.2 Relevant actors and procedures

In India, the interception of communication is carried out by various authorised Central and State level LEAs. The nine Central agencies authorised for this purpose are – (i) Intelligence Bureau (**IB**), (ii) Narcotics Control Bureau, (iii) Directorate of Enforcement, (iv) Central Board of Direct Taxes, (v) Directorate of Revenue Intelligence, (vi) Central Bureau of Investigation (**CBI**), (vii) National Investigation Agency, (viii) Research & Analysis Wing (**R&AW**), (ix) Directorate of Signal Intelligence, Ministry of Defence – for Jammu & Kashmir, North East & Assam Service Areas. The State LEAs that are authorised to intercept communication comprise of the Director General of Police of the concerned State or the Commissioner of Police, Delhi for Delhi Metro City Service Area.[12]

The Ministry of Home Affairs has issued Standard Operating Procedures (**SOPs**) to the Central LEAs for lawful interception, handling, use, sharing, copying, storage and destruction of records by them. In addition, the Department of Telecommunications has also issued SOPs for lawful interception

Magistrate, the Commissioner of Police or District Superintendent of Police can require the postal or telegraph authority to search for such document pending a judicial order.

[10]Bureau of Police Research and Development, http://bprd.nic.in/content/63_1_ModelPoliceManual.aspx.

[11] See Mrinal Satish, "Bad Characters, History Sheeters, Budding Goondas and Rowdies", 23(1) *Natl L. School of India Rev* 133-160 (2011) for more details.

[12]Response by Mr. M. K. Raghavan, Minister of State, Ministry of Home Affairs to Lok Sabha Starred Question No. 294, answered on February 11, 2014.

to Telecom Service Providers (**TSPs**).[13] According to the SOPs applicable to TSPs, interception orders should be subject to eight types of checks before the monitoring can be allowed. These include, receiving the original written request "in a sealed envelope"; a requirement that any "request received by telephone, SMS and fax, should not be accepted under any circumstances";[14] and the initiation of an inquiry process (if required) to check the authenticity of the request.[15]

It is important to note that amongst the Central LEAs, intelligence agencies such as the IB and R&AW, have not been created by any statute of the Parliament, and do not have any clearly established roles or limitations on power. Further, the legal status of the CBI is currently under challenge.[16] In 2011, Mr. Manish Tewari introduced the Intelligence Services (Powers and Regulation) Bill, 2011 (**the Bill**), to regulate the manner of functioning and exercise of powers of Indian intelligence agencies, specifically the IB, R&AW, and the National Technical Research Organisation (functioning under the control of the Prime Minister). The Bill provided for a Designated Authority for authorisation procedures and systems of warrants (for surveillance), and established a National Intelligence Tribunal for investigating complaints against these three agencies. The Bill sought to achieve effective oversight through the creation of a National Intelligence and Security Oversight Committee, while also providing for an Intelligence Ombudsman

[13]Response by Hansraj Gangaram Ahir, Minister of State, Ministry of Home Affairs to Lok Sabha, Unstarred Question No. 4186, answered on March 28, 2017; Response by Mr. M. K. Raghavan, Minister of State, Ministry of Home Affairs to Lok Sabha, Starred Question No. 294, answered on February 11, 2014; Response by Mr. Naresh Agrawal, Minister of State, Ministry of Home Affairs to Rajya Sabha, Unstarred Question No. 2593, answered on August 12, 2015.

[14]If a request is made on e-mail, a physical copy must reach the TSP within 48 hours.

[15]Shalini Singh, "Centre issues new guidelines for phone intercept", *The Hindu*, 10 January 2014, available at http://www.thehindu.com/todays-paper/tp-national/centre-issues-new-guidelines-for-phone-interception/article5560426.ece.

[16]In *Navendra Kumar v. Union of India*, W.A. No. 119/08 decided by the Division Bench of the Gauhati High Court on 06.11.2013 held that Resolution No. 4/31/61-T dated 01.04.1963 issued by Secretary to the Government of India constituting the CBI is *ultra vires*; that the CBI is neither an organ nor part of the Delhi Special Police Establishment Act; and that it cannot be treated as a police force constituted under the Act. The High Court's reasoning was based on the fact that no "police force" could be empowered to investigate crimes if it had been constituted by a mere resolution of the MHA in the purported exercise of its executive powers. It further held that the impugned resolution was not 'law' within the meaning of Article 13(3)(a) of the Constitution, and the executive instructions therein could not be regarded as "procedure established by law" under Article 21. However, the Supreme Court on 10.11.2013 stayed the operation of the High Court's judgment, and there has been no movement on the matter ever since.

for efficient functioning of the agencies. However, the Bill lapsed in October 2012,[17] continuing the current legislative vacuum.

2.3 Key judicial decisions

One of the first cases concerning surveillance in India was *Kharak Singh v. State of U.P*,[18] which questioned the constitutionality of a range of surveillance activities being carried out on "history sheeters" under the U.P. Police Regulations. The Court upheld some aspects of the surveillance design, such as "secret picketing", but struck down the provision on "night time domiciliary visits" as being violative of "ordered liberty" under Article 21 of the Constitution. To the extent that the majority held that the right to privacy is not protected by the Constitution, it was overruled by the nine judge bench in *Puttaswamy* in 2017.

Nine years after *Kharak Singh*, the Supreme Court considered the issue of surveillance again in *R.M. Malkani v. State of Maharashtra*,[19] where it held that there was no compulsion or coercion in attaching a tape recorder to a telephone and Section 25 of the Telegraph Act, which deals with intentionally damaging or tampering with telegraphs, was not violated. Rejecting a privacy-based challenge, the Court stated that while the targeted telephone tapping of a "guilty person" would not be struck down, "*the telephone conversation of an innocent citizen will be protected by Courts against wrongful or high handed interference by tapping the conversation.*"

The tide turned with *Gobind v. State of M.P.*,[20] where Regulations 855 and 856 of State Police Regulations – under which a history sheet was opened against the petitioner who was placed under surveillance – were read down. Although the Court did not give a specific finding on the existence of the right to privacy, it proceeded on an "assumption" of such a right, which could be curtailed and narrowly tailored in light of compelling state interest. This was followed by a series of decisions, starting with *Malak Singh v. State of P&H*,[21] where a surveillance register for habitual and potential offenders was upheld, as long as it was for the purpose of preventing crime and there was

[17] Manish Tewari, "State of the Union: Time for intelligence reforms?", *Deccan Chronicle*, 19 March 2016, available at https://www.deccanchronicle.com/opinion/op-ed/190316/state-of-the-union-time-for-intelligence-reforms.html.

[18] (1964) 1 SCR 332.

[19] (1973) 1 SCC 471.

[20] (1975) 2 SCC 148.

[21] (1981) 1 SCC 420.

no illegal interference.

In the context of communications surveillance, the constitutionality of Section 5(2) of the Telegraph Act, particularly the absence of procedural safeguards, was challenged before a two-judge bench of the Supreme Court in *PUCL v. Union of India*.[22] While upholding the section, the Supreme Court issued a series of guidelines[23] to narrowly tailor the restrictions on privacy due to wire tapping of phones. These guidelines subsequently formed the basis for the amendment of the Telegraph Rules.[24] Notably, the Court observed that "*in the absence of any provision in the statute, it is not possible to provide for prior judicial scrutiny as a procedural safeguard*". Accordingly, the Court did not mandate prior judicial review of interception requests in the procedure suggested by it.

On the question of standards of admissibility of evidence, the Supreme Court has in many cases, including *R.M. Malkani* and *Pooran Mal v. Director of Inspection (Investigation)*,[25] held that illegality in search does not vitiate the entire proceedings and there is no constitutional bar in using illegally obtained evidence. Similarly, in *State v. Navjot Sandhu*,[26] illegally obtained evidence was admitted on the principle that Indian law (and specifically the Telegraph Act) does not prohibit admitting otherwise relevant evidence on the ground that it was illegally obtained. After citing these decision, the Court in 2013 in *Umesh Kumar v. State of A.P.* held that "*It is a settled legal proposition that even if a document is procured by improper or illegal means, there is no bar to its admissibility if it is relevant and its genuineness is proved.*"[27]

[22](1997) 1 SCC 301.

