PRIVACY INTERNATIONAL

Stakeholder Report
Universal Periodic Review
27th Session – India

The Right to Privacy in India

Submitted by Centre for Internet and Society India and Privacy International

October 2016

PRIVACY INTERNATIONAL

Submitted by Centre for Internet and Society India and Privacy International

October 2016

Introduction

1. This stakeholder report is a submission by Centre for Internet and Society India (CIS India) and Privacy International (PI). CIS is a non-profit organisation that undertakes interdisciplinary research on internet and digital technologies from policy and academic perspectives. Through its diverse initiatives, CIS explores, intervenes in, and advances contemporary discourse and practices around internet, technology and society in India, and elsewhere. PI is a human rights organisation that works to advance and promote the right to privacy and fight surveillance around the world.

2. CIS and PI wish to bring concerns about the protection and promotion of the right to privacy in India before the Human Rights Council for consideration in India's upcoming review.

The right to privacy

3. Privacy is a fundamental human right, enshrined in numerous international human rights instruments.[1] It is central to the protection of human dignity and forms the basis of any democratic society. It also supports and reinforces other rights, such as freedom of expression, information and association.

4. Activities that restrict the right to privacy, such as surveillance and censorship, can only be justified when they are prescribed by law, necessary to achieve a legitimate aim, and proportionate to the aim pursued.[2]

5. As innovations in information technology have enabled previously unimagined forms of collecting, storing and sharing personal data, the right to privacy has evolved to encapsulate State obligations related to the protection of personal data.[3] A number of international instruments enshrine data protection principles,[4] and many domestic legislatures have incorporated such principles into national law.[5]

1 Universal Declaration of Human Rights Article 12, United Nations Convention on Migrant Workers Article 14, UN Convention of the Protection of the Child Article 16, International Covenant on Civil and Political Rights, International Covenant on Civil and Political Rights Article 17; regional conventions including Article 10 of the African Charter on the Rights and Welfare of the Child, Article 11 of the American Convention on Human Rights, Article 4 of the African Union Principles on Freedom of Expression, Article 5 of the American Declaration of the Rights and Duties of Man, Article 21 of the Arab Charter on Human Rights, and Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms; Johannesburg Principles on National Security, Free Expression and Access to Information, Camden Principles on Freedom of Expression and Equality.

2 Universal Declaration of Human Rights Article 29; General Comment No. 27, Adopted by The Human Rights Committee Under Article 40, Paragraph 4, Of The International Covenant On Civil and Political Rights, CCPR/C/21/Rev.1/Add.9, November 2, 1999; See also Martin Scheinin, "Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism," 2009, A/HRC/17/34.

3 Human Rights Committee general comment No. 16 (1988) on the right to respect of privacy, family, home and correspondence, and protection of honour and reputation (art. 17)
See: A/HRC/WG.6/13/MAR/3, para. 37

4 See the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (No. 108), 1981; the Organization for Economic Co-operation and Development Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data (1980); and the Guidelines for the regulation of computerized personal data files (General Assembly resolution 45/95 and E/CN.4/1990/72)

5 As of December 2013, 101 countries had enacted data protection legislation.
See: David Banisar, National Comprehensive Data Protection/Privacy Laws and Bills 2014 Map (January 28, 2014). Available at SSRN:http://ssrn.com/abstract=1951416 or http://dx.doi.org/10.2139/ssrn.1951416

6. Privacy also has implication for the freedom of opinion and expression. The Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression emphasises that the "right to privacy is often understood as an essential requirement for the realization of the right to freedom of expression. Undue interference with individual's privacy can both directly and indirectly limit the free development and exchange of ideas."[6]

Follow up to the previous UPR

7. There was no mention of the right to privacy within the context of communication surveillance and data protection in the National Report submitted by India.

8. The right to privacy was not raised as an issue of concern either by UN Members States nor external stakeholders.

Domestic laws related to privacy

9. The Constitution of India does not specifically guarantee a right to privacy, however through various judgements over the years the Courts of the country have interpreted the other rights in the Constitution to be giving rise to a (limited) right to privacy – primarily through Article 21 – the right to life and liberty. In 2015, this interpretation was challenged and referred to a larger Bench of the Supreme Court (the highest Court in the country) in the writ petition Justice K.S Puttaswamy & Another vs. Union of India and Others, the case is currently pending in the Supreme Court.

