

Policy Recommendations for Surveillance Law in India and an Analysis of Legal Provisions on Surveillance in India and the Necessary & Proportionate Principles

- By Maria Xynou

The Government of India has created a legal framework which supports the carrying out of surveillance by authorities through its various laws and license agreements for service providers. The Centre for Internet and Society (CIS) acknowledges that lawful, warranted, targeted surveillance can potentially be a useful tool in aiding law enforcement agencies in tackling crime and terrorism. However, current Indian laws and license agreements appear to overextend the Government's surveillance capabilities in certain cases, while inadequately safeguarding individuals' right to privacy and data protection¹. As such, the Centre for Internet and Society (CIS) suggests the following policy recommendations.

Privacy Law

Current laws and license agreements in India which allow for surveillance entail a significant potential for abuse, since the country lacks sufficient privacy safeguards². A privacy law is deemed necessary to ensure that data is not retained indefinitely, that data is not shared and disclosed to unauthorised third parties and that unauthorised parties do not have access to collected and intercepted data. In a democratic regime, surveillance should be targeted and carried out under a judicial warrant and the absence of privacy legislation deprives individuals from necessary safeguards³.

While the Information Technology Act and its Rules do entail some provisions for data protection and regulate certain types of surveillance, they appear to be inadequate⁴. This is partly due to the fact that there is currently no law in India which establishes the right to privacy and as such, there is a potential for abuse. The Information Technology (Reasonable

¹Pranesh Prakash, "How Surveillance Works in India", The New York Times, 10 July 2013,
http://india.blogs.nytimes.com/2013/07/10/how-surveillance-works-in-india/?_php=true&_type=blogs&_r=0

²Ibid

³Richard Stallman, "How Much Surveillance Can Democracy Withstand?", Wired, 14 October 2013,
<http://www.wired.com/opinion/2013/10/a-necessary-evil-what-it-takes-for-democracy-to-survive-surveillance/>

⁴The Government of India, Ministry of Communications and Information Technology, Department of Telecommunications, *The Information Technology (Amendment) Act, 2008*,
<http://police.pondicherry.gov.in/Information%20Technology%20Act%202000%20-%202008%20%28amendment%29.pdf>

Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, represent a decisive step in creating a legal regime in India for data protection, but nonetheless appear inadequate in addressing issues relating to the collection of, access to, sharing of, disclosure and retention of data⁵. Furthermore, they do not ensure the establishment of an independent body, such as a Privacy Commission, to oversee the handling of personal data and to address potential cases of breach.

Justice AP Shah Privacy Principles

The Planning Commission of the Government of India held meetings of the Group of Experts on Privacy Issues throughout 2012, which was chaired by Justice AP Shah, the former chief justice of the Delhi High Court⁶. The CIS participated in these meetings and helped draft the Report of the Group of Experts on Privacy by the Justice AP Shah committee⁷. This report entails a list of recommended national privacy principles, which should be followed in the creation of a privacy law. According to the report, the national privacy principles of India should be the following:

- Principle of Notice
- Principle of Choice and Consent
- Principle of Collection Limitation
- Principle of Purpose Limitation
- Principle of Access and Correction
- Principle of Disclosure of Information
- Principle of Security
- Principle of Openness
- Principle of Accountability⁸

The first principle of notice states that the data collector should notify all individuals of its information practices, before any personal information is collected about them. According to this principle, data collectors are required to notify individuals with regards to what personal data is being collected about them, the purposes and uses for such data collection, whether or not such personal data will be disclosed to third parties, the security safeguards established in relation to the personal information, the processes available to data subjects to access and correct their own personal information and the contact details of the privacy officers for filing complaints. Additionally, this principle also requires data controllers to notify individuals when their personal data has been breached, when such data has been legally accessed by third parties and when the data controller's privacy policy changes⁹.

The second principle of choice and consent states that the data controller should provide individuals the choice to opt-in or opt-out with regards to the provision of their personal data, as well as that individual consent should only be taken by the data controller after providing

⁵R Ananthapur, "India's new Data Protection Legislation", (2011) 8:2 *SCRIPTed* 192,
<http://www.law.ed.ac.uk/ahrc/script-ed/vol8-2/ananthapur.asp>

⁶Prasad Krishna, "Sixth Meeting of the two Sub-Groups on Privacy Issues under the Chairmanship of Justice AP Shah", The Centre for Internet and Society, 23 August 2012, <http://cis-india.org/news/sixth-meeting-of-sub-groups-on-privacy-issues>

⁷ Justice Ajit Prakash Shah, Former Chief Justice, High Court of Delhi, "Report of the Group of Experts on Privacy", Planning Commission (CIT&I Division), Government of India, 16 October 2012,
http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf

⁸Ibid

⁹Ibid

notice of its information practices. The third principle of collection limitation states that the data controller shall only collect personal information from data subjects as is necessary for the purposes identified for such collection, regarding which notice has been provided and consent from the individual taken. It is also stated that such collection should be through lawful and fair means¹⁰.

The fourth principle of purpose limitation states that personal data collected and processed by data collectors should be adequate and relevant to the purposes for which they are processed. In other words, a data controller should only collect, process, disclose, make available or otherwise use personal data for the purpose as stated in the notice after taking consent from individuals. The fifth principle of access and correction applies to individuals. In particular, this principle states that individuals should have the right to access their personal information which is being held by a data controller and to make corrections or to delete information when it is inaccurate¹¹.

The sixth principle of disclosure of information prohibits the data controller from disclosing personal data to third parties, unless informed consent has been provided by the individual for such disclosure. This principle also states that disclosure of information for law enforcement purposes must be in accordance with the laws in force. The seventh principle of security states that data controllers should be responsible for ensuring the security of all personal data that they have collected or which is in their custody. Such security safeguards should prevent loss, unauthorised access, destruction, use, processing, storage, modification, de-anonymization, unauthorised disclosure (either accidental or incidental) or other reasonably foreseeable risks¹².