[23] These included designating the Home Secretary as the authorised officer; requiring the specification of the communication to be intercepted and the address from where it is to be intercepted; requiring a consideration of whether the target information could be reasonably acquired by other means, limiting the duration of interception and the use of intercepted material, record keeping, and establishing a review committee.

[24]Rule 419A of the Indian Telegraph Rules, 1951

[25](1974) 1 SCC 345.

[26](2005) 11 SCC 600.

[27](2013) 10 SCC 591. The Court further went on to hold that "*If the evidence is admissible, it does not matter how it has been obtained. However, as a matter of caution, the court in exercise of its discretion may disallow certain evidence in a criminal case if the strict rules of admissibility would operate unfairly against the accused. More so, the court must conclude that it is genuine and free from tampering or mutilation.*"

2.4 Provisions in telecom licenses

State surveillance is also facilitated by the obligations cast upon TSPs under the telecom license agreements entered into by them with the Government. There are various clauses in the Unified Access Services License Agreement ("**UASL**") and the Unified License that regulate monitoring, confidentiality of information and record keeping requirements.[28] The UASL is as an umbrella license agreement, which is applicable to both ISPs and TSPs that were granted licenses prior to 2013, whereas post-2013, the Unified License has been in operation.[29]

Surveillance capacity is also enhanced through government programs such as the Central Monitoring System (**CMS**). Announced via a press release issued in 2009, the CMS is "*a centralized system to monitor communications on mobile phones, landlines and the internet in the country.*" It is designed to facilitate the flow of intercepted communication between TSPs and LEAs on a "near real-time basis" using a secured and dedicated network.[30]

In 2013, provisions of telecom licenses were specifically amended to require TSPs to set up the prescribed infrastructure for their systems to be directly connected with regional monitoring centers (RMCs) of CMS through interception, store and forward servers.[31] In response to a parliamentary question in 2017, the government stated that technology development and pilot trials of CMS had been completed and 18 of the 21 planned RMCs had been

[28] See Vipul Kharbanda, "Policy Paper on Surveillance in India", *The Centre for Internet & Society*, August 2015, available at https://cis-india.org/internet-governance/blog/policy-paper-on-surveillance-in-india.

[29] Global Network Initiative, "India: Legislative Background", available at https://globalnetworkinitiative.org/clfr-india/.

[30] Press Information Bureau, "Centralised System to Monitor Communication", 26 November 2009, available at http://pib.nic.in/newsite/PrintRelease.aspx?relid=54679 and Response by Mr. Ravi Shankar Prasad, Minister of Communications and Information Technology to Lok Sabha UnStarred Question No. 1714, answered on 4 May, 2016. Also see Addison Litton, "The State of Surveillance in India: The Central Monitoring System's Chilling Effect on Self Expression", 14 *Wash. U. Global Stud. L. Rev.* 799, 2015 and Chaitanya Ramachandran, "PUCL v. Union of India Revisited: Why Indias Surveillance Law Must Be Revised for the Digital Age", 7 *NUJS L. Rev.* 105-119 (2014).

[31] Amendment to Condition 41.16 of the UASL, 11 October 2013, available at http://dot.gov.in/sites/default/files/DOC231013-005.pdf?download=1; Amendment to Condition No. 8.2 of Part II of the Unified License Agreement, 11 October 2013, available at http://dot.gov.in/sites/default/files/DOC231013.pdf?download=1; and Amendment to the Cellular Mobile Telephony Services (CMTS) License Agreement, 11 October 2013, available at http://dot.gov.in/sites/default/files/DOC231013-006.pdf?download=1.

technically commissioned.[32]

The telecom license agreements also contain certain restrictions relating to the encryption standards that may be adopted by TSPs. Crucially, Clause 37.1 of the Unified License Agreement, Clause 39.1 of the UASL and Part 1, Clause 2.2(vii) of the Internet Service Provider (**ISP**) License Agreement, all prohibit bulk encryption by TSPs. In addition, the ISP License Agreement[33] also requires that ISP must obtain prior governmental approval to deploy encryption standards that are higher than 40 bits. Setting out such low encryption standards, can make it easier for LEAs to access the target information but it also exposes all users to other security threats. [34] The Telecom Regulatory Authority of India (TRAI) has noted that the encryption standards in the telecom sector are significantly lower than those adopted in other regulated areas like Internet trading; Internet banking; and Aadhaar related transactions. This prompted the telecom regulator to make recommendations to the Government to amend the telecom licenses to bring their encryption standards at par with other sectors.[35]

With the increased adoption of encrypted software and devices, search and surveillance activities often rely on decryption requests for seeking access to the encrypted materials. Under Section 69 of the IT Act, the Government can order the decryption of a computer resource under certain specified conditions. Further, Section 84A of the law authorises the Central Government to frame rules for prescribing encryption standards and methods to secure electronic communications. A draft national encryption policy was released by the Government in September 2015. The draft policy *inter alia* required that users should be able to "*reproduce the same plain text and encrypted text pairs using the software/hardware used to produce the encrypted text from the given plain text*" "on demand." This plain text information was required to be stored for 90 days from the date of transaction and made available to LEAs "as and when demanded in line with the provisions of the laws of the country". The draft policy was retracted shortly afterwards by

[32]Response by Mr. Manoj Sinha, Minister of State, Ministry of Communications to Rajya Sabha UnStarred Question No. 3411, answered on 31 March, 2017.

[33]Part 1, Clause 2.2(vii), ISP License Agreement, available at http://dot.gov.in/sites/default/files/internet-licence-dated%2016-10-2007_0.pdf.

[34]See Vrinda Bhandari, Smriti Parsheera, and Faiza Rahman, "India's communication surveillance through the Puttaswamy lens", 18 May 2018, available at https://ajayshahblog.blogspot.com/2018/05/indias-communication-surveillance.html.

[35]TRAI, Recommendations on Privacy, Security and Ownership of the Data in the Telecom Sector, 16 July, 2018, available at https://www.trai.gov.in/sites/default/files/RecommendationDataPrivacy16072018.pdf.

the Government.[36]

3 Applying the *Puttaswamy* tests to existing practices

In August 2017, nine judges of the Supreme Court in *Puttaswamy* unanimously affirmed the fundamental right to privacy as an integral part of Article 21 and other Part III rights. As stated earlier, it also clarified that, like any other fundamental right, the right to privacy is also not absolute and the State may have an interest in placing reasonable restrictions on this right in pursuance of legitimate aims such as protecting national security, preventing and investigating crime, encouraging innovation, and preventing the dissipation of social welfare benefits. Apart from indicating the broad parameters for restrictions to the right to privacy, all the judges agreed that any restriction of the right to privacy must meet the test under Article 21 of the Constitution, i.e it must be just, fair and reasonable. Further, a majority of the judges (Chandrachud J. speaking for 4 judges and Kaul J. in his separate concurrence) endorsed the use of the following tests (similar to those used by the European Court of Human Rights) to gauge the constitutionality of restrictions on right to privacy: legality, legitimate goal, proportionality and procedural guarantees.

In this section, we discuss the extent to which India's current communication surveillance practices are likely to withstand scrutiny under the tests identified by the judges in the *Puttaswamy* case.

- **Legality:** The requirement of legality demands that the restriction of the right to privacy must have its basis in law.

  In light of this principle, we note that the central and state governments do have the statutory authority to order lawful interception activities under the aforementioned provisions of the Telegraph Act, the IT Act and the rules under them. However, the principle of legality needs to be seen from a broader perspective – it is not just about the existence

[36] See Department of Electronics and Information Technology "Draft National Encryption Policy" (2015), available at https://netzpolitik.org/wp-upload/draft-Encryption-Policyv1.pdf for the draft policy and Press Information Bureau, "Encryption Policy of the Government", 22 September 2015, available at http://pib.nic.in/newsite/PrintRelease.aspx?relid=127106 for the press release withdrawing the policy.

of a law, but also the context in which that legality was conferred.[37]

India's legal regime on surveillance came into existence at a time when bulk surveillance was not easily possible and the discourse around privacy and surveillance was not as well developed as today. The capability of interception technologies and data analytics tools at the disposal of government agencies, and the volume of interceptions being carried out have undergone a massive change in the intervening years. This merits a re-examination of the existing legal framework.[38]

As per the Working Draft of the Legal Instrument on Government-led Surveillance and Privacy prepared by UN Special Rapporteur, Joseph Cannataci, in order to meet the standards of legality, the law should be publicly available, sufficiently clear and precise so as to enable a person to foresee its application.[39] It should also provide for explicit authorisation of specific agencies to carry out surveillance in specific situations and to meet specific ends.[40]

Applying this criteria to a programme like the CMS reveals that even through the provisions on lawful interception have a legislative basis, the specific design of CMS or the exact procedure to be followed under it is not codified in any legal instrument.