10. The constitutional right to privacy in India is subject to a number of restrictions. These restrictions have been culled out through the interpretation of various provisions and judgements of the Supreme Court of India:

    - The right to privacy can be restricted by procedure established by law which procedure would have to be just, fair and reasonable (Maneka Gandhi v. Union of India);

    - Reasonable restrictions can be imposed on the right to privacy in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence; (Article 19(2) of the Constitution of India, 1950)
    - The right to privacy can be restricted if there is an important countervailing interest which is superior (Gobind v. State of M.P.);

6 A/HRC/23/40

- The right to privacy can be restricted if there is a compelling state interest to be served (Gobind v. State of M.P.);

- The protection available under the right to privacy may not be available to a person who voluntarily thrusts her/himself into controversy (R. Rajagopal v. Union of India).

- Like most fundamental rights in the Indian Constitution, the right to privacy has been mostly interpreted as a vertical right applicable only against the State, as defined under Article 12 of the Constitution, and not against private citizens. (Zoroastrian Cooperative Housing Society v District Registrar)

11. India does not have a comprehensive privacy legislation and limited data protection standards can be found under section 43A and associated Rules in the Information Technology Act 2000.

International obligations

12. India has ratified the International Covenant on Civil and Political Rights ('ICCPR'). Article 17 of the ICCPR provides that "no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation". The Human Rights Committee has noted that states party to the ICCPR have a positive obligation to "adopt legislative and other measures to give effect to the prohibition against such interferences and attacks as well as to the protection of this right [privacy]."[7]

Areas of concern

I. Communications surveillance

Broad and fragmented standards for surveillance

13. Communication surveillance in India is primarily regulated by two different statutes, the Telegraph Act, 1885 ("Telegraph Act") (which deals with interception of calls) and the Information Technology Act, 2000 ("IT Act") (which deals with interception of electronic data).

14. Before 1996, the state authorities relied upon the provisions of the Telegraph Act to carry out interception of phone calls. The Act allows any authorized public official to intercept communications on the occurrence of any public emergency or in the interest of public safety.[8] Communications can be intercepted under the Telegraph Act during "public emergencies" or

7 General Comment No. 16 (1988), para. 1
8 Section 5(2) of the Indian Telegraph Act, 1885

in the interest of "public safety" provided that such interception is in the interests of certain other grounds, namely, the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order and for preventing the incitement of offences. Such broad and vague justifications for surveillance have become a feature of many jurisdictions. The concept of national integrity or security are usually defined very broadly and are vulnerable to misuse as a means to target certain kinds of actors and propagate unnecessary secrecy around law enforcement measures, thus, having an adverse impact on transparency and accountability.[9]

15. However, in 1996 the Supreme Court noticed the lack of procedural safeguards in the provisions of the Telegraph Act and laid down certain guidelines for interceptions. These guidelines formed the basis of the Rules defining the procedures of interception that were codified by introducing Rule 419A in the Telegraph Rules in 2007. These guidelines were, in part also reflected in the Rules prescribed under the IT Act in 2009.

16. Section 69 of the IT Act allows for the interception, monitoring and decryption of digital information in the interest of the sovereignty and integrity of India, of the defence 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 offense. While this provision is similar to interception provision under the Telegraph Act mentioned above, it is noteworthy that it dispenses with the sine qua non of "the occurrence of public emergency of the interest of public safety", thus dramatically broadening the ambit of powers. The rules framed under Section 69 and 69B[10] (the "IT Interception Rules") include safeguards stipulating who may issue directions of interception and monitoring, how such directions are to be executed, the duration they remain in operation, to whom data may be disclosed, confidentiality obligations of intermediaries, periodic oversight of interception directions by a Review Committee under the Indian Telegraph Act, the retention of records of interception by intermediaries and to the mandatory destruction of information in appropriate cases. Rule 3 allows the "competent authority" to issue directions for monitoring for any of a number of specified purposes related to cyber security.