The eighth principle of openness requires data controllers to take all necessary steps to implement practices, procedures, policies and systems in a manner proportional to the scale, scope and sensitivity to the data they collect, in order to ensure compliance with the privacy principles, information regarding which shall be made in an intelligible form, using clear and plain language, available to all individuals. Finally, the ninth principle of accountability states that the data controller should be accountable for complying with measures which give effect to the privacy principles. Such measures should include mechanisms to implement privacy policies, including tools, training, education, as well as external and internal audits¹³.

In the report, the Group of Experts on Privacy recommended that such national privacy principles are applied to the cases of interception of communications, access to data and audio and video recording. In particular, it is emphasized that, with regards to the interception of communications and access to data in India, the principles of notice, choice and consent, and access and correction should be applied. With regards to audio and video recording in India, the application of the same principles, additionally including the principle of collection limitation, is recommended¹⁴.

Furthermore, the Group of Experts on Privacy also recommended the enactment of a privacy law in India which would include the establishment of Privacy Commissioners, as well as of self-regulating organisation (SROs) and co-regulation, which would supplement the role

¹⁰Ibid

¹¹Ibid

¹²Ibid

¹³Ibid

¹⁴Ibid

played by the Privacy Commissioners to ensure the implementation and enforcement of policies for a wide range of sectors and industries. Additionally, the Group of Experts recommended the establishment of a system of complaints which would include Alternative Dispute Resolution Mechanisms (ADRs), as well as the inclusion of offenses, penalties and remedies in the Privacy Act¹⁵.

International Principles on the Application of Human Rights to Communications Surveillance

The Electronic Frontier Foundation (EFF), Privacy International and Access started drafting the international principles on the application of human rights to communications surveillance in late 2012. The goal of these principles is to provide civil society groups, the industry and governments with a framework to evaluate whether current or proposed surveillance laws and practices are consistent with human rights. These principles were developed through a consultation with experts from civil society groups and industry across the world¹⁶. The thirteen principles on the application of human rights to communications surveillance are the following¹⁷:

“Legality: Any limitation to the right to privacy must be prescribed by law. The State must not adopt or implement a measure that interferes with the right to privacy in the absence of an existing publicly available legislative act, which meets a standard of clarity and precision that is sufficient to ensure that individuals have advance notice of and can foresee its application. Given the rate of technological changes, laws that limit the right to privacy should be subject to periodic review by means of a participatory legislative or regulatory process.

Legitimate Aim: Laws should only permit communications surveillance by specified State authorities to achieve a legitimate aim that corresponds to a predominantly important legal interest that is necessary in a democratic society. Any measure must not be applied in a manner which discriminates on the basis of race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.

Necessity: Laws permitting communications surveillance by the State must limit surveillance to that which is strictly demonstrably necessary to achieve a legitimate aim. Communications surveillance must only be conducted when it is the only means of achieving a legitimate aim, or when there are multiple means, it is the means least likely to infringe upon human rights. The onus of establishing this justification, in judicial as well as in legislative processes, is on the State.

Adequacy: Any instance of communications surveillance authorised by law must be appropriate to fulfill the specific legitimate aim identified.

Proportionality: Communications surveillance should be regarded as a highly intrusive act

¹⁵Ibid

¹⁶Elonnai Hickok, “Draft International Principles on Communications Surveillance and Human Rights”, The Centre for Internet and Society, 16 January 2013, <http://cis-india.org/internet-governance/blog/draft-intl-principles-on-communications-surveillance-and-human-rights>

¹⁷Electronic Frontier Foundation, Privacy International & Access, “International Principles on the Application of Human Rights to Communications Surveillance”, Necessary & Proportionate, 10 July 2013, <https://www.eff.org/files/necessaryandproportionatefinal.pdf>

that interferes with the rights of privacy and freedom of opinion and expression, threatening the foundations of a democratic society. Decisions about communications surveillance must be made by weighing the benefit sought to be achieved against the harm that would be caused to the individual's rights and to other competing interests, and should involve a consideration of the sensitivity of the information and the sensitivity of the infringement on the right to privacy.

Specifically, this requires that, if a State seeks access to or use of protected information obtained through communications surveillance in the context of a criminal investigation, it must establish to the competent, independent, and impartial judicial authority that:

- there is a high degree of probability that a serious crime has been or will be committed
- evidence of such a crime would be obtained by accessing the protected information sought
- other available less invasive investigative techniques have been exhausted
- information accessed will be confined to that reasonably relevant to the crime alleged and any excess information collected will be properly destroyed or returned
- information is accessed only by the specified authority and used for the purpose for which authorisation was given

If the State seeks access to protected information through communication surveillance for a purpose that will not place a person at risk of criminal prosecution, investigation, discrimination or infringement of human rights, the State must establish to an independent, impartial and competent authority:

- other available less invasive investigative techniques have been considered
- information accessed will be confined to what is reasonably relevant and any excess information collected will be promptly destroyed or returned to the impacted individual
- information is accessed only by the specified authority and used for the purpose for which authorisation was given

Competent Judicial Authority: Determinations related to communications surveillance must be made by a competent judicial authority that is impartial and independent. The authority must be:

- separate from the authorities conducting communications surveillance
- conversant in issues related to and competent to make judicial decisions about the legality of communications surveillance, the technologies used and human rights
- have adequate resources in exercising the functions assigned to them¹⁸

Due Process: Due Process requires that States respect and guarantee individual's rights by ensuring that lawful procedures that govern any interference with human rights are properly enumerated in law, consistently practiced, and available to the general public. Specifically, in the determination of one's human rights, everyone is entitled to a fair and public hearing within a reasonable time by an independent, competent and impartial tribunal established by law, except in cases of emergency where there is imminent risk of danger to human life. In such instances, retroactive authorisation must be sought within a reasonably practicable time period. Mere risk of flight or destruction of evidence shall never be considered as sufficient to justify retroactive authorisation.

¹⁸Ibid

User Notification: Individuals should be notified of a decision authorising communications surveillance with enough time and information to enable them to appeal the decision, and should have access to the materials presented in support of the application for authorisation. Delay in notification is only justified in the following circumstances:

- Notification would seriously jeopardize the purpose for which the surveillance is authorised, or there is an imminent risk of danger to human life
- Authorisation to delay notification is granted by the competent judicial authority at the time that authorisation for surveillance is granted
- The individual affected is notified as soon as the risk is lifted or within a reasonably practicable time period, whichever is sooner, and in any event by the time communications surveillance has been completed. The obligation to give notice rests with the State, but in the event that the State fails to give notice, communications service providers shall be free to notify individuals of the communications surveillance, voluntary or upon request.