As stated earlier, CMS was launched through a press release in 2009[41] and it only finds mention in the terms of the telecom licenses, which are contractual arrangements between the government and TSPs. Accordingly, no specific parliamentary approval has been sought for its

[37]The Necessary & Proportionate principles, which were also referred to by Nariman J. in *Puttaswamy*, highlight that in this age of rapid technological changes, legality vis-a-vis communication surveillance would require laws that restrict the right to privacy to be subject to periodic review through a consultative legislative or regulatory process. See, The Necessary and Proportionate Coalition, "The Necessary & Proportionate International Principles on the Application of Human Rights Law to Communications Surveillance"(May 2014), available at https://necessaryandproportionate.org/principles.

[38]Bhandari *et al*, *supra* note 34.

[39]According to the European Court of Human Rights, the principle of forseeability requires the law to be drafted with sufficient precision to enable the individual to anticipate the consequences of a given action and to regulate their conduct accordingly. See European Court of Human Rights,*Sanoma Uitgevers BV v. Netherlands [2010] App. no. 38224/03 [81]*.

[40]Joseph Cannataci, "Working Draft Legal Instrument on Government-led Surveillance and Privacy", 2018, available at https://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2018AnnualReportAppendix7.pdf.

[41]Press Information Bureau, *supra* note 30.

implementation.[42]

- **Legitimate goal:** Chandrachud J. held that apart from being sanctioned by a law, any interference with privacy rights must also pursue a legitimate state aim. He illustrated this by specifically noting goals such as national security and the prevention and investigation of crimes. Therefore, any order for interception of communications or decryption would satisfy the requirements of legitimate aim so long as it is issued in pursuance of legitimate objectives specified under the Telegraph Act and IT Act. However, it is harder to make this claim in case of something like the restrictions imposed by telecom licenses on the adoption of encryption standards by TSPs and ISPs. Arguably, lower encryption standards threaten the overall security of the network (in addition to interfering with the right to privacy of users) and such blanket restrictions are unlikely to achieve even the generally legitimate aim of protecting national security.

- **Proportionality:** The third test requires that the means being adopted (in the interference with privacy rights) should be proportionate and suitable to achieving the identified aim. In the context of communication surveillance, this would require the authority ordering interception to weigh the degree of interference caused by the proposed intrusion against its anticipated gain, and ensure that the interference is narrowly tailored and that the measure is effectively conducive to achieving the legitimate objective.[43] Further, in *Puttaswamy*, Kaul J. held that the proportionality test also encapsulates within itself the principle of necessity, which requires that interception of communication should take place only when it is the least restrictive way of achieving the legitimate purpose. For instance, Rule 419A(3) of the Telegraph Rules adopts the necessity principle by stating that relevant officer should issue an interception order only when it is not possible to acquire the information by any other reasonable means.

  It is important to note that the Supreme Court in *PUCL* was not considering the issue of bulk surveillance, since that it not envisaged under Section 5 of the Telegraph Act.[44] However, after *Puttaswamy* has put

[42]Human Rights Watch, "India: New Monitoring System Threatens Rights", 7 June 2013, available at https://www.hrw.org/news/2013/06/07/india-new-monitoring-system-threatens-rights.

[43]See Jan Oster, Media Freedom as a Fundamental Right, Cambridge University Press (2015).

[44]See Gautam Bhatia, "State surveillance and the right to privacy in India: A constitutional biography", *26 Natl L. School of India Rev, 128-158 (2014).*

forth the proportionality doctrine as the standard to test restrictions of the right to privacy, it becomes all the more important to discuss issues of bulk or mass surveillance, which would indeed be a disproportionate infringement on the right to privacy and thus not pass constitutional muster. As noted by the UN Special Rapporteur on human rights and countering terrorism, bulk access to communications is incompatible with the normative understanding of privacy as the "*very essence of the right to the privacy of communication is that infringements must be exceptional, and justified on a case-by-case basis*".[45] Any form of bulk surveillance essentially reduces everyone to a suspect in the eyes of the law, therefore reshaping the behaviour of individuals.

Extending the same principle to the framework for decryption on demand, we note that while ordering decryption of a particular computer resource, based on evidence of suspicion, can qualify as targeted access, requiring private companies to create backdoors within all systems clearly would not. Such a requirement would render computer resources of several unsuspected individuals vulnerable to access by government and hackers alike.[46]

Security experts note that creating such backdoors for LEAs lead to three concerns. First, it would amount to taking a U-turn from the best practices depoloyed to ensure Internet security including the practice of "forward secrecy" – where decryption keys are deleted immediately after use. Second, it will increase system complexity considerably as almost every new feature has the potential to interact with others to create more vulnerabilities. Third, security credentials that unlock the data would have to be held either by the platform providers, LEAs, or a trusted third party. This will create concentrated targets that may attract bad actors.[47]

Therefore, ordering entities to create backdoors in their systems would not qualify as the least restrictive way of achieving a legitimate aim. To

[45]Report of the UN Special Rapporteur on human rights and countering terrorism (2014), available at https://www.justsecurity.org/wp-content/uploads/2014/10/EmmersonReportMassSurveillance.pdf.

[46]Robby Mooke, "Encryption keeps us safe. It must not be compromised with backdoors", *The Guardian*, 12 February, 2018, available at https://www.theguardian.com/commentisfree/2018/feb/12/encryption-safe-hillary-clinton-secure-backdoors-privacy.

[47]Abelson et al.,"Keys Under Doormats: Mandating insecurity by requiring government access to all data and communication",*MIT-CSAIL-TR-2015-026*, available at https://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf.

the contrary, this would increase system complexity and create concentrated targets that may attract bad actors. Such broad-based measures are therefore unsuitable, even if the underlying purpose may qualify as a legitimate aim, and they would not satisfy the proportionality standard.

- **Procedural guarantees**: Kaul J. adds a fourth test of procedural guarantees which requires the presence of procedural safeguards within the interception framework to check against the abuse of state interference.

  As stated earlier, Rule 419A of the Telegraph Rules and the 2009 IT rules set out certain procedural safeguards to govern the interception of communications. The procedural requirements under both these rules are very similar.

  While these rules are in accordance with Supreme Court's decision in the *PUCL* case, significant time has lapsed since that verdict and both the scope and the volume of surveillance activities has increased. Over the last few years, the government has launched surveillance programmes such as the CMS, Network Traffic Analysis System (NETRA),[48] National Intelligence Grid (NATGRID)[49] and has made corresponding changes to telecom licenses to provide "near real-time" access to the traffic flowing through TSP networks. Even without taking into account these developments, we find that the current procedure would not constitute a "fair, just and reasonable" process on the following counts:

  – Rule 419A and the 2009 IT rules authorise members of the executive – the Secretary to the Ministry of Home Affairs in the case of central government and the Secretary of the Home Department in the case of a state government (or in unavoidable

[48]NETRA is a surveillance software designed to perform real time analysis of Internet traffic based on pre-defined keywords. See Livemint, "India to deploy Internet spy system Netra", January 6 2014, available at https://www.livemint.com/Politics/To4wvOZX7RmLM4VqtBshCM/India-to-deploy-Internet-spy-system-Netra.html.

[49]The NATGRID is an integrated intelligence grid that connects the databases of several government entities in order to collect data, detect patterns and provide real time (sometimes even predictive) analysis of data gathered by LEAs and, military agencies. The programme intends to provide 11 security agencies real-time access to 21 citizen data sources to track terror activities across the country. See Centre for Internet and Society, "The Design & Technology behind Indias Surveillance Programmes", available at https://cis-india.org/internet-governance/blog/the-design-technology-behind-india2019s-surveillance-programmes.

circumstances, a Joint Secretary) – to sanction orders of interception. As per a right to information response sought by SFLC, an average of 7500 - 9000 telephone-interception orders are issued by the central government each month.[50] Add to this the orders for data interception issued under the IT Act and orders issued by the state governments and the total figure is expected to be much higher.[51] Taking into account this volume of orders being issued by the government on a regular basis, it is difficult to ensure due application of mind to each and every request placed before the officers in charge of this function.