17. Access to stored data is also potentially addressed under Section 91 of the Code of Criminal Procedure, 1973 ("Cr.P.C.") which states that a Court in India or any officer in charge of a police station may summon a person to produce any document or any other thing that is necessary for the purposes of any investigation, inquiry, trial or other proceeding under the Cr.P.C. Thus, theoretically, under section 91, law enforcement agencies in India can access stored data. Section 92 of the Cr.P.C. also allows District Magistrates and Courts to issue directions requiring document, parcel or "things" within the custody of any postal or telegraph authority to be

9 A/HRC/23/40
10 The Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.

produced before it if needed for the purpose of any investigation, inquiry, trial or other proceeding under the Code. There is little judicial clarity on the subject but it may be argued that it is possible to interpret the provisions in a way that even private ISPs can be considered as postal or telegraph authorities and thus become subject to interception under this section.

18. Although there is broad symmetry between the legislations, there are still important differences as to when surveillance can be undertaken under the Information Technology Act, 2000 vis-à-vis the Indian Telegraph Act, 1885.

19. In 2012, a group of experts was appointed by the government to identify privacy issues and prepare a paper to inform a Privacy legislation in India.[11] As part of their report, the Group of Experts undertook a review of the Telegraph Act and Information Technology Act noting that that there were clear inconsistencies with regards to: "permitted grounds,", "type of interception," "granularity of information that can be intercepted," the degree of assistance from service providers, and the "destruction and retention" of intercepted material. The report of the Group of Experts concluded that these discrepancies, "have created an unclear regulatory regime that is non-transparent, prone to misuse, and that does not provide remedy for aggrieved individuals."[12]

Broad access obligations imposed on service providers

20. The Department of Telecommunication simplified the licensing regime by releasing a unified license agreement to allow telecom companies in India to offer services (mobile, fixed line, Internet and long-distance calls and other telecom services) through a single license, delinking spectrum from future licenses.[13] The UAS License Agreement has also been amended from time to time.[14]

21. Whilst many provisions in various licensing agreements provide strong safeguards for data protection of subscriber data, prohibit unlawful and mass surveillance and provide for robust penalties, contradictorily there are numerous legal and technical provisions which compel service providers to facilitate surveillance directly or indirectly.[15] Reflecting on this issue various jurisdictions the UN Special Rapporteur on freedom of expression noted that the practice of mandating broad access to communications data held by communications services providers through licenses necessary to provide such services gives the state a "carte blanche access to communications data with little oversight or regulation."[16]

11 "Report of the Group of Experts on Privacy", Planning Commission of India, 7: 19, October 16, 2012, http:// planningcommission.nic.in/reports/genrep/rep_privacy.pdf
12 "Report of the Group of Experts on Privacy", Planning Commission of India, 7: 19, p. 60-61, October 16, 2012, http:// planningcommission.nic.in/reports/genrep/rep_privacy.pdf
13 Available at: http://pib.nic.in/newsite/erelease.aspx?relid=84613
14 Available at: http://cis-india.org/internet-governance/blog/uas-license-agreement-amendment
15 Xinou, M., Policy Recommendations for Surveillance Law in India and an Analysis of Legal Provisions on Surveillance in India and the Necessary & Proportionate Principles, CIS. Available at: http://cis-india.org/internet-governance/blog/policy-recommendations-for-surveillance-law-in-india-and-analysis-of-legal-provisions-on-surveillance-in-india-and-the-necessary-and-proportionate-principles.pdf, pp. 15
16 A/HRC/23/40

Obligation to Install Hardware for Interception

22. Under the ISP License[17] the licensee is required to install the equipment that may be prescribed by the government for monitoring purposes. The UASL License[18] requires the licensee to install the necessary hardware/ software to enable the government to monitor simultaneous calls. As per the ISP License[19] and the UASL[20], in case of remote access of information, the licensee is required to install suitable technical devices enabling the creation of a mirror image of the remote access information for monitoring purposes.[21] The CMTS License Agreement[22] requires the installation of "necessary facilities" to aid the interception of messages by service providers.[23] However, it remains unclear what "necessary facilities" constitute, as well as what type of monitoring equipment would generally be used for such purposes.[24]

Disclosure of Call Record Details

23. The Unified License (Access Services) Agreement[25] requires service providers to disclose Call Data Records to law enforcement agencies.[26] However, the conditions for such disclosure are not specified. Though it is likely that a Court would read the conditions in the Telegraph Act and the IT Act into this clause, but not specifying the conditions here leaves it open for law enforcement agencies to put pressure on service providers into disclosing information which may not be allowed under law. Furthermore, the Unified License (Access Services) Agreement[27] requires service providers to provide the geographical location of any subscriber to law enforcement agencies at any given point of time.[28] 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.