Transparency: States should be transparent about the use and scope of communications surveillance techniques and powers. They should publish, at a minimum, aggregate information on the number of requests approved and rejected, a disaggregation of the requests by service provider and by investigation type and purpose. States should provide individuals with sufficient information to enable them to fully comprehend the scope, nature, and application of the laws permitting communications surveillance. States should enable service providers to publish the procedures they apply when dealing with State communications surveillance, adhere to those procedures, and publish records of State communications surveillance.

Public oversight: States should establish independent oversight mechanisms to ensure transparency and accountability of communications surveillance. Oversight mechanisms should have the authority to access all potentially relevant information about State actions, including, where appropriate, access to secret or classified information; to assess whether the State is making legitimate use of its lawful capabilities; to evaluate whether the State has been transparently and accurately publishing information about the use and scope of communications surveillance techniques and powers; and to publish periodic reports and other information relevant to communications surveillance. Independent oversight mechanisms should be established in addition to any oversight already provided through another branch of government.¹⁹

Integrity of Communications and Systems: In order to ensure the integrity, security and privacy of communications systems, and in recognition of the fact that compromising security for State purposes almost always compromises security more generally, States should not compel service providers or hardware or software vendors to build surveillance or monitoring capabilities into their systems, or to collect or retain particular information purely for State surveillance purposes. A priori data retention or collection should never be required for service providers. Individuals have the right to express themselves anonymously; States should therefore refrain from compelling the identification of users as a precondition for service provision.

Safeguards for International Cooperation: In response to changes in the flows of

¹⁹Ibid

information, and in communications technologies and services, States may need to seek assistance from a foreign service provider. Accordingly, the mutual legal assistance treaties (MLATs) and other agreements entered into by States should ensure that, where the laws of more than one state could apply to communications surveillance, the available standard with the higher level of protection for individuals is applied. Where States seek assistance for law enforcement purposes, the principle of dual criminality should be applied. States may not use mutual legal assistance processes and foreign requests for protected information to circumvent domestic legal restrictions on communications surveillance. Mutual legal assistance processes and other agreements should be clearly documented, publicly available, and subject to guarantees for procedural fairness.

Safeguards against Illegitimate Access: *States should enact legislation criminalizing illegal communications surveillance by public or private actors. The law should provide sufficient and significant civil and criminal penalties, protections for whistle blowers, and avenues for redress by affected individuals. Laws should stipulate that any information obtained in a manner that is inconsistent with these principles is inadmissible as evidence in any proceeding, as is any evidence derivative of such information. States should also enact laws providing that, after material obtained through communications surveillance has been useful for the purpose for which information was given, the material must be destroyed or returned to the individual²⁰. ”*

The Centre for Internet and Society (CIS) strongly supports the International Principles on the Application of Human Rights to Communications Surveillance and recommends that laws in India comply with them. In particular, the CIS urges the Government of India to amend existing laws, policies and license agreements with regards to these principles, to ensure that surveillance carried out in the country complies with safeguards and protects human rights. Furthermore, the CIS strongly urges the Government of India to form MLATs in accordance with the principle of “Safeguards for International Cooperation”, as mentioned above²¹.

Amendments to National Laws on Surveillance

The Centre for Internet and Society (CIS) recommends that current national laws which regulate surveillance in India are amended in accordance with the National Privacy Principles²² and the International Principles on the Application of Human Rights to Communications Surveillance²³, and that a privacy law is enacted.

Amendment of draft Rule 419B under the Indian Telegraph Act, 1885

In June 2013, draft Rule 419B under the Indian Telegraph Act, 1885, was proposed. This draft Rule requires the disclosure of Call Data Records (CDR), otherwise known as Call Detail Records, to law enforcement agencies²⁴. However, the CIS recommends that if draft

²⁰Ibid

²¹Ibid

²² Justice Ajit Prakash Shah, Former Chief Justice, High Court of Delhi, “Report of the Group of Experts on Privacy”, Planning Commission (CIT&I Division), Government of India, 16 October 2012, http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf

²³Electronic Frontier Foundation, Privacy International & Access, “International Principles on the Application of Human Rights to Communications Surveillance”, Necessary & Proportionate, 10 July 2013, <https://www.eff.org/files/necessaryandproportionatefinal.pdf>

²⁴Maria Xynou, “India’s Central Monitoring System (CMS): Something to Worry About?”, Centre for Internet

Rule 419B is adopted, the specific conditions for the disclosure of Call Data Records should be legally specified, which would limit the potential for abuse and unauthorised disclosure of personal information. Additionally, the CIS recommends that adequate documentary evidence should be provided to a court prior to any disclosure of such records, which would prove that such a disclosure is necessary to protect individuals from an imminent threat. Furthermore, individuals should be notified about the disclosure of their records and law enforcement agencies should be held accountable in instances of unauthorised disclosure. In short, the CIS recommends that this draft Rule is amended in compliance with the Justice AP Shah Principles of Disclosure of Information²⁵ and Transparency²⁶.

Amendments to the Information Technology Act, 2000

It is noteworthy that the Information Technology (Amendment) Act, 2008, removed the preconditions of “public emergency” and “public safety” which are grounded in the Indian Telegraph Act, 1885, and expanded the power of the Government to order the interception of communications for the “investigation of any offense”²⁷. While the term “offense” is legally specified, it remains rather broad and vague, which could create a potential for abuse. As such, similarly to the amendments recommended for Section 5(2) of the Indian Telegraph Act, 1885, the CIS recommends that documentary evidence by law enforcement agencies is brought to court as a prerequisite to the authorisation for interception. In other words, it is recommended that authorisations for the interception of communications under the Information Technology Act are in compliance with the International Principles of Legality, Legitimate Aim, Necessity, Adequacy and Proportionality²⁸.