- The rules mentioned above also set up a Review Committee to check if interception orders were issued in accordance with the law. This committee comprises only of members from the executive such as the Cabinet/Chief Secretary along with Secretaries in charge of legal affairs and telecommunications. There is a conflict of interest in this review mechanism, as both the interception order issuing authority and the oversight authority comprise of members only from the executive.[52]
- There is no pre- or post-judicial oversight over the decision to place an individual under surveillance.[53]

The lack of independent judicial oversight has already been pointed out as an issue in the context of interception under the Telegraph Act and IT Act earlier in this paper. This issue is further compounded in case of CMS which has been criticised widely for its all-encompassing

[50] SFLC, *supra* note 7.

[51] Information revealed under Google's transparency report offers another indication of the volume of requests made by Indian authorities – in 2017 Google received 8,351 user data disclosure requests from India, affecting about 14,932 user accounts. See Google's transparency report, available at https://transparencyreport.google.com/user-data/overview?user_requests_report_period=authority:IN.

[52] It is pertinent to note that while the present framework of review flows from the Supreme Court decision in *PUCL*, the judgement was delivered by a smaller bench of two judges and the stricter requirements under the proportionality standard flow from the nine judge bench decision of the Court in Puttaswamy.

[53] It is critical to highlight that the Supreme Court in *PUCL* noted that "*in the absence of any provision in the statute, it is not possible to provide for prior judicial scrutiny as a procedural safeguard.*" However, given *Puttaswamy's* emphasis on the necessary and proportionality test, the need for procedural safeguards, and its endorsement of the Necessary and Proportionate Principles regarding communication surveillance, the question of whether *PUCL* requires reconsideration post *Puttaswamy* is open.

nature, privacy threats and likely chilling effect.[54]

4 International experience

The Snowden revelations in 2013 marked a watershed moment in the matter of state surveillance. The scale, extent, and ubiquity of signals intelligence[55] gathering demonstrated by this episode, led to global awareness about the need to adapt both national and international laws and practices to the modern communication era. This became a pivotal moment for surveillance reform as numerous countries began to revisit their surveillance related laws, with a particular focus on ensuring (a) a higher standard of care for communications data of citizens; and (b) strengthening the powers of intelligence agencies, particularly on issues of foreign surveillance, while also creating more robust mechanisms for oversight over their actions.

That said, the fact that most jurisdictions do not yet have human rights compatible surveillance mechanisms has been made clear by the UN Special Rapporteur on the Right to Privacy, Joseph Cannataci, who informed the UN Human Rights Council earlier this year that *"Unfortunately, there is no one piece of national surveillance legislation which perfectly complies with and respects the right to privacy"*.[56] The Special Rapporteur has also presented a draft text for a legal instrument on government led surveillance and privacy, which echoed the principles of legality and proportionality that have been previously discussed.[57]

[54] Addison Litton, "The State of Surveillance in India: The Central Monitoring System's Chilling Effect on Self Expression", *14 Wash. U. Global Stud. L. Rev. 799, 2015*,available at https://bit.ly/2AeDKh6.

[55] 'Signals intelligence' refers to the gathering of intelligence through the interception of signals. In the US, the primary body tasked with collection of foreign signals intelligence is the National Security Agency. See NSA "Signals Intelligence", available at https://www.nsa.gov/what-we-do/signals-intelligence/

[56] United Nations Human Rights Office of the Commissioner, "Urgent action needed to protect privacy in cyberspace, UN rights expert warns", available at https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=22762&LangID=E.

[57] Cannataci, *supra* note 40. Note also that the principles of legality and proportionality are a core component of the International Principles on the Application of Human Rights to Communication Surveillance (the Necessary and Proportionate principles), which have been endorsed by over 600 organisations from around the world. See International Principles on the Application of Human Rights to Communication Surveillance, available at https://necessaryandproportionate.org/.

4.1 Practice in other jurisdictions

This section summarises the law and practices relating to surveillance and interception, as seen in other jurisdictions. It focuses mainly on the procedural safeguards and oversight mechanisms adopted in countries like the USA, Germany and the UK to protect the right to privacy of individuals, while authorising intelligence agencies and LEAs to carry out legitimate surveillance practices.

The general practice across jurisdictions is that privacy and data protection laws are also applicable to state intelligence and security agencies, subject to various exceptions.[58] These exceptions are generally designed to ensure that information pertaining to live investigations, confidential material, etc., is not made public so as to vitiate the purpose of gathering intelligence. For instance, the Privacy Act, 1974 in the US, which is applicable to the federal public sector, is also applicable to the military and LEAs. The law, *inter alia*, requires the disclosure of the types of databases maintained by an agency and the intended uses of the system, recognises the rights to access and modify records, contains data minimisation requirements and rules for disclosure of information, creates penalties (both civil and criminal) for violations, and establishes independent oversight mechanisms. While exempting the LEAs from certain obligations, the law imposes mandatory provisions, notably concerning disclosure of information, publication on the nature and character of information retained, adherence to fair information principles and establishment of safeguards to protect personal information.[59]

Similarly, the UK's Data Protection Act, 2018, contains a separate chapter for processing by LEAs. Part 3 of the statute contains similar privacy protections as to 'normal' processing, but applied to a law enforcement context, implying that certain rights are necessarily limited.[60]

The UK Investigatory Powers Act, 2016, which is applicable to intelligence

[58] International Conference of Data Protection & Privacy Commissioners, Counting on Commissioners: High level results of the ICDPPC Census 2017, September, 2017, available at https://icdppc.org/wp-content/uploads/2017/09/ICDPPC-Census-Report-1.pdf. Of the 74 jurisdictions covered in the study 55 countries provided a partial exemption for intelligence and security agencies while 19 contained a complete exemption.

[59] Electronic Privacy Information Centre, "The Privacy Act of 1974", available at https://www.epic.org/privacy/1974act/.

[60] For instance, an individual's right to access can be limited to the extent it is a necessary and proportionate measure to protect national security, protect public security, avoid obstructing a legal inquiry or investigation, etc. See "Data Protection Act, 2018," available at http://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpga_20180012_en.pdf.

agencies also contains similar principles, for instance, requiring data gathering to be necessary and proportionate and for data not to be retained for longer than necessary.[61]

The referenced countries have also prescribed procedures for the maintenance and disposal of records (or principles related thereto). For example, in the US, the Law Enforcement Records Retention Schedule prepared by the Secretary of State has prescribed specific retention schedules for data of different types collected by LEAs, as well as methods for archiving and destruction of such information.[62]

4.2 Judicial oversight

Having an independent approval and oversight mechanism for the conduct of surveillance activities by intelligence agencies and LEAs is one of the basic requirements of a balanced surveillance framework. The oversight mechanisms adopted for this purpose often require prior judicial approval to authorise the surveillance, which is considered to be an essential requirement by many privacy advocates.[63]

To take a few examples, Canada has a system of specially designated judges in the Federal Court to approve warrants requested by the Canadian Security Intelligence Service (CSIS).[64] In Australia, warrants are required to access content of messages in transit and in storage, while access to metadata relating to use of communications services does not require a warrant.[65] The US also requires intelligence and law enforcement agencies to obtain warrants, subpoenas and other court orders in order to conduct domestic surveillance activities.[66]

[61] See for instance, Sections 87 and 150 of the Investigatory Powers Act, 2016, pertaining to data retention by intelligence agencies.

[62] Office of the Secretary of State, "Law Enforcement Records Retention Schedule Version 7.2", January 2017, available at https://www.sos.wa.gov/_assets/archives/recordsmanagement/law-enforcement-records-retention-schedule-v.7.2-(january-2017).pdf.

[63] Necessary and Proportionate, "Global Legal Analysis", https://necessaryandproportionate.org/global-legal-analysis.

[64] Part II of the Canadian Security Intelligence Service Act, 1985 deals with "judicial control" on the procedures for application for warrant.

