Government access to private-sector data in India

Sunil Abraham*, and Elonnai Hickok

Abstract

- India does not have many laws that explicitly prescribe or prohibit systematic government access to private-sector data apart from some provisions in laws such as the Information Technology Act, Prevention of Money Laundering Act, and the Epidemic Diseases Act.
- Security consultants and employees of private-sector organizations impacted by such regulation who spoke under conditions of anonymity did not agree about the existence and scope of governmental access.
- While some security consultants paint a picture of comprehensive and unfettered access to databases of personal information, others claim strict adherence to the letter and spirit of the law, both in terms of proactive, reactive, and systematic access to data; the truth must lie somewhere in between.

The appetite in some parts of the government for access to information held by the private sector appears to be growing. In February 2012, the Intelligence Bureau (IB) wrote to the Department of Telecom demanding that telecom operators and Internet Service Providers (ISPs) cooperate to enable comprehensive real-time tracking of Internet usage on mobile phones. This included plans of an India-centric 'Skype'[1] for use by government officials and to address national security, and the establishment of a core group 'for finalization of Internet Protocol Detail Record (IPDR) for Internet services, and standardization of parameters that will have to be stored by mobile phone companies in a log.'[2] This is because apparently the telecom operators and ISPs were unable to identify mobile customers that had visited specific websites.

A month later, a national newspaper obtained documents revealing that the government was planning amendments to the operator licences to ensure real-time monitoring of 'location data' of all mobile phones.[3] Combined with large scale surveillance projects like the Unique Identity (UID),[4] National Intelligence Grid (NATGRID),[5] and the Central Monitoring System (CMS),[6] it would be fair to say that systematic access to private-sector data by the Indian government is increasing. Specifically, systematic access is growing in the mobile and IT sector in India; it is taking place through newly enacted legislation, policy amendments, projects, or outside the scope of legislation; it is being justified by reasons of national security and/or crime detection; and in practice there is a dilution and disconnect between policy and implementation. This essay provides an overview of the policies and practices around governmental access to information collected and held by the private sector.

For the sake of clarity, we divide governmental access into three categories: proactive, reactive, and systematic. By proactive access, we refer to those situations where the government is provided information by the private sector on a periodic basis, usually under a statute, delegated legislation, or executive order that

* Executive Director, The Centre for Internet & Society. Elonnai Hickok, graduated from the University of Toronto in 2012, and is now the Program Officer for Internet Governance at the Centre for Internet and Society.

1 An Indian centric Skype would mean that the server would be located in India.

2 *The Economic Times*, Intelligence Bureau want Telcos to keep eye on internet traffic on mobile phones. 23 February 2012, available at: <http://articles.economictimes.indiatimes.com/2012-02-23/news/31091065_1_phones-ip-internet-usage>accessed 28 July 2012.

3 A Sarkar, Soon, govt will keep track of where every mobile user. 16 February 2012, available at: <http://www.indianexpress.com/news/soon-govt-will-keep-track-of-where-every-mobile-user-is/912681/0> accessed 28 July 2012.

4 The UID is India's proposed National Identification scheme that will issue all residents a unique number based on their biometrics. The number is envisioned to become universal and used as an authenticator in all transactions.

5 NATGRID is a network that will allow access to 21 sets of data sources and allow access to 10 security agencies. See: http://www.deccanchronicle.com/360-degree/when-spies-connect-dots-708> accessed 27 August 2012.

6 The CMS is an interception network that will allow Security Agencies to intercept emails, cyber chats, monitor voice calls, SMS, etc. all in real time.

© The Author 2012. Published by Oxford University Press. All rights reserved. For Permissions, please email: journals.permissions@oup.com

Downloaded from https://academic.oup.com/idpl/article/2/4/302/676984 by guest on 11 April 2024

requires such routine and proactive disclosure. By reactive access, we refer to those situations where the government is provided information by the private sector only upon a specific request, usually under a statute, delegated legislation, or executive order that allows the government to seek such disclosure. Lastly, by systematic access, we refer to those situations where the government has real-time access to information held by the private sector.