With regards to data retention, the CIS highly recommends that Section 67C of the Information Technology Act is amended to specify the data retention periods. Section 67C of the Act requires the retention of data, but does not specify its time period²⁹. This could create a potential for abuse and deprives individuals from their “right to be forgotten”. As such, the proposed amendment of Section 67C should categorize and specify the various data retention periods for different types of data. Furthermore, Section 67C should detail the procedures for the full destruction of data once it has exceeded its data retention period, as well as specify the conditions under which authorised access to retained data can be granted. In order to

and Society, 30 January 2014, <http://cis-india.org/internet-governance/blog/india-central-monitoring-system-something-to-worry-about>

²⁵Justice Ajit Prakash Shah, Former Chief Justice, High Court of Delhi, “*Report of the Group of Experts on Privacy*”, Planning Commission (CIT&I Division), Government of India, 16 October 2012, http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf

²⁶Electronic Frontier Foundation, Privacy International & Access, “*International Principles on the Application of Human Rights to Communications Surveillance*”, Necessary & Proportionate, 10 July 2013, <https://www.eff.org/files/necessaryandproportionatefinal.pdf>

²⁷The Government of India, Ministry of Communications and Information Technology, Department of Telecommunications, *The Information Technology (Amendment) Act, 2008*, <http://police.pondicherry.gov.in/Information%20Technology%20Act%202000%20-%202008%20%28amendment%29.pdf>

²⁸Electronic Frontier Foundation, Privacy International & Access, “*International Principles on the Application of Human Rights to Communications Surveillance*”, Necessary & Proportionate, 10 July 2013, <https://www.eff.org/files/necessaryandproportionatefinal.pdf>

²⁹The Government of India, Ministry of Communications and Information Technology, Department of Telecommunications, *The Information Technology (Amendment) Act, 2008*, <http://police.pondicherry.gov.in/Information%20Technology%20Act%202000%20-%202008%20%28amendment%29.pdf>

legally specify the conditions for access to, sharing and disclosure of retained data, Section 67C should be amended and a privacy law should be enacted to regulate data protection.

Lastly, the CIS recommends the re-examination of Sections 44 and 80 of the Information Technology Act. In particular, Section 44 imposes penalties on anyone who fails to provide requested information to authorities, while Section 80 allows inspectors of the police to conduct searches and seize suspects in public places without a warrant³⁰. The CIS recommends that Section 44 is amended to include legal specifications with regards to such requested information, in order to limit the potential for abuse. Furthermore, the CIS recommends that Section 80 is also amended to legally list the conditions under which suspects can be seized in public places and to require a judicial warrant in every such case.

Amendments to License Agreements

The Centre for Internet and Society (CIS) recommends the amendment of certain clauses of the License Agreements for service providers in India which require the surveillance of communications.

Amendments to the ISP License Agreement

In particular, clause 2.2. of the ISP License Agreement prohibits bulk encryption, as well as encryption that exceeds 40 bits in symmetric key algorithms³¹. Under this clause, users can only use encryption over 40 bits if they have acquired written permission from the service provider and disclosed their private encryption keys. However, encryption below 40 bits in symmetric key algorithms is extremely limited and disincentives individuals from using encryption. Furthermore, the requirement to disclose their private encryption keys in order to legally gain permission to use encryption that exceeds 40 bits in symmetric key algorithms deprives individuals from their right to online anonymity, right to privacy and freedom of expression. Additionally, the RBI Guidelines on Internet Banking³² require banks to use a minimum of 128 bit SSL encryption which would violate the terms of the ISP License. As such, the CIS highly recommends that clause 2.2. of the ISP License Agreement is amended to allow for bulk encryption, as well as to permit encryption that exceeds 40 bits in symmetric key algorithms.

Furthermore, it is recommended that this clause is amended to prohibit service providers from requiring users to disclose their private encryption keys. The decryption of information should be a last resort and should be strictly restricted to instances where law enforcement have provided a court adequate documentary evidence to support the claim that the specific encrypted information needs to be decrypted.

Clause 34.6 of the ISP License Agreement requires designated persons of the Government of India or of State Governments to monitor the telecommunications traffic in every node or in any other technically feasible point in the network³³. However, the CIS recommends that this

³⁰Ibid

³¹Government of India, Ministry of Communications and Information Technology, Department of Telecommunications, *License Agreement for Provision of Internet Services*, 1998,
<http://www.dot.gov.in/data-services/internet-services>

³²Reserve Bank of India, *Internet Banking in India – Guidelines*,
<http://www.rbi.org.in/scripts/NotificationUser.aspx?Id=414&Mode=0>

³³Ibid

clause is amended to include provisions for checks and balances and for transparency. In particular, an independent oversight mechanism should be established to oversee the monitoring of telecommunications traffic by the authorities and to report potential cases of breach. This would potentially not only increase transparency, but also limit the potential for abuse.

Clause 34.27 of the ISP License Agreement allows service providers to install central monitoring centres at their premises but does not specify the conditions under which they would function³⁴. As such, the CIS recommends that the necessity and utility of such central monitoring systems is adequately proven in court prior to their installation. Furthermore, the CIS recommends the establishment of an independent oversight mechanism, such as a Privacy Commission or a Surveillance Oversight Committee (Chapter 3), which would oversee the function of such central monitoring systems and report potential cases of breach.

Amendments to the CMTS License Agreement

Clause 22.2 of the CMTS License Agreement requires the installation of “necessary facilities” to aid the interception of messages by service providers³⁵. However, it remains unclear what “necessary facilities” constitute, as well as what type of monitoring equipment would generally be used for such purposes. The CIS sent RTI requests with regards to the monitoring equipment used by service providers, but this information was not disclosed on the grounds of national security. However, the various types of monitoring equipment, such as FinFisher spyware which can remotely be deployed into a target’s computer without his or her knowledge or consent, can potentially violate individuals right to privacy and other human rights³⁶. Therefore, the CIS highly recommends that not only is the Department of Telecommunications transparent about the types of monitoring equipment that it authorises, but that clause 22.2 – and all other similar clauses – is amended in order to legally specify the “necessary facilities” for the interception of messages³⁷.