[65] Part 2-2 and 2-5 of the Australian Telecommunications (Interception and Access) Act, 1979.

[66] See Sections 2516-2518 of the Electronic Communication Privacy Act of 1986, 18 USC 2510-22.

Foreign intelligence gathering in the US is governed by the Foreign Intelligence Surveillance Act, which has created special courts for granting orders to conduct foreign intelligence investigations.[67] Similarly, New Zealand has also drawn a distinction in the approval process for its own citizens and residents and foreign subjects. In case of the former, a Commissioner of Intelligence Warrants, who must be a former High Court judge, has joint responsibility with the authorising minister to issue the warrants, while in the latter case the authority lies solely with the authorising minister.[68]

Some countries have also drawn a distinction in the approval processes applicable to intelligence agencies and general LEAs. In Germany, the G-10 Commission, consisting of four members appointed by the German Federal Parliament, is responsible for approving surveillance measures by intelligence agencies. LEAs, on the other hand, require court orders to intercept communications although in cases of imminent danger the interception of communications may be also ordered by the public prosecutor's office. Such administrative interception orders expire within three days unless they are confirmed by a court.[69]

Similar to the current laws in India, the Regulation of Investigatory Powers Act, 2000 in UK also authorised the Secretary of State to issue warrants of interception based on requests made by intelligence agencies. As a result, a majority of the surveillance decisions were made without either prior judicial authorisation or effective judicial oversight on an ex post facto basis.[70] The UK has since moved away from this system by enacting the Investigatory Powers Act, 2016 (IPA), which created the Investigatory Powers Commissioner's Office. The IPA has strengthen the approval process under the old law by introducing a "double lock" system under which the warrant issued by the Secretary of State is also subject to review by a Judicial Commissioner (part of the IPC's office) before it comes into effect.[71]

[67] Foreign Intelligence Surveillance Act, 1978, 50 USC 1803-1805.

[68] See Sections 52-84 and Sections 112-117 of the New Zealand Intelligence and Security Act, 2017.

[69] Sec. 100b para. 1 of the German Code of Criminal Procedure.

[70] Global Legal Analysis, *supra* note 63.

[71] See Sections 19 and 23 of the Investigatory Powers Act, 2016 and Investigatory Powers Commissioner's Office, "What we do", available at https://ipco.org.uk/default.aspx.

4.3 Reporting and transparency

The absence of transparency concerning surveillance activities prevents meaningful oversight of the actions of executive agencies,[72] and it militates against the system of checks and balances inherent in India's constitutional make-up. Democracy entails permitting citizens, whether through their representatives or otherwise, to assess whether surveillance techniques are being used appropriately and in accordance with prescribed norms.[73]

This implies that no surveillance should be carried out without some form of transparency sufficient to enable a check on whether principles of necessity, proportionality and adherence to due process (as required by *Puttaswamy*), are being followed by the LEAs. While certain information about surveillance systems may need to remain secret from the common man, this should not in itself lead to the unaccountable use of power in any circumstances.

Transparency and reporting requirements may be broadly segregated, based on the LEA or type of information concerned, into five categories:

- **Information provided directly to the public**: For instance, access requests fulfilled by LEAs under data protection laws[74] or aggregated statistics published suo moto or permitted to be published by telecom and other service providers.[75]
- **Information provided to institutions of democratic control**: Such bodies usually have a free hand in so far as their oversight role is concerned. For instance, the US Congress and its committees have complete authority over all federal LEAs and intelligence services, with no statutory bars on what information they can access.[76] Similarly, the Germany parliament contains a panel known as the *Kontrollgremiumgesetz*, which is required to *inter alia* be informed of the general activities of intelligence agencies as well as events of particular importance. The reporting requirements are not restricted to post facto

[72] Global Legal Analysis, *supra* note 63.

[73] *Id.*

[74] As discussed previously, these requirements may have limitations compared to access requests made to normal data controllers.

[75] For instance, many major technology companies such as Google and Facebook, etc., publish aggregated statistics as part of their transparency procedures. Reporting is however subject to statutory requirements and court orders.

[76] Cat Barker et al, "Oversight of intelligence agencies: a comparison of the Five Eyes nations", Parliament of Australia, 2017, available at https://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/rp/rp1718/OversightIntelligenceAgencies.

reports and the panel has complete access to files and documents of intelligence services. The panel may also compel the government to produce any relevant information it may wish to examine.[77] LEAs are also answerable to the executive. Notably, the Federal Intelligence Services Act requires mandatory reporting by intelligence agencies to the Federal Chancellery.[78]

The UK utilises an independant parliamentary authority, the Intelligence and Security Committee, which operates under a memorandum of understanding signed with the Prime Minister. The Committee produces an annual report as well as reports on specific investigations (it may also submit secret reports to the Prime Minister).[79]

- **Independent regulators**: These may range from data protection authorities (as in Germany and the UK, though their mandate may be limited when it comes to LEA and intelligence agencies) to specific statutory authorities tasked with overview of LEAs/intelligence agencies. To take a few examples, the UK empowers the Office of the Investigatory Powers Commissioner to review, audit, inspect and investigate activities of all LEAs and intelligence agencies.[80] The US, has in place the President's Intelligence Advisory Board and the Privacy and Civil Liberties Oversight Board[81] (as well as independant commissions appointed by congress) to ensure intelligence agencies adhere to constitutional norms, while in Germany, specific authorities are tasked with overview of intelligence agencies (for instance, the G-10 Commission mentioned previously).[82]

[77] See the German Control Panel Act of 2009 (Law on the parliamentary control of Federal intelligence service (*Kontrollgremiumgesetz*).

[78] Jenny Gesley, "Foreign Intelligence Gathering Laws: Germany", Library of Congress, September 27, 2016, available at https://www.loc.gov/law/help/intelligence-activities/germany.php.

[79] Intelligence and Security Committee of Parliament, "About the Committee", available at http://isc.independent.gov.uk/, and Sections 2, 3, and Schedule I of the Justice and Security Act, 2013.

[80] See Sections 227 and 229 of the Investigatory Powers Act, 2016, and Investigatory Powers Commissioner's Office, "What we do", August 30, 2017, available at https://www.ipco.org.uk/.

[81] The Privacy and Civil Liberties Oversight Board, "History and Mission", available at https://www.pclob.gov/about/ and the White House of Barack Obama, "President's Intelligence Advisory Board and Intelligence Oversight Board", available at https://obamawhitehouse.archives.gov/administration/eop/piab.

[82] Bundesnachrichtendienst "G10 Commission", available at http://www.bnd.bund.de/EN/Scope_of_Work/Supervision_and_Control/G10_Commission/G10_Commission_node.html.

- **Executive/administrative authorities**: Countries often have multiple layers of executive and administrative oversight for both LEAs and intelligence services. In Germany, the Federal Intelligence Services Act requires mandatory reporting by intelligence agencies to the Federal Chancellery, while Section 100b of the Criminal Code requires mandatory reporting by LEAs to submit annual reports to the Federal Office of Justice.[83]

  In the US, intelligence activities are overseen by Inspector Generals, who are answerable directly to Congress. These officials are empowered to *inter alia* audit, investigate, and review the practices of specific federal LEAs, while the Office of the Inspector General of the Intelligence Community (IGIC) has cross agency jurisdiction. The Office of the Federal Director of National Intelligence (which falls under the IGIC) also contains a separate office of Civil Liberties, Privacy and Transparency.[84]

- **Judicial authorities**: As discussed in the previous section, most countries have in place judicial oversight mechanisms - which may therefore involve public scrutiny (though such scrutiny is usually restricted to LEAs and does not extend to intelligence agencies).[85]

Importantly, these bodies are able to: (a) scrutinise in some detail, the workings of the LEAs and intelligence agencies (thereby ensuring an application of mind and an adherence to privacy norms), and (b) ensure a measure of public accountability over not just the LEAs/intelligence agencies, but also their own monitoring activities. To illustrate, Section 100b of the German Code of Criminal Procedure requires the Federal Office of Justice to publish reports indicating the number of surveillance proceedings (by LEAs), number

[83]Bundesnachrichtendienst, "Federal Intelligence Service Act", available at http://www.bnd.bund.de/EN/Scope_of_Work/Supervision_and_Control/Federal_Intelligence_Service_Act/Federal_Intelligence_Service_Act_node.html and the Germany Code of Criminal Procedure, 1987, available at https://www.gesetze-im-internet.de/englisch_stpo/englisch_stpo.html.