National legal context and fundamental principles

In India, the Constitution establishes a federal structure of governance comprised of a central government and multiple national states. Both the central government and the states have various levels of legislative and executive authority. The Indian Constitution also establishes a framework for the judiciary that is comprised of the Supreme Court, High Courts, and subordinate courts that exist at the state and sub-state level. In this system courts are granted jurisdiction over issues found in both federal and state laws, while the higher judiciary is empowered to take decisions on constitutional issues. Additionally, a range of tribunals and special courts have been established with authority over specific sectoral issues.[7]

Statutory and regulatory overview

Provisions defining what information can be accessed by a government are typically found under specific sectoral legislation, and are indications of an intent to protect a right to privacy. Currently, in India there is no explicit or fundamental right to privacy and no horizontal privacy law. Instead, 50 policies (including statutes, rules, regulations, and executive orders) covering other subjects contain provisions which either implicitly or explicitly protect privacy rights.[8] In addition, the right to privacy has been read into the Constitution of India by the Supreme Court as a component of the right to life and personal liberty under Article 21. For example, recently the Indian Judicial system ruled in favour of a right to privacy in the Naz Foundation case. In this case, the Delhi High Court, read down Section 377 of the Indian Penal Code to de-criminalize homosexuality in India. A critical aspect of the ruling was the court's recognition of the citizen's fundamental right to privacy.[9] This case is currently being appealed in the Supreme Court of India.[10]

Between mid-2010 and September 2011 the Department of Personnel and Training (DoPT) and the Ministry of Law worked on several versions of a draft Privacy Bill. At least three versions of the draft bills have been leaked. Currently, the author is a member of a Committee established to compile a report that is to be published in the Fall of 2012, which could influence the drafting of the India Privacy Bill. When the Bill becomes law, it may serve as the umbrella legislation, defining key principles and instituting the office of the privacy commissioner. In the absence of such overarching privacy legislation, questions of jurisdiction and boundaries of governmental access to private-sector data are currently defined predominantly through sectoral policy. But not all sectors have addressed the question. For instance, there is no explicit policy or case law addressing government access to footage captured on CCTV cameras by private companies. Furthermore, there is little harmonization of practices and principles across different sectors. For example, in the financial sector, there are provisions that clearly limit governmental access to information held by private companies through safeguards such as limiting access to written requests,[11] while in the telecommunications sector the Government can access information real time and on a systematic basis.[12]

Laws allowing reactive access private-sector data to the government

In India, reactive access to private sector information by the government does not necessarily entail a complete bypassing of safeguards, but is enabled instead through bodies being vested with powers analogous to a civil court, generic application of provisions, extended data retention periods, broad collection of data, and lack of safeguards to specifically prevent reactive access from taking place. Three bodies of Indian

7 Id. P Iyengar, Country Report. The Centre for Internet and Society, 2011, p. 4; available at: <http://cis-india.org/internet-governance/country-report.pdf/view> accessed 6 July 2012.

8 See Privacy in India an Early Draft. Available at: <http://cis-india.org/internet-governance/privacy-in-india-draft-chapters> accessed 12 September 2012.

9 Naz Foundation. Case # 7455/2001. Para. 8; Judgment available at: <http://www.nazindia.org/judgement_377.pdf> accessed 6 July 2012.

10 Bar and Bench. Naz Foundation Update: SC begins hearing; Court says "the meaning is never constant, we have travelled sixty years". February 20th 2012. Available at: <http://barandbench.com/brief/2/2081/naz-foundation-update-sc-begins-hearing-court-says-quotthe-meaning-is-never-constant-we-have-travelled-sixty-yearsquot> accessed 12 September 2012.

11 As discussed in section "Banking Laws".

12 As discussed in section "Systematic access by law enforcement for reasons of national security".

Downloaded from https://academic.oup.com/idpl/article/2/4/302/676984 by guest on 11 April 2024

law that we have examined, enable information by the government include legislation pertaining to: traditional search and seizure, banking and securities, and health. Indian tax laws, customs laws, and companies laws also allows reactive access to private sector data to the government, but are not discussed in this article.

Search and seizure law

The government has always had generic access to information held by private entities via the technologically neutral Section 91 of The Code of Criminal Procedure, 1973 (CrPc), which empowers 'any court or any officer in charge of a police station' to issue a summons for the production of 'any document or other thing', and Section 92 which enables 'any Judicial or Executive Magistrate, commissioner of police, or District Superintendent of police' to 'require any document, parcel or thing in the custody of a postal or telegraph authority'.[13] Even today, law enforcement officials approach private-sector organizations using CrPc Section 91 and 92, instead of relevant sections under the appropriate legislation. However, access to communication information under section 92 of the CrPc is subject to judicial oversight, as a court order must be issued before accessing information, while access to documents under section 91 of the CrPc is possible using executive or judicial orders. Therefore, the generic use of section 91 transforms it into a policy tool that can be used for reactive. For example, anonymous sources that spoke to us from international Internet intermediaries have stated that the government has used section 91 to ask for payload information.[14] Because communication data requires a court order under section 92, the intermediaries only provide basic subscriber information and meta-data. But it is unclear if Indian intermediaries comply with these unlawful requests.