Amendments to the BTS License Agreement

According to clause 1.10.7 of the BTS License Agreement, service providers are responsible for ensuring the privacy of communications in their networks and that unauthorised interception does not take place³⁸. Similar provisions are also included in other clauses of license agreements. However, it remains unclear how service providers are required to prevent unauthorised interception and to ensure users privacy, when many other clauses of the same License Agreements require the interception and monitoring of communications. While the CIS strongly supports clause 1.10.7 of the BTS License Agreement – and all other

³⁴Ibid

³⁵Government of India, Ministry of Communications and Information Technology, Department of Telecommunications, *License Agreement for Provision of Cellular Mobile Telephone Service, 1994*, <http://www.usof.gov.in/usof-cms/tender/cmtsAGREEMENT.pdf>

³⁶Morgan Marquis-Boire, Bill Marczak, Claudio Guarnieri & John Scott-Railton, “*For Their Eyes Only: The Commercialization of Digital Spying*”, The Citizen Lab, 30 April 2013, <https://citizenlab.org/2013/04/for-their-eyes-only-2/>

³⁷Government of India, Ministry of Communications and Information Technology, Department of Telecommunications, *License Agreement for Provision of Cellular Mobile Telephone Service, 1994*, <http://www.usof.gov.in/usof-cms/tender/cmtsAGREEMENT.pdf>

³⁸Government of India, Ministry of Communications and Information Technology, Department of Telecommunications, *License Agreement for Provision of Basic Telephone Service, 1992*, <http://www.usof.gov.in/usof-cms/tender/usotender18Jan07/BasicServiceLicence.pdf>

similar clauses in other License Agreements – it appears to be extremely contradictory with regards to the other clauses which allow for the interception of communications³⁹. As such, the CIS recommends that the above – and following – proposed amendments with regards to clauses which allow for the interception of communications are seriously taken into consideration.

Amendments to the UAS License Agreement

In June 2013, clause 41.10 of the UAS License Agreement was amended to include provisions for the Central Monitoring System (CMS). In particular, the amended clause requires data to be automatically transmitted from service providers to the CMS through MPLS connectivity. However, the CMS is not legally mandated which raises questions of whether service providers should enable the transmission of data through their networks to the CMS data centre. Furthermore, by bypassing service providers and enabling the automatic transmission of data to the CMS, the amended clause is enabling the centralisation of intercepted data. Security experts, though, have pointed out that the centralisation of data does not necessarily increase its security but, on the contrary, creates a centralised point for cyber attacks. Moreover, the CMS lacks parliamentary and public debate prior to its implementation, which raises questions with regards to its legality and constitutionality. As such, the CIS recommends that amended clause 41.10 is reconsidered and possibly further amended, since it entails details for the carrying out of a system which lacks public and parliamentary debate and creates the potential for security threats.

Clause 41.12 of the UAS License Agreement appears to be quite contradictory because, on the one hand, it prohibits service providers from employing bulk encryption and, on the other hand, requires them to ensure the privacy of communications in their networks⁴⁰. In order to remove this oxymoron, the CIS urges the amendment of this clause which will allow bulk encryption in networks. Furthermore, clauses 41.17, 41.19 and 41.20 of the UAS License Agreement allow for data retention, but do not specify the data retention periods for the various types of data, nor the conditions for such retention⁴¹. The CIS therefore recommends that these clauses are amended to include specific conditions for data retention, which limit access to, sharing and disclosure of retained data and which comply with the National Privacy Principles⁴² and/or with the International Principles on the Application of Human Rights to Communications Surveillance⁴³. More importantly though, the CIS recommends the establishment of a privacy law which will regulate data retention.

Amendments to the Unified License (Access Services) Agreement

Clause 41.12 of the Unified License (Access Services) Agreement requires service providers

³⁹Ibid

⁴⁰Government of India, Ministry of Communications and Information Technology, Department of Telecommunications, *License Agreement for Provision of Unified Access Services After Migration from CMTS*, 2003, <http://www.dot.gov.in/access-services/unified-access-services>

⁴¹Ibid

⁴²Justice Ajit Prakash Shah, Former Chief Justice, High Court of Delhi, “Report of the Group of Experts on Privacy”, Planning Commission (CIT&I Division), Government of India, 16 October 2012, http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf

⁴³Electronic Frontier Foundation, Privacy International & Access, “International Principles on the Application of Human Rights to Communications Surveillance”, Necessary & Proportionate, 10 July 2013, <https://www.eff.org/files/necessaryandproportionatefinal.pdf>

to disclose Call Data Records to law enforcement agencies⁴⁴. However, the conditions for such disclosure are not specified, which is why the CIS recommends that this clause is amended to specify the conditions for authorised disclosure of such records. Furthermore, clause 41.26(x) of the Unified License (Access Services) Agreement requires service providers to provide the geographical location of any subscriber to law enforcement agencies at any given point of time⁴⁵. This clause potentially violates individuals right to privacy and other human rights, which is why it is recommended that the clause is amended to specify the conditions under which such information can be disclosed. Lastly, clause 41.26(xiv) of the Unified License (Access Services) Agreement requires the use of a “suitable technical device” in which a mirror image of remote access to information can be made available online for monitoring purposes⁴⁶. However, this clause does not specify the parties which can be authorised to use such a device, nor does it specify who can have authorised remote access to such information for monitoring purposes. As such, the vagueness of the clause could create a potential for abuse, which is why it is recommended that it is amended accordingly.

In general, the CIS recommends that the License Agreements for communications service providers in India are amended in accordance with the National Privacy Principles⁴⁷ and the International Principles on the Application of Human Rights to Communications Surveillance⁴⁸.

Specific prohibition of mass surveillance

As discussed in this chapter, mass surveillance in India is a legally gray area. Though not specifically mandated, it is not prohibited and the License Agreements for ISPs and TSPs include technical and legal requirements that could allow for mass surveillance.

As in line with the Necessary and Proportionate principle of *Proportionality*⁴⁹ and the Justice AP Principle of *Purpose Limitation*⁵⁰, it is recommended that surveillance should be regarded as a highly intrusive act that interferes with the rights to privacy and freedom of opinion and expression, threatening the foundations of a democratic society. Decisions about communications surveillance must be made by weighing the benefit sought to be achieved against the harm that would be caused to the individual's rights and to other competing interests, and should involve a consideration of the sensitivity of the information and the severity of the infringement on the right to privacy. It is therefore recommended that Indian law is amended to specifically prohibit mass surveillance.