[84]Office of the Director of National Intelligence, "Office of the Intelligence Community Inspector General - What we do", https://www.dni.gov/index.php/who-we-are/organizations/ic-ig/ic-ig-what-we-do and Wendy Ginsberg and Michael Greene, "Federal Inspectors General: History, Characteristics, and Recent Congressional Actions", Congressional Research Service, December 8, 2014, https://bit.ly/2KmTj7g.

[85]By way of example, proceedings of the American FISA Court are generally kept secret, though the matter is currently under legal challenge. Niki Anderson and Lorenzo Arvantis, "Law clinic pushes for FISA Court transparency", Yale Daily News, February 27, 2018, https://yaledailynews.com/blog/2018/02/27/law-clinic-pushes-for-fisa-court-transparency/.

of initial and follow up orders, types of communication which are surveilled, etc. Similarly, the German *Kontrollgremiumgesetz* produces annual reports detailing both its and the activities of intelligence agencies.

Separately, ensuring transparency and accountability of LEAs/intelligence agencies may also necessitate a review of various other laws that implicate privacy and data protection - for instance laws pertaining to whistleblower protection, right to information and access to confidential documents / official secrets.[86]

Given the need to ensure that those within LEAs who expose illegalities or divergences from due process are adequately protected, it may not be prudent to grant general exemptions to matters related to sovereignty or strategic interests of the state, etc, in whistleblower related laws. It may in fact be appropriate to create separate mechanisms for whistleblowing in such contexts.[87] Similar nuanced exemptions should also be crafted in right to information laws. This is the extant practice in countries such as Germany, UK and US, where the relevant freedom of information laws do not provide for blanket exemptions for LEAs. The sensitive nature of much of the material dealt with by these entities does however imply that exceptions and exclusions are in place to ensure no active investigations or security assets are impacted.[88]

[86]The US permits citizens to request review of specific documents for declassification and release under Executive Orders 13526.

[87]For instance, the US has implemented separate whistleblower protections for intelligence agency related whistleblowing so as to ensure protection from the normal federal agencies under Presidential Policy Directive 19 and Intelligence Community Directive 120. These procedures ensure a measure of confidentiality even in disclosure of the information and enhance protection for the whistleblower. See General of National Intelligence, "What are my IC protections", https://www.dni.gov/ICIG-Whistleblower/protected.html.

[88]The UK's Freedom of Information Act, 2000, which is applicable to LEAs and armed forces but not intelligence agencies, contains 23 exemptions. Section 30 exempts certain information from disclosure if used in connection with investigation of offences by public authorities, while Section 31 contains specific exemptions for law enforcement purposes and limits the disclosure of information that could prejudice detection of a crime, apprehension or prosecution of offenders, operation of immigration controls, maintainance of order in prisons, etc. Germany's Federal Act Governing Access to Information Held by the Federal Government, 2005, (*Informationsfreiheitsgesetz*) applies to LEAs but bars disclosure of information where it may have detrimental effects on international relations, military and other security interests of the armed forces, internal or external security interests, etc.; the American Freedom of Information Act, 1967, also does not contain blanket exceptions for LEAs.

4.4 Other organisational safeguards

The US, Germany and the UK have also implemented various administrative and technical safeguards to ensure adherence to privacy norms. Notably, all these countries require LEAs and intelligence agencies to have in place privacy and/or ethics officers to ensure respect for civil liberties in the day to day conduct of activities. For instance, the CIA's Office of Privacy and Civil Liberties (OPCL) provides privacy and civil liberties guidance and training to officials. Similar offices exist for agencies such as the NSA and FBI.[89]

In the UK, LEAs contain independent officials within the organisations who are tasked with scrutinising all surveillance requests to ensure the action is necessary and proportionate and that no less intrusive means can be adopted to achieve the same ends. These authorisations are available for scrutiny by the judicial commissioners appointed under the Regulation of Investigatory Powers Act, 2016.[90]

Intelligence agencies may also be required to implement various technical and legal measures to ensure citizens are not caught up in bulk surveillance of foreign intelligence. To illustrate, certain procedures such as masking techniques can be used to ensure that domestic citizens are not caught up in surveillance of foreigners.[91]

4.5 Notice to the data subject

A common view on surveillance has been that the very nature and logic of secret surveillance implies that it has to be conducted without the knowledge of the concerned individual and therefore sufficient protections and guarantees to safeguard the individual's rights need to be built in through other mech-

[89] Central Intelligence Agency, "Privacy and Civil Liberties at CIA", January 18, 2017, available at https://www.cia.gov/about-cia/privacy-and-civil-liberties; Office of the Director of National Intelligence, Office of Civil Liberties, Privacy and Transparency, "Protecting US Person Identities in Disseminations under the Foreign Intelligence Services Act", November 2017, available at https://bit.ly/2KpkBKb.

[90] MI5 Security Service, "Law and Governance", available at https://www.mi5.gov.uk/law-and-governance.

[91] Rebecca J Richards, "Review of US Person Privacy Protections in the Production and Dissemination of Serialised Intelligence Reports Derived from Signals Intelligence Acquired Pursuant to Title I and Section 702 of the Foreign Intelligence Surveillance Act", NSA Civil Liberties and Privacy Office, October 11, 2017, available at https://www.nsa.gov/about/civil-liberties/reports/assets/files/20171011-nsa-clpo-dissemination-report.pdf.

anisms.[92] There are, however, several jurisdictions that make it mandatory to provide notice of surveillance to the data subject, particularly if criminal proceedings are to be initiated based on the collected information. In Canada, for instance, the Criminal Code provides that if the interception relates to an offence for which proceedings may be commenced by the Attorney General of Canada, the person is entitled to receive written notice of the interception within 90 days. The period of 90 days may be extended under specified circumstances.[93] In 2011, the Belgium Constitutional Court found a provision which stated that a person, who has been subjected to a secret intelligence method like tapping or secret house searches, is only informed afterwards 'on request', to be contrary to the human rights enshrined in the Belgian Constitution and the European Convention on Human Rights. The court held that "*By not notifying the citizens, every possibility to effective supervision and subsequent legality control would be excluded.*"[94]

The law in Germany also requires that the affected data subjects should be notified after completion of surveillance measures authorised by the G-10 Commission. Such notification is not required in circumstances where it would endanger the purpose of surveillance or create a disadvantage for Germany or one of its federal states. Similar provisions are also applicable to surveillance measures undertaken by LEAs. Austria also requires that data subjects have to be notified in case they have been the subject of lawful interception.[95]

In a challenge relating to the Bulgarian Special Surveillance Means Act, the European Court of Human Rights held that "*as soon as notification can be made without jeopardising the purpose of the surveillance after its termination, information should be provided to the persons concerned*".[96] The Court, however, stopped short of finding that notification was a necessary requirement of surveillance laws in general.[97]

[92] *Klass v. Germany*, A 28 (1978), 2 EHRR 214.

[93] Criminal Code RSC 1985, c.C-46, Part VI, Section 196.

[94] *Belgium Constitutional Court*, Case No. 145/2011, 22 September 2011. See Paul De Hert and Fraziska Boehm, "The Rights of Notification after Surveillance is over: Ready for Recognition?", Digital Enlightenment Yearbook, 2012, available at http://www.vub.ac.be/LSTS/pub/Dehert/408.pdf.

[95] See Section 139 of the Austrian Criminal Procedure Code.

[96] *Association of European Integration and Human Rights and Ekindzhievv, Bulgaria*, Application No. 62540/00, 28 June 2007.

[97] Global Legal Analysis, *supra* note 63.