17 Clause 34.4 and Clause 41.7 of the ISP License
18 Clause 41.10 of the UASL License
19 Clause 34.28(xiv) of the ISP License
20 Clause 41.20 (xiv) of the UASL
21 Vodafone, Law Enforcement Disclosure Repor, Updated Legal Annexe, February 2015. Available: https://www.vodafone.com/content/dam/sustainability/2014/pdf/operating-responsibly/law_enforcement_disclosure_report_2015_update.pdf, pp. 48
22 Available at: http://www.wipo.int/edocs/lexdocs/laws/en/in/in098en.pdf
23 Government of India, Ministry of Communications and Information Technology, Department of Telecomunications, License Agreement for Provision of Cellular Mobile Telephone Service, 1994, http://www.usof.gov.in/usof-cms/tender/cmtsAGREEMENT.pdf
24 Xinou, M., Policy Recommendations for Surveillance Law in India and an Analysis of Legal Provisions on Surveillance in India and the Necessary & Proportionate Principles, CIS. Available at: http://cis-india.org/internet-governance/blog/policy-recommendations-for-surveillance-law-in-india-and-analysis-of-legal-provisions-on-surveillance-in-india-and-the-necessary-and-proportionate-principles.pdf, pp. 10
25 Clause 41.12 of the Unified License (Access Services) Agreement
26 Government 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
27 See: http://www.wipo.int/edocs/lexdocs/laws/en/in/in098en.pdf
28 Ibid

Provision of Mirror Image for Monitoring

24. Lastly, the Unified License (Access Services) Agreement[29] 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 purposes.[30] 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.

25. The UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression has highlighted concerns of the increasing, sometime complicit role, of the private sector in facilitating unlawful surveillance.[31] He noted that the private sector must be able "to carry out its functions independently in a manner that promotes individual's human rights"[32]. In his 2016 report, the Special Rapporteur also noted how "state capacity to conduct surveillance may depend on the extent to which business enterprises cooperate with or resist such surveillance".[33] He recommend that "Access to communications data held by domestic corporate actors should only be sought in circumstances where other available less invasive techniques have been exhausted"[34] and "States must refrain from forcing the private sector to implement measures compromising the privacy, security and anonymity of communications services, including requiring the construction of interception capabilities for State surveillance purposes or prohibiting the use of encryption."[35]

Lack of judicial authorisation for surveillance orders

26. In India, neither the Telegraph Act nor the Information Technology Act provide for judicial authorisation or oversight of surveillance. According to Rule 419A of the Telegraph Rules, the interception of any message or class of messages can only be done by an order of the Secretary of the Ministry of Home Affairs at the Central level and the Secretary of the Home Department at the State level. In emergency cases interception may to be carried out with the prior approval of the Head or the second senior most officer of the authorised security agency at the Central Level and with the approval of officers authorised in this behalf not below the rank of Inspector General of Police, at the State Level.[36]

29 Clause 41.26(xiv) of the Unified License (Access Services) Agreement
30 Ibid
31 A/HRC/23/40
32 Ibid, para 77
33 A/HRC/32/38, para. 57
34 Ibid, para 85
35 Ibid, para 96
36 1) in remote areas, where obtaining of prior directions for interception of messages or class of messages is not feasible; or 2) for operational reasons, where obtaining of prior directions for interception of message or class of messages is not feasible

27. According to the IT Interception Rules, only the competent authority can issue an order for the interception, monitoring or decryption of any information generated, transmitted, received or stored in any computer resource under sub-section (2) of section 69 of the Information Technology Act.[37] At the State and Union Territory level, the State Secretaries respectively in charge of the Home Departments are designated as "competent authorities" to issue interception directions.[38] In unavoidable circumstances the Joint Secretary to the Government of India, when so authorised by the Competent Authority, may issue an order. Interception may also be carried out with the prior approval of the Head or the second senior most officer of the authorised security agency at the Central Level and at the State Level with the approval of officers authorised in this behalf not below the rank of Inspector General of Police, in the emergent cases.[39]

28. Judges are best suited to apply the legal tests that ensure that any interference with the right to privacy carried out by intelligence or security agencies complies with the principles of necessity and proportionality. There is growing recognition by international experts and by national laws that surveillance should only be carried out on the basis of a judicial order.[40] The judicial authority should also ensure that any surveillance carried out is in compliance with such order and, more broadly, respect the right to privacy.