⁴⁴Government of India, Ministry of Communications and Information Technology, Department of Telecommunications, *License Agreement for Unified License (Access Services)*, 2013, <http://www.dot.gov.in/sites/default/files/DOC270613-013.pdf>

⁴⁵Ibid

⁴⁶Ibid

⁴⁷Justice Ajit Prakash Shah, Former Chief Justice, High Court of Delhi, “Report of the Group of Experts on Privacy”, Planning Commission (CIT&I Division), Government of India, 16 October 2012, http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf

⁴⁸Electronic Frontier Foundation, Privacy International & Access, “International Principles on the Application of Human Rights to Communications Surveillance”, Necessary & Proportionate, 10 July 2013, <https://www.eff.org/files/necessaryandproportionatefinal.pdf>

⁴⁹Electronic Frontier Foundation, Privacy International & Access, “International Principles on the Application of Human Rights to Communications Surveillance”, Necessary & Proportionate, 10 July 2013, <https://www.eff.org/files/necessaryandproportionatefinal.pdf>

⁵⁰Justice Ajit Prakash Shah, Former Chief Justice, High Court of Delhi, “Report of the Group of Experts on Privacy”, Planning Commission (CIT&I Division), Government of India, 16 October 2012, http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf

Harmonization of circumstances for surveillance

Presently, the Indian surveillance regime allows for the same surveillance techniques to be used in different circumstances. This is based on the difference between digital and non-digital data, as well as on the difference between legislations and operating licenses. For example, Section 5(2) of the Indian Telegraph Act, 1885, allows for the interception of telephonic conversations on the occurrence of any public emergency or in the interest of public safety⁵¹. The Central Government or a State Government or any officer specially authorised in this behalf by the Central Government or a State Government may order interception, if satisfied that it is necessary or expedient to do so in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of an offense.

Section 69 of the Information Technology Act, however, allows for the interception, monitoring and decryption of digital information in the interest of the sovereignty and integrity of India, of the defense of India, security of the State, friendly relations with foreign nations, public order, preventing the incitement to the commission of any cognizable offense relating to the above, and for the investigation of an offense⁵². As such, it is evident that the legal circumstances for surveillance in India lack harmonization and the same applies to license agreements, which also allow for surveillance, but under varying circumstances.

For example, section 41.10 of the UAS License Agreement empowers the designated person of the Central/State Government with the right to monitor the telecommunications traffic in every MSC/Exchange/MGC/MG or any other technically feasible point in the network set up by the Licensee⁵³. However, section 69B of the Information Technology Act 2008 requires the monitoring of traffic data to enhance cyber security and to enable the identification, analysis and prevention of intrusion or spread of computer contaminant in the country⁵⁴.

Further highlighting discrepancies in the Indian surveillance regime include section 41.20 (xix) of the UAS License Agreement which states “*In order to maintain the privacy of voice and data, monitoring shall be in accordance with rules in this regard under the Indian Telegraph Act, 1885*”⁵⁵. Yet, the Indian Telegraph Act, 1885, provides for 'interception' and does not specifically provide for 'monitoring' capabilities⁵⁶.

⁵¹Government of India, Ministry of Communications and Information Technology, Department of Telecommunications, *Indian Telegraph Act, 1885*, <http://www.ijlt.in/pdffiles/Indian-Telegraph-Act-1885.pdf>

⁵²Government of India, Ministry of Communications and Information Technology, Department of Telecommunications, *The Information Technology (Amendment) Act, 2008*, <http://police.pondicherry.gov.in/Information%20Technology%20Act%202000%20-%202008%20%28amendment%29.pdf>

⁵³Government of India, Ministry of Communications and Information Tehcnology, Department of Telecommunications, *License Agreement for Provision of Unified Access Services After Migration from CMTS, 2003*, <http://www.dot.gov.in/access-services/unified-access-services>

⁵⁴Government of India, Ministry of Communications and Information Technology, Department of Telecommunications, *The Information Technology (Amendment) Act, 2008*, <http://police.pondicherry.gov.in/Information%20Technology%20Act%202000%20-%202008%20%28amendment%29.pdf>

⁵⁵Government of India, Ministry of Communciations and Information Tehcnology, Department of Telecommunications, *License Agreement for Provision of Unified Access Services After Migration from CMTS, 2003*, <http://www.dot.gov.in/access-services/unified-access-services>

⁵⁶Government of India, Ministry of Communications and Information Technology, Department of Telecommunications, *Indian Telegraph Act, 1885*, <http://www.ijlt.in/pdffiles/Indian-Telegraph-Act-1885.pdf>

Therefore it is recommended that the circumstances for surveillance are harmonized based on technique and capability. As such, the application of a surveillance technique should be legally permitted according to the same set of circumstances.

Periodic review of legislation and practices

Presently, the Indian Government is in the process of amending the Indian Telegraph Act, 1885, to account for access to call record details (CDR). As discussed in this chapter, the Department of Telecommunications is proposing to amend the 419A Rules and to introduce Rule 419B, which is to be read with Section 5(2) of the Indian Telegraph Act, 1885. If passed, this Rule will allow for the disclosure of “message related information”/ Call Data Records (CDRs) to Indian authorities⁵⁷. However, the collection, access, retention, sharing and disclosure of all such data currently lacks adequate legal backing.

Furthermore, Indian law still does not account for a number of situations arising out of new technologies. For example, the evidential status of social media content has not been addressed legally, and neither has 'metadata' been legally defined and addressed. Many surveillance technologies, such as drones, CCTV cameras and monitoring solutions, are currently unregulated. Clearly, there is a need for the Indian Government to review existing laws and practices and to ensure that all provisions are current and relevant.

As in the Necessary and Proportionate principle of *Legality*, it is recommended that existing laws are reviewed on a periodic basis⁵⁸. This review should be participatory.

Narrowing of circumstances for surveillance

Presently, in the operating Licenses for service providers, the circumstances for different types of surveillance are not defined and left legally ambiguous.