Securities law

Reactive access is also enabled by different bodies being vested with powers analogous to a civil court. The Securities and Exchange Board of India Act (1992)[15] establishes the Securities and Exchange Board of India (SEBI) to govern and regulate the use of individual's credit information.[16] In the Act, reactive access by the government is mediated through SEBI, which is empowered with broad access to private-sector data related to the securities market. For example, SEBI is vested with the same powers as a civil court,[17] and among other powers, has the ability to:

- determine what information is to be disclosed by companies
- require the production of account books and other documents
- call for information
- undertake inspection
- make inquiries into the stock exchanges and mutual funds of entities in the securities market as it sees fit for the purposes of protecting the interests of investors, promoting the development of, and regulating the securities market.[18]

As a safeguard to unauthorized reactive access, SEBI is permitted to undertake inspection only if it has reasonable grounds to believe that: a company has been indulging in insider trading or fraudulent, unfair trading practices are being used, transactions in securities are being dealt with in a manner detrimental to the investor, or an intermediary or any person associated with the securities market is contravening any provision in the Act.[19] The Act re-enforces reactive access to and disclosure of information by penalizing any person who fails to furnish the required information.[20]

Health law

The Persons with Disabilities (Equal Opportunities, Protection of Rights and Full Participation) Act 1995, among other things, provides for education, social security, creation of a barrier-free environment, and the reservation of job posts for persons with disabilities.[21] In doing so, the Act provides the government reactive access to personal information regarding individuals with disabilities. For example, to enable access to employment opportunities for the disabled, the Act establishes a body known as the Special Employment Exchange, which collects information relating to vacancies appointed for persons with disability.[22] The Act, allows any person who is authorized by the Special Em-

13 Code of Criminal Procedure, 1973 section 91 & 92, available at: <http://www.vakilno1.com/bareacts/crpc/Criminal-Procedure-Code-1973.htm>.

14 Payload information refers to the content of communications.

15 Securities and Exchange Board of India Act 1992, available at: <http://www.sebi.gov.in/acts/act15ac.pdf> accessed 28 July 2012.

16 Id. sect. 2((1) (a)) 'Board' means the Securities and Exchange Board of Indian established under section 3 of the Act.

17 Id. sect. 11 (2 (m)(3)).

18 Id. sects 11(2 (a))–11(2(m)).

19 Id. sects 11B - 11C.

20 Id. sect. 15A.

21 Persons with Disabilities (Equal Opportunities, Protection of Rights and Full Participation) Act (1995), available at: <http://www.unipune.ac.in/dept/Education_Extension/www/PWD.htm> accessed 28 July 2012.

22 Id. Definition x, Sect. 34.

Downloaded from https://academic.oup.com/idpl/article/2/4/302/676984 by guest on 11 April 2024

ployment Exchange, to access, inspect, question and copy any relevant record, document or information in the possession of any establishment.[23] Furthermore, the Act requires that every employer maintain a record pertaining to the individual with a disability that is employed. The contents of this record are to be prescribed by the government, and must be open for inspection by persons authorized by the a general or special order issued by the government.[24] Although it is not clear that access to this information by the government is violative of an individual's rights, the vague language used in the Act, along with the the lack of defined privacy principles regulating collected information, leaves the information open to potential abuse.

Reactive and systematic access by law enforcement for reasons of national security

Reactive and systematic access to information by authorized agencies[25] for reasons of national security can be found in India's internet and communications legislations. In India, provisions that enable reactive and systematic access for these reasons often (a) allow access for reasons of investigation, but with no explicit requirement of probable cause; (b) do not specifically require law enforcement or government agencies to produce a court or executive order for each case of access; (c) do not define or limit how the agency can use accessed information; (d) do not restrict the undertaking of the access to prespecified ranks of officials; (e) penalize the private entity for non-compliance with disclosure or access requests. For the private sector, the rules allowing reactive and systematic access are potentially harmful as they hold specific actors responsible for providing information to the government through penalty, while failing to provide a form of redress if an official abuses this power, or if the information is used for unauthorized purposes.