Lack of comprehensive and independent oversight of state surveillance

29. The Rules under the Telegraph Act envisage the constitution of a Review Committee which has the Cabinet Secretary as its Chairman and the Secretary to the Government in charge of Legal Affairs and the Secretary to the Department of Telecom as its members. This Review Committee is also mandated to oversee the application of the Rules established under section 69 of the IT Act. Every order of interception monitoring or decryption under the Telegraph Act as well as the IT Act shall be sent to the Review Committee within 7 days and the Review Committee is to meet at least once every two months at the central/state level and must validate the legality of order. The committee has the authority to revoke orders and destroy copies of the intercepted message or class of message.

30. The Review Committee which acts as a check on the misuse of powers by the competent authorities is a very important cog in the entire process. However, it is staffed entirely by the executive and does not have any members of any other background. Whilst it is probably impractical to have civilian members in the Review Committee which has access to potentially

37 Rule 3, Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.
38 Rule 2(d), Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.
39 1)in remote areas, where obtaining of prior directions for interception or monitoring or decryption of information is not feasible; or 2) for operational reasons, where obtaining of prior directions for interception or monitoring or decryption of any information generation, transmitted, received or stored in any computer resource is not feasible,
40 See U N High Commissioner for Human Rights' report on the right to privacy in the digital age, UN doc. A/HRC/27/37, 30 June 2014.

sensitive information, it is extremely essential that the Committee has wider representation from other sectors specially the judiciary. One or two members from the judiciary on the Review Committee would provide a greater check on the workings of the Committee as this would bring in representation from the judicial arm of the State so that the Review Committee does not remain a body manned purely by the executive branch. This could go some ways to ensure that the Committee does not just "rubber stamp" the orders of interception issued by the various competent authorities.

31. While the interception activities of the police and intelligence agencies in India must be carried out in accordance with the procedures contained in the Telegraph Act, 1885 and the Information Technology Act, 2000 and the Rules framed under those legislations, non-interception access as well as passive interception surveillance by intelligence agencies is not governed by these legislations. It is possible that these capabilities may be governed by internal guidelines or operation manuals, etc. of individual agencies, but these are not easily available public.

Lack of comprehensive accountability of law enforcement and intelligence agencies

32. In India, there are at least sixteen[41] different intelligence agencies that have been established. Intelligence agencies in India are often established via executive orders and most of the intelligence agencies in India do not have clearly established oversight mechanisms other than the departments that they report to. For example, CBI and RAW report to the Prime Minister's Office, Directorate of Revenue Intelligence reports to the Finance Ministry, and the Military Intelligence agencies report to the Ministry of Defence. As such, intelligence agencies do not come under the purview of Parliament, the Right to Information Act, and their functions are not subject to audit by the Comptroller and Auditor General – despite many agencies being funded from the Consolidated Fund of India.

33. While the Rules under the Telegraph Act provide for major penalties for cases of unauthorized surveillance, which can include imprisonment and even cancellation of the telecom license, however these penalties are only specified for the service providers or private individuals and do not cover the enforcement agencies. The penalty for law enforcement agents who conduct unauthorized surveillance is imprisonment which may extend to three years or a fine.

41 National Technical Research Organisation; Research and Analysis Wing (R&AW); The Aviation Research Centre (ARC) and the Radio Research Centre (RRC), which are a part of the Research and Analysis Wing (R&AW); Electronics and Technical; Services (ETS), which is the ELNIT arm of R&AW; Intelligence Bureau; Narcotics Control Bureau; Directorate of Revenue Intelligence; Central Economic Intelligence Bureau; Central Bureau of Health Intelligence; Defence Intelligence Agency; Joint Cipher Bureau; Signals Intelligence Directorate; Directorate of Air Intelligence; Directorate of Navy Intelligence; Directorate of Military Intelligence; Directorate of Income Tax (Intelligence and Criminal Investigation); Directorate General of Income Tax Investigation and Joint Intelligence Committee (JIC)

34. The Rules under the IT Act specify that any person who indulges in unauthorized interception shall be punished as per the provisions of law. However, the Information Technology Act does not provide for a penalty specifically for unauthorized interception, which means that these acts will have to be brought under some other provisions of the statute (which is still an argument untested in court) or under the "catch-all" provision of section 45 which provides for a maximum penalty of Rs. 25,000/-.