For example, section 41.10 of the UAS License Agreement states “*The Licensee shall be required to provide the call data records of all specified calls handled by the system at specified periodicity, as and when required by security agencies*”. Furthermore, section 41.16 of the UAS License Agreement states “*The Licensee shall make available, at any prescribed instant, to the Licenser or its authorised representative details of the subscribers using the service*”⁵⁹.

Therefore, as in the Necessary and Proportionate principles of *Legality* and *Legitimate Aim*⁶⁰,

⁵⁷Maria Xynou, “*India’s Central Monitoring System (CMS): Something to Worry About?*”, Centre for Internet and Society (CIS), 30 January 2014, <http://cis-india.org/internet-governance/blog/india-central-monitoring-system-something-to-worry-about>

⁵⁸Electronic Frontier Foundation, Privacy International & Access, “*International Principles on the Application of Human Rights to Communications Surveillance*”, Necessary & Proportionate, 10 July 2013, <https://www.eff.org/files/necessaryandproportionatefinal.pdf>

⁵⁹Government of India, Ministry of Communications and Information Tehcnology, Department of Telecommunications, *License Agreement for Provision of Unified Access Services After Migration from CMTS, 2003*, <http://www.dot.gov.in/access-services/unified-access-services>

⁶⁰Electronic Frontier Foundation, Privacy International & Access, “*International Principles on the Application of Human Rights to Communications Surveillance*”, Necessary & Proportionate, 10 July 2013, <https://www.eff.org/files/necessaryandproportionatefinal.pdf>

it is recommended that:

- All surveillance techniques that limit the right to privacy are grounded in a legislative act which meets a standard of clarity and precision that is sufficient to ensure that individuals have advance notice of and can foresee its application
- Any circumstance on which surveillance can legally take place must achieve a legitimate aim that corresponds to a predominantly important legal interest that is necessary in a democratic society

Technical requirements

The Indian surveillance regime contains a number of provisions requiring service providers to extend all facilities necessary and to install monitoring equipment on their networks as prescribed and when required. Furthermore, service providers are required to retain a number of different types of information to be shared with authorised agencies on a pro-active basis. Additionally, the Indian surveillance regime requires mandatory registration and identification of all subscribers, prior to providing service⁶¹.

As in the Necessary and Proportionate principle of *Integrity of Communications and Systems*⁶², it is recommended that the Indian Surveillance regime does not:

- Compel service providers to install particular surveillance or monitoring capabilities into their systems
- Compel service providers to pro-actively retain and disclose information to authorized agencies - Access should always be on a re-active basis
- Compel the identification of subscribers as a precondition for service provision

Limitation on collection and use of surveilled material

The contemporary Indian surveillance regime requires that directions for interception contain the reasons for the interception, and if additional information is collected during the authorized interception, law enforcement is permitted to collect and use this information. As such, it is evident that there are no limits to the use of material collected through other forms of surveillance.

As in the Justice AP Shah principles of *Purpose Limitation* and *Collection Limitation*⁶³ and in the Necessary and Proportionate principle of *Safeguards Against Illegitimate Access*⁶⁴, it is

⁶¹Government of India, Ministry of Communications and Information Technology, Department of Telecommunications, *License Agreement for Provision of Unified Access Services After Migration from CMTS, 2003*, <http://www.dot.gov.in/access-services/unified-access-services>

⁶²Electronic Frontier Foundation, Privacy International & Access, “*International Principles on the Application of Human Rights to Communications Surveillance*”, Necessary & Proportionate, 10 July 2013, <https://www.eff.org/files/necessaryandproportionatefinal.pdf>

⁶³Justice Ajit Prakash Shah, Former Chief Justice, High Court of Delhi, “*Report of the Group of Experts on Privacy*”, Planning Commission (CIT&I Division), Government of India, 16 October 2012, http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf

⁶⁴Electronic Frontier Foundation, Privacy International & Access, “*International Principles on the Application of Human Rights to Communications Surveillance*”, Necessary & Proportionate, 10 July 2013, <https://www.eff.org/files/necessaryandproportionatefinal.pdf>

recommended that:

- Law enforcement may only collect information relevant to the purpose, as specified in the lawful order
- Information that is collected that does not relate to the purpose stated in the lawful order should be destroyed or new authorization should be obtained to use the information
- Information may be used only for the purpose as stated in the lawful order

Principles of due process

Presently, the Indian surveillance regime does not contain provisions that provide critical elements of due process to the citizen, such as notice, appeal, and effective remedies.

As defined in the Necessary and Proportionate principle of *due process* and *user notification*⁶⁵, and partially in the Justice AP Shah principle of *notice*⁶⁶ - it is recommended that the Indian surveillance regime incorporates the following:

- A process for individuals to access a fair and public hearing for unauthorized interception, with access to effective remedies
- Provision of access to the materials presented in support of the application for authorisation
- Return of information collected through surveillance to individuals after the completion of an investigation

Proportional Penalties

The surveillance regime in India holds intermediaries and citizens liable for up to seven years in prison for not complying with an interception, monitoring, or decryption order, and three years in prison for not complying with an order for the collection of traffic data⁶⁷. This penalty is disproportionate to the offense committed and does not provide incentives for service providers to challenge, question, or reject unauthorized or questionably legal surveillance orders.

As implied in the principle of Necessary and Proportionate principle of *safeguards against illegitimate access*,⁶⁸ it is recommended that service providers have the ability to refuse extra legal requests without fear of imprisonment. It is also recommended that the Indian surveillance regime defines penalties that are proportionate to the offence committed, and specifically does not penalize intermediaries for questioning the legality of requests.

⁶⁵Ibid

⁶⁶Justice Ajit Prakash Shah, Former Chief Justice, High Court of Delhi, “Report of the Group of Experts on Privacy”, Planning Commission (CIT&I Division), Government of India, 16 October 2012, http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf

⁶⁷Government of India, Ministry of Communications and Information Technology, Department of Telecommunications, *The Information Technology (Amendment) Act, 2008*, <http://police.pondicherry.gov.in/Information%20Technology%20Act%202000%20-%202008%20%28amendment%29.pdf>

⁶⁸Electronic Frontier Foundation, Privacy International & Access, “International Principles on the Application of Human Rights to Communications Surveillance”, Necessary & Proportionate, 10 July 2013, <https://www.eff.org/files/necessaryandproportionatefinal.pdf>

Safeguards for International Cooperation

As demonstrated by the research in this chapter, India has entered into mutual legal assistance treaties (MLATs) for the purpose of intelligence sharing and aiding investigations. The MLAT agreements that India has entered into are publicly available, but the Memorandum of Understanding (MOU) agreements for international cooperation for investigative purposes are not publicly available⁶⁹.