4.6 Redress mechanisms

The lack of notice about surveillance activities could imply that the affected persons lack the knowledge required to initiate a challenge against the surveillance proceedings or are unable to establish proper standing before a judicial/ review body. However, a number of jurisdictions have created specialised mechanisms to address these issues. In UK, the Investigatory Powers Tribunal is an independent court constituted under the Regulation of Investigatory Powers Act, 2000 to look into complaints of unlawful intrusion by public bodies, including security and intelligence agencies, the police and local authorities. A complaint can be made to the tribunal by persons who believe that there has been an interference with their privacy rights, their property or communications. The IPA, 2016 has also created a mechanism for preferring an appeal before the Court of Appeal in England and Wales or the Court of Session against any decisions of the tribunal.[98]

On the issue of standing, the ECHR, in *Klass v. Germany*, noted that the applicants could claim to be victims of a violation of Article 8 of ECHR (Right to private life, family life, correspondence and home) without proving that they had been the concrete target of secret surveillance measures.[99] In contrast, the US Supreme Court in *Clapper v. Amnesty International*[100] rejected a claim by a group of attorneys and human rights, labor, legal, and media organisations on the ground that their claim was too speculative since they as the plaintiffs could not prove that the government had or would ever target someone with whom the plaintiffs regularly communicated.[101]

In many cases even though the data subject may not be able to directly challenge the interception request, laws allow the entity receiving such request (such as telecom service providers or other intermediaries) to question the validity and scope of the request. Section 702 of the Foreign Intelligence Surveillance Act in the US, for instance, provides that an electronic communication service provider that receives a directive to provide any assistance or information to the Government may file a petition before the Foreign Intelligence Surveillance Court to modify or set aside such directive. In the case of

[98] Section 67A, IPA, 2016.

[99] Paul De Hert and Fraziska Boehm, "The Rights of Notification after Surveillance is over: Ready for Recognition?", Digital Enlightenment Yearbook, 2012, available at http://www.vub.ac.be/LSTS/pub/Dehert/408.pdf.

[100] 568 U.S. 398 (2013).

[101] "Standing, Surveillance, and Technology Companies", 131 Harv. L. Rev. 1742, available at https://harvardlawreview.org/2018/04/standing-surveillance-and-technology-companies/.

In re Directives to Yahoo! Inc.,[102] the US Foreign Intelligence Surveillance Court of Review allowed Yahoo Inc. to challenge the directions received by it to share information relating to its users on the ground that it was an illegal violation of the Fourth Amendment rights of its users. The case was however decided against Yahoo on its merits.[103]

5 Key design principles for India

On mapping the legal framework and practices on surveillance in India against the *Puttaswamy* tests and globally recognised surveillance principles we find our current framework to be lacking in many respects. The present system is not well suited to meet the requirements of a system that guarantees a constitutional right to privacy or, for that matter, one that faces limited state capacity in carrying out effective surveillance activities. We therefore need a system that is designed in a manner where the resources of the surveillance machinery can be optimally utilised without undue infringements on the right to privacy. Addressing these issues requires both a reassessment of the current legal framework as well as a rethink of the philosophy that drives surveillance related activities by intelligence agencies and LEAs in India.

5.1 A risk-based approach to surveillance

The broad path towards safeguarding civil liberties in a system with limited state capacity lies in adopting a risk-based approach to surveillance. Countries such as the US and the UK have already moved in this direction by embedding certain risk management techniques within their surveillance architecture. This approach essentially recognises that any country's resources are limited and therefore the surveillance architecture should focus on credible risks, whether they be reputational or operational.[104]

Apart from calibrating responses to the risk posed by different kinds of threats, this approach takes into account broader risks such as the risks to privacy and other civil liberties, reduction of international trust in domestic firms and the impacts of intelligence operations on relationships with other

[102] No. 08-01, 2008 WL 10632524 (FISA Ct. Rev. Aug. 22, 2008).

[103] "Standing, Surveillance, and Technology Companies", *supra* note 101.

[104] Hilary Tuttle, "How the NSAs first CRO is integrating risk into security management", Risk Management Magazine, available at https://bit.ly/1lX5aw2.

countries.[105] We recommend that the Indian surveillance framework should also adopt systematic risk management as a key design principle to balance national security and privacy on one hand and limited state capacity issues on the other. The report of the Srikrishna Committee has also endorsed this recommendation of having systematic risk management techniques embedded in the country's surveillance architecture.

5.2 Reassessing the legal framework

India needs to build a strategic plan towards a robust legal framework governing the functioning of intelligence agencies. This requires the creation of a statutory framework governing intelligence agencies and LEAs, including their constitution, composition, powers, accountability measures and the legal processes expected to be followed by them. The report of the Srikrishna Committee recommends that the *"Central Government carefully scrutinise the question of oversight of intelligence gathering and expeditiously bring in a law to this effect"*. It then goes on to state that although these recommendations are not directly made a part of the data protection statute proposed by the Committee, they are important for the effective implementation of data protection principles and must be urgently considered.

While a data protection law would admittedly not be an appropriate site for pursuing a comprehensive reform of intelligence agencies and LEAs, there are several critical changes that can be adopted through the data protection law as well as amendments to existing laws. The surveillance reform agenda can therefore proceed without waiting for the adoption of a comprehensive framework to govern intelligence agencies. We highlight below the specific recommendations that will help to ensure that any intrusion into an individual's right to privacy by state surveillance is in consonance with accepted principles of necessity and proportionality as affirmed by the Hon'ble Supreme Court in the *Puttaswamy* case. This is followed by a discussion on the recommendations of the Srikrishna Committee and extent to which they satisfy the identified objectives.

1. *Prior judicial review* – Present Indian laws confer wide powers on the Government machinery in terms of deciding the need for surveillance in a particular case (by intelligence agencies and LEAs), granting authorisation for surveillance requests (by the Home Secretary in the Central

[105] David Omand, Securing the State (2010); See also David Omand, Securing the State: A Question of Balance, available at https://www.chathamhouse.org/sites/default/files/public/Meetings/Meeting%20Transcripts/080610davidomand.pdf.

and State Governments) and review of the authorisation orders (by a Review Committee consisting of members of the executive). The decision in *Puttaswamy* held that any intrusion by the state in an individual's privacy rights is permissible only if it is supported by a "fair, just and reasonable procedure established by law". Independent review and oversight over the surveillance process by a judicial body must therefore be regarded as prerequisites of a process that seeks to meet these goals. The role of this body would be to apply the principles of necessity and proportionality in each and every case to ensure that the nature of surveillance, its duration and scope is in line with the purpose that is sought to be achieved.

We recommend that the current process of authorisation of surveillance requests by the executive therefore needs to be amended to incorporate an element of prior judicial review (or post-facto judicial scrutiny in cases of emergency). This review may be conducted through specialised courts designated for this purpose or by judicial members of an independent body, such as a Data Protection Authority. In addition, there needs to be a mechanism for filing an appeal against the decision of the judicial body. The adoption of the proposed structure would require corresponding amendments to the Telegraph Act, IT Act and the rules framed under those laws.

2. *Reporting and transparency by LEAs* – We recommend that relevant laws must be enacted/amended to ensure appropriate reporting and transparency requirements are implemented pertaining to all surveillance activities. These requirements may differ depending on the nature of information and the entity to which it is being provided. Reporting must be on both ex-ante and post facto basis, as may be relevant to the circumstances. In any event, no surveillance program must be carried out without some form of transparency sufficient to enable a check on whether principles of necessity, proportionality and adherence to due process (as required by the *Puttaswamy* judgment), are being followed by the intelligence bodies and LEAs. Oversight bodies must also be required to publish periodic reports of their activities and that of LEAs/intelligence agencies under their supervision, while service providers must be permitted to publish aggregated statistics detailing volume and nature of surveillance requests.

3. *Other necessary protections and safeguards* – In addition to the structural redesign of the surveillance architecture and introduction of specific reporting and transparency requirements, we recommend that the

following protections must be built into the data protection law:

- *Implementation of data retention norms, principles of fair processing* – Principles of fair processing must be applicable even to data processed by intelligence bodies/LEAs. They must also ensure that as far as possible, personal data is up to date and accurate, while data retention norms need to be appropriately designed to ensure only relevant data is stored by the authorised agencies.
- *Notice to the data subject* – In order to achieve a balance between the objectives of surveillance and the rights of the data subject, the law should provide for an obligation to ensure that the affected data subjects are notified after completion of the surveillance. However, the agency may seek the approval of the judicial body to delay or avoid the requirement of notice under certain exceptional circumstances, for instance if it can be established that such a disclosure would defeat the purpose of surveillance.
- *Right to seek redress* – The requirement of notice to the data subject must be accompanied by a right to challenge and seek appropriate redress against surveillance activities. This right should extend to a person who is, or has reasonable apprehension of being, the subject of surveillance. In addition, intermediaries that are required by law to facilitate access to information by law enforcement agencies should also have the legal right to question the scope and purpose of the orders received by them.
- *Privacy officers in LEAs* – Independent officials must be appointed to the intelligence agencies and LEAs to scrutinise requests for surveillance (before they are put up to the sanctioning judicial body) and ensure adherence to the law. Such scrutiny must be recorded in writing and available to relevant oversight bodies (if not the public).