Lack of transparency of state surveillance

35. While as per Rule 419A (15) of the Indian Telegraph Rules, 1951 and Rule 21 of the IT Interception Rules, service providers are required to maintain the secrecy and confidentiality of the intercepted information, there does not appear to be any specific prohibition on them disclosing the number of surveillance orders issued in an aggregate form. In practice though, it appears that some service providers interpret the requirement of secrecy to extend to aggregate information regarding interception orders as in Vodafone's 2014 'Disclosure Report'[42] the company noted that as per law it could not disclose information on the interception of communications and access to communications data.

Blanket subscriber registration for use of postpaid, prepaid, and public wifi services

36. According to the Unified Access Service (UAS) license, service providers are required to maintain a subscriber database and require proof of identity and address when issuing SIMs to individuals.[43]

37. In light of national security concerns around the misuse of public Wi-Fi, the Department of Telecommunication, Government of India, published a regulation dated February 2009, defining procedures for the establishment and use of public Wi-Fi to prevent misuse of public Wi-Fi and to be able to track the perpetrator in case of abuse. In this, the DOT has stated that "Insecure Wi-Fi networks are capable of being misused without any trail of user at later date". Regarding Wi-Fi services provided at public places, the Regulations state that "bulk login IDs shall be created for controlled distribution with authentication done through a centralized server. Individuals using public Wi-Fi are required to register with a temporary user ID and password and must submit a copy of photo identity to the provider which is to be maintained for one year and receive details of a user ID and password via SMS on their mobile phone." Which implies that users are required to register using their mobile phones to use public Wi-Fi and no new connections will be activated before the subscriber's details are registered by the ISP.

42 Vodafone, Country-by-country disclosure of law enforcement assistance demands. Available at: https://www.vodafone.com/content/sustainabilityreport/2014/index/operating_responsibly/privacy_and_security/law_enforcement/country_by_country.html

43 UAS license section 41.10

Broad Data Retention Standards

38. In India, multiple legal provisions and regulations provide for mandatory data retention measures by service providers.

39. Service providers are required to collect the following information: called/ calling party, location, telephone numbers of call forwarding, data records of failed call attempts, and call data records (UAS license section 41.10).

40. The Information Technology (Guidelines for Cyber Café) Rules, 2011 established under section 79(2) of the ITA provide regulations for the maintenance of user records by cyber cafés. Under Rule 4(2) of these Rules[44], cyber cafes are required to retain copies of user identification for a period of one year. Section 5 of the Rules requires cyber cafes to retain logs of user information and browsing history for a period of one year. If requested by authorized authorities, Cyber Café owners must provide the requested documents.[45]

41. Under section 3(4) of the Information Technology (Intermediary Guidelines) Rules 2011[46], intermediaries are required to retain content that has been removed and associated information for a period of 90 days.

42. These measures are in place to ensure mandatory data retention requiring services providers to "collect and preserve communications content and information about users' online activities." Such provisions are indiscriminate in their nature and expensive, and increase the scope of state surveillance.[47] There could be significant interference with the rights of individuals caused by a regime that requires companies to retain immense quantities of their communications data, not based on reasonable suspicion. Various human rights experts and institutions have maintained that laws that impose blanket, indiscriminate retention of personal data violate the right to privacy.

II. Data protection

Lack comprehensive Privacy Legislation

43. India is yet to enact a comprehensive data protection framework. Since 2010, starting with an Approach Paper on Privacy, and the Report the Group Experts on Privacy, India has been considering enacting a privacy legislation. Within this legal void, the strongest legal protection provided to personal information in India is through section 43A of the IT Act and the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011[48] ("Data Protection

44 See: http://meity.gov.in/sites/upload_files/dit/files/GSR315E_10511(1).pdf
45 See: http://meity.gov.in/sites/upload_files/dit/files/GSR315E_10511(1).pdf
46 See: http://meity.gov.in/sites/upload_files/dit/files/GSR314E_10511(1).pdf
47 A/HRC/23/40
48 Available at: http://www.wipo.int/edocs/lexdocs/laws/en/in/in098en.pdf

Rules") issued thereunder. Section 43A requires a body corporate who receives, possesses, stores, deals, or handles any 'sensitive personal data' to implement and maintain 'reasonable security practices', failing which, they are held liable to compensate those affected.