As in the Necessary and Proportionate principle of *Safeguards for International Cooperation*⁷⁰, it is recommended that the Indian surveillance regime should ensure that when entering into an MLAT or MOU with another country, where the laws of more than one state could apply to communications surveillance, the available standard with the higher level of protection for individuals is applied. All agreements entered into should be clearly documented, publicly available, and subject to guarantees of procedural fairness.

Mechanisms and protections for whistleblowers

The Indian surveillance regime presently does not provide protection or immunity to whistleblowers exposing unauthorized or extralegal surveillance. Furthermore, there is no established mechanism for whistleblowers to report such instances.

As in the Necessary and Proportionate principle of *safeguards against illegitimate access*⁷¹ it is recommended that the Indian surveillance regime establishes a mechanism for whistleblowers to report information and to provide legal protection to whistleblowers.

Comprehensive transparency mechanisms

The Indian surveillance regime does not incorporate transparency mechanisms. Due to this, information about the surveillance practices of the Indian Government that reach the public domain is unofficial or based on leaked information.

As in the necessary and proportionate principle of *transparency and public oversight*⁷² it is recommended that the Indian surveillance regime incorporates the following transparency mechanisms:

- Transparency about the use and scope of communications techniques and powers, including the publication of the number of requests approved and rejected, disaggregation of the requests by service provider, investigation type, and purpose
- Transparency of the laws permitting communications surveillance
- Transparency of the requirements that service providers must comply with, with respect to communications surveillance
- Transparency of procedural components of surveillance to the extent possible,

⁶⁹Central Bureau of Investigation – India, *MLATs*, <http://cbi.nic.in/interpol/mlats.php>

⁷⁰Electronic Frontier Foundation, Privacy International & Access, “*International Principles on the Application of Human Rights to Communications Surveillance*”, Necessary & Proportionate, 10 July 2013, <https://www.eff.org/files/necessaryandproportionatefinal.pdf>

⁷¹Ibid

⁷²Ibid

including the process of giving surveillance powers to different authorities/departments, development of new surveillance schemes and powers, acquisition and development of surveillance technology

- Transparency by allowing service providers to publish the procedures they apply when dealing with state communications surveillance
- Establishment of an independent oversight mechanism to ensure transparency and accountability of communications surveillance, including accountability as to whether the Indian Government has been transparently and accurately publishing information about the use and scope of communications surveillance techniques and powers. This oversight mechanism should be in addition to any oversight already provided through another branches of government

Transparency of agencies/ departments authorised to surveil and scope of powers

India has a number of agencies and governmental departments that have powers to conduct different types of surveillance, such as interception and monitoring, yet the scope of their surveillance powers is unclear.

It is recommended that all bodies legally authorized to conduct surveillance, along with their respected scope of powers, are made transparent to the public.

Comprehensive and expanded scope of Review Committee

The Indian surveillance regime has established a Review Committee under the Indian Telegraph Act, 1885.⁷³ This Review Committee oversees orders issued under the Indian Telegraph Act and the Information Technology Act to determine the legality and validity of interception, monitoring, decryption, and collection of traffic data orders. The Review Committee has the power to revoke a surveillance order if it is determined to be extra-legal and order the destruction of any information collected, intercepted, or monitored under that order.

As in the Justice AP Shah principle of *Accountability*⁷⁴ it is recommended that the scope of the Review Committee duties be expanded to oversee all types of surveillance orders under existing legislation (interception, monitoring, decryption, collection of traffic data, access, tracing) and to:

- Ensure accountability and oversight of authorizing authorities
- Ensure accountability and oversight of intelligence agencies

Harmonization and strengthening of authorization process

The surveillance regime in India has a number of different authorization processes, different authorities, and different requirements for application of a surveillance order. These practices vary on the type of surveillance, as illustrated in the tables below.

⁷³Government of India, Ministry of Communications and Information Technology, Department of Telecommunications, *Indian Telegraph Act, 1885*, <http://www.ijlt.in/pdffiles/Indian-Telegraph-Act-1885.pdf>

⁷⁴Justice Ajit Prakash Shah, Former Chief Justice, High Court of Delhi, “*Report of the Group of Experts on Privacy*”, Planning Commission (CIT&I Division), Government of India, 16 October 2012, http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf

to access information by other means

Orders for a particular subject

Specified use of intercepted message
Name and designation of receiving officer

As in the Necessary and Proportionate principles of *Proportionality* and *Competent Judicial Authority*⁷⁵, it is recommended that the authorization process for surveillance in India is harmonized and strengthened. Specifically:

- Any order for any type of surveillance should come from an independent, impartial, and competent authority. Though the principle recommends that this authority be judicial, the realities of India's judicial system and the need for often immediate response to authorization requests has raised questions as to whether a judge is the best authority to vest these powers in
- For all instances of surveillance the law must require that prior to the issuance of a surveillance order, it must be established and demonstrated that:
 - There is a high degree of probability that a serious crime has been or will be committed
 - Other available less invasive investigative techniques have been exhausted, information accessed will be confined to that reasonably relevant to the crime alleged and any excess information collected will be properly destroyed or returned, information is accessed only by the specified authority and used for the purpose for which authorisation was given
 - The surveillance is necessary for achieving a legitimate aim
- All authorities responsible for authorizing surveillance must possess knowledge and the capacity to make determinations on the legality of surveillance, the use of such technologies, and the impact on human rights

⁷⁵ Electronic Frontier Foundation, Privacy International & Access, “*International Principles on the Application of Human Rights to Communications Surveillance*”, Necessary & Proportionate, 10 July 2013, <https://www.eff.org/files/necessaryandproportionatefinal.pdf>