4. *Technical measures to enhance privacy* – We recommend that technical measures and privacy by design principles must be used to inform surveillance procedures and assist in maintenance of proportionality and due process. This may imply for instance, the use of masking techniques to protect identities of citizens caught up in bulk surveillance of foreign intelligence, ensuring collected data is encrypted and only accessible pursuant to specific authorisation, etc.
5. *Evidentiary value of information collected in breach of data protection law* – The current position of law in India is that illegality in conducting

search and surveillance activities does not lead to a bar on the use of that evidence in subsequent proceedings. As a result, the incentives of LEAs are not fully aligned with the objective of ensuring that the legal processes governing surveillance are strictly followed, in letter and spirit. This will continue to pose a challenge once we introduce a more robust set of privacy safeguards in the law. We therefore recommend that relevant laws should be amended to bar the admissibility of any information that is obtained by the agencies in breach of the proposed data protection law and other surveillance related laws.

6. *Revisiting telecom licenses* – Telecom licenses contain specific provisions relating to the obligations of TSPs and ISPs to facilitate lawful interception activities. We recommend that to the extent that any of the provisions contained in telecom licenses create additional restrictions on the privacy rights of individuals, these provisions need to adopted through legislative instruments. For instance, the procedures and requirements relating to CMS need to be specifically incorporated in the Telegraph and IT Act and rules under them to provide legal basis to the system and offer more accurate information to the public about its design and procedures. Further, we recommend that the terms of telecom licences also need to be revisited in so far as they contain restrictions on the encryption standards that can be adopted by TSPs and ISPs, which in turn limits the privacy rights of their users.

   The recent recommendations on data protection made by TRAI indicate a positive move in this direction.[106] The telecom regulator recommended that the Department of Telecommunication needs to re-examine the encryption standards laid down in the telecom license conditions. It noted the need for personal data of telecom consumers to be encrypted, both during storage and in motion. Further, TRAI recommended that decryption by authorised entities should be permitted on a needs basis, either with the consent of the consumer or in accordance with legal requirements.

7. *Transparency regarding SOPs* – We recommend that any standard operating procedures devised by the Government to give effect to the legal provisions governing surveillance must be made publicly available and stakeholders should also be given an opportunity to contribute to the framing of such procedures. The development of the SOPs must there-

[106] TRAI, Recommendations on Privacy, Security and Ownership of the Data in the Telecom Sector, 16 July, 2018, available at https://www.trai.gov.in/sites/default/files/RecommendationDataPrivacy16072018.pdf.

fore flow from a transparent and consultative process. To the extent that the SOPs might create any independent obligations on individuals or intermediaries, we recommend that the same should be supported by a legislative instrument.

8. *Amendments to other laws concerning transparency and accountability*: We recommend that relevant provisions of the Whistleblowers Protection Act, 2011, need to be revisited, to ensure adequate protection is given to whistleblowers who expose mala fides or illegalities in surveillance procedures. In particular, the general exemptions granted under the statute (to matters impinging on sovereignty or strategic interests of the state, disclosures under the Official Secrets Act, 1923, etc) may need to be revisited. Similarly, revisions may be required to the generic exemptions granted under the Right to Information Act, 2005, to various LEAs.

6 Analysis of Srikrishna Committee's recommendations

The Srikrishna Committee submitted its report and an accompanying draft law on protection of personal data to the Government on 27 July, 2018. The proposed law lays down protections relating to the collection, processing and use of personal data of individuals (referred to as data principals) and seeks to protect them from related harms.[107] The definition of "harm" under Section 3(21) of the proposed law includes (i) any restriction placed or suffered directly or indirectly on speech, movement or any other action arising out of a fear of being observed or surveilled; and (ii) any observation or surveillance that is not reasonably expected by the data principal.

Sections 42 and 43 of the proposed law deal with the processing of personal data in the (i) *interests of the security of the state*; and (ii) for *prevention, detection, investigation and prosecution of any offence or any other contravention of law*, respectively. In both these cases the identified activities are exempted from the requirements under the draft data protection law if they satisfy the requirements of legality, necessity and proportionality. The exemption, however, does not include the requirement to ensure that any personal data is processed in a fair and reasonable manner (Section 4) and in accordance with reasonable security standards, including methods such as

[107]Section 39(2) of the draft Personal Data Protection Bill, 2018.

de-identification and encryption of the data and prevention of misuse and unauthorised access (Section 31).

In drafting these provision, the Committee has reiterated the position laid down by the judges in the *Puttaswamy* case but without addressing the related structural and procedural elements required to make these principles work. For instance, the requirement of legality is incomplete without a description on what constitutes legality in case of access by intelligence agencies/ LEAs. Should it include only legality of the means of access or also the need for a legislative basis for the agencies to whom such access is provided? Similarly, what factors should be taken into account to judge whether a proposed intervention is "necessary and proportionate" in the facts of the case? Who should be making this determination? The report prepared by the Committee dwells a little further on some of these aspects, although it also falls short of proposing a comprehensive solution.

In the context of discussing the exemption of measures taken to ensure "security of the state", the Committee's report acknowledges that executive review alone is not sufficient to grant legitimacy to such activities. It discusses the judicial and legislative oversight mechanisms adopted in other democratic nations and concludes that the lack of such inter-branch oversight in India *"is not just a gap that is deleterious in practice but, post the judgment of the Supreme Court in Puttaswamy, potentially unconstitutional"*.

The Committee proposes that the law should provide for *ex-ante* access controls by designating a district judge to hear requests for processing of personal information by intelligence agencies in closed door proceedings. It also proposes that all such approvals should be time-bound and require periodic renewal, subject to the judge being satisfied that the purpose for processing remains relevant. In addition to recommending a need for ex-ante judicial scrutiny of surveillance requests, the report also talks about ensuring accountability through *ex-post* periodic reporting and review by a parliamentary committee.

The recommendations of the Committee point in the right direction but their effectiveness is marred by the suggestion that such measures be adopted if and when the Government decides to pursue a comprehensive law governing intelligence agencies. Given that surveillance activities are already taking place in the absence of such a comprehensive law, the immediate requirement would be to make amendments to the laws that enable such access to personal information by intelligence agencies and LEAs, namely the Telegraph and IT Acts and the procedural rules made under them. The draft law proposed by the Srikrishna Committee already suggests some amendments to provisions

contained in the IT Act and the Right to Information Act, 2005. The logical step would have been to incorporate similar suggestions on amendments to existing surveillance related laws to build in the safeguards suggested in its report regarding ex-ante analysis and ex-post accountability for surveillance related activities.

In terms of our other suggestions in the previous section, the proposed law includes an obligation of fair and reasonable processing and ensuring security of data even when such processing takes place under the given exemptions. It, however, fails to recognise some of the other important requirements like having data protection officers inside intelligence agencies and LEAs; (deferred) notice to the concerned individual, and the right to seek appropriate redress. Further, the draft law also fails to address the issue of the evidentiary value of information collected in breach of the proposed data protection law.[108]

The proposed law therefore has scope for improvement both in terms of strengthening the protections available to individuals who are subjected to surveillance activities as well as the structural and procedural safeguards governing such access. Having said that, we believe that the recommendations contained in the report, particularly on *ex-ante* and *ex-post* safeguards against surveillance, are an important starting point for this discussion. To take these suggestions to their logical conclusion, it is important that corresponding amendments should be made to the draft data protection law before it shapes into a bill that will be placed before the Parliament.

[108] Vrinda Bhandari, Data Protection Bill: Missed Opportunity for Surveillance Reform, The Quint, 28 July, 2018, available at https://www.thequint.com/voices/opinion/personal-data-protection-bill-2018-draft-srikrishna-committee-loopholes-surveillance.