Lack of data protection standards for the public sector

44. Section 43A and associated Rules apply only to "body corporates", thus not extending the same requirements to the public sector. The lack of a comprehensive data protection policy that is applicable to the public sector is particularly concerning giving the numerous government led data-driven initiatives which have already been implemented and others that are emerging in India including Digital India, the Unique Identity Scheme, and the National Population Register. The intent of these schemes is to register all residents of the country and provide them with unique identifiers,[49] seeding of different databases (feeding information into the database) with unique identifiers,[50] and enable the implementation of large e-governance projects,[51] all of which will involve collection of vast amount of personal data. The absence of any regulation governing the collection, use and sharing of such data leads to serious privacy concerns.[52]

Limited scope of data protection standards

45. Section 43A and associated Rules apply to personal and sensitive personal data. Given the dynamic nature of data, the generation of new forms of data and data sources, and the evolving nature of data, the limited scope of these Rules is concerning.

Limited Definition of Personal Sensitive Data

46. The Rules apply to personal information and sensitive personal information. Personal information is defined as ""Personal information" means any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person." Rule 3 of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 defines "sensitive personal data or information" as (i) password; (ii) financial information such as Bank account or credit card or debit card or other payment instrument details; (iii) physical, physiological and mental health condition; (iv) sexual orientation; (v) medical records and history; and (vi) Biometric information. This rule follows from the principle that "certain kinds

49 See: https://uidai.gov.in/beta/about-uidai/about-uidai/vision-mission.html
50 See: https://uidai.gov.in/images/aadhaar_seeding_june_2015_v1.1.pdf
51 See: http://www.digitalindia.gov.in/
52 Press Trust of India, US academics raise privacy concerns over 'Digital India' campaign, Your Story, 31 August 2015. Available at: http://yourstory.com/2015/08/us-digital-india-campaign/

of personal information are particularly sensitive, due to the intimate nature of their content in relation to the right to privacy".[53] However, this definition is inadequate as it does not include electronic communications such as emails, browsing and chat logs within its scope. With increased penetration of Information and Communication Technologies, there is a greater need for electronic communication to also be included within the ambit of sensitive personal data or information. Since these Rules provide for regulations only for "sensitive personal data" therefore other kinds of data which does not fit into the definition such as chat logs, emails, etc. will not be granted the level of protection that is given to "sensitive personal data".

Lack of comprehensive and technically appropriate consent mechanisms

47. Rule 5 of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 lays down the requirements for consent of the data subject to be taken in writing before the collection of sensitive personal data. The provision fails to mandate that the data collectors ensure that the consent provided is informed, explicit and freely given and address technical forms of obtaining consent. Further, this Rule applies only to sensitive personal data or information and not all kinds of personally identifiable information, thus, significantly narrowing the application of consent before collection of personal data.[54]

53 CIS India, Comments on the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, 13 March 2013. Available at: http://cis-india.org/internet-governance/blog/comments-on-the-it-reasonable-security-practices-and-procedures-and-sensitive-personal-data-or-information-rules-2011

54 Ibid

Recommendations

48. We recommend that the Government of India:

- Harmonise the legal framework which regulate communications surveillance in India to ensure that the law is accessible and clear, and meets India's international human rights obligations;

- Establish an independent and effective oversight mechanism with a mandate to monitor all stages of interceptions of communications to ensure they are compliant with India's domestic and international obligations to respect and protect the right to privacy and other human rights;

- Establish independent accountability mechanisms and clear standards for India's security and intelligence agencies to ensure they are subject to independent oversight mechanisms and guarantee transparency of their mandate and operations in accordance with international human rights standards;

- Review and reform the regulations regarding export and import of surveillance technologies to and from India;

- Review all licensing agreements which impose obligations on the private sector to facilitate and/or conduct communication surveillance, and take the necessary measures to ensure that the private sector – in both policy and practice – comply with international human rights law and standards;

- Review the proportionality of data retention requirements placed on telecommunications companies;

- Adopt and enforce a comprehensive data protection legal framework that meets international standards, applies to both the private and public sector, and establish an independent data protection authority that is appropriately resourced and has the power to investigate data protection breaches and order redress.