Internet law

The Information Technology Act (ITA) 2008 allows authorized agencies broad reactive access to personal information held by the private sector for investigation purposes. Unlike interception provisions, they do not establish grounds for access, for example national security. This expands the access possible, as it removes a critical safeguard. The following Sections and Rules are relevant:

1. Reasonable Security Practices and Procedures and Sensitive Personal Data or Information Rules 2011:20[26]

   Through these quasi data protection rules access is permitted by:

(a) Lowering standards for access by not requiring agencies authorized under law to gain prior, and case-case authorization for access, thus enabling blanket authorizations.[27] For example, although authorized agencies are required under law to state in writing the reason for requesting information,[28] they do not have to gain prior authorization from a court or executive body.[29]

(b) Allowing accessed information to be used for broad and generic purposes.[30] For example, authorized agencies are permitted to request access to any type of sensitive information, and when obtained, sensitive personal information may be used broadly for: 'verification of identity, prevention, detection, investigation including cyber incidents, prosecution, and punishment of offences.'[31]

2. Intermediaries Guidelines Rules 2011[32]

   These safe harbour Rules could allow for reactive access to personal information when used broadly by authorized agencies.[33] This is accomplished by:

(a) Requiring that information that has been taken down by an intermediary be retained for a period of 90 days.[34]

23 Id. Sect. 35.

24 Id. Sect. 37.

25 It is not entirely clear which governmental agencies are empowered to undertake wiretapping, but news items have listed agencies including: the Intelligence Bureau, Central Economic Intelligence Bureau, Directorate of Revenue Intelligence, Income Tax Department, Central Bureau of Investigations, Research Analysis Wing, the National Technical Research Organization, and the Enforcement Directorate. <http://www.livemint.com/2011/05/18002647/Govt-to-come-down-hard-on-unau.html> accessed 28 July 2012.

26 Section 43A. Reasonable Security Practices and Procedures and Sensitive Personal Data or Information Rules, 2011, available at: <http://www.mit.gov.in/sites/upload_files/did/files/GSR313E_10511%281%29.pdf>.

27 Id. sect. 6(1) 'The Government agency shall *send a request in writing to the body corporate possessing* the sensitive personal data or information stating clearly the purpose of seeking such information.'

28 Id. sect. 6(1).

29 This represents a dilution from traditional search and seizure procedure established under the Cr.Pc.

30 Id. sect. 6 (1) '. . . obtain information including sensitive personal data or information *for the purpose of verification of identity, or for prevention, detection, investigation including cyber incidents, prosecution, and punishment of offences* . . .'

31 Id. sect. 6(1).

32 ITA Section 79(2). Information Technology Intermediaries Guidelines Rules 2011, available at: <http://www.mit.gov.in/sites/upload_files/dit/files/GSR314E_10511%281%29.pdf> accessed 28 July 2012.

33 The Rules lay out procedures intermediaries must follow with respect to what content is allowed to be posted on the website. Among other things, intermediaries are responsibile for taking down content that is in contravention of the provision.

34 Id. sect. 3 (4).

Downloaded from https://academic.oup.com/idpl/article/2/4/302/676984 by guest on 11 April 2024

(b) Requiring that intermediaries provide any authorized agency information that is requested in writing.[35]

Thus, the provisions could facilitate reactive access by allowing a wide range of data to be taken down and subsequently retained for access by authorized agencies, while at the same time creating low standards as to which agencies can access the removed and retained information. For example, if a website is hosting information about sexual minorities, and an offended individual or the government sends a notice for the take down of the entire website, the website complies—removing and retaining the entire platform—it is unclear if authorized agencies now potentially have complete access to all information (log in, passwords, user Ids) stored on the website.

3. Guidelines for Cyber Cafe Rules[36]

This provision creates procedures for Cyber Cafes to follow, and facilitates reactive access and proactive disclosure to authorized agencies by requiring that Cyber Cafes to:

(a) Retain a copy of identification documents at the time of registration for at least one year.[37]

(b) Maintain a log register for at least one year. The log register must contain: name, 'address, gender, contact number type and detail of Id document, date, computer terminal identification, long in time, and log out time'.[38] The Cyber Cafe owner may also take a photo of a user for the purposes of establishing identity.[39] This photo will be kept in the log register. The log register must be disclosed to the registration agency or person identified by the registration agency on a monthly basis showing date-wise usage details of the computer resources.[40]

(c) Store and maintain backups for at least one year of log records for each user access including: history of accessed websites and logs of proxy servers.[41]

In addition to the extensive amount of information that is retained, reactive access is facilitated by the provision, because the rank of the official, the number of officials, and circumstances for who can access information and when information can be accessed is not set, and could be changeable according to authorization by the registering agency.[42]

Interception legislation

Governmental systematic access to data held by the private sector is facilitated through interception and access provisions found in the Code of Criminal Procedure, the Indian Post Office Act 1898, the Telegraph Act (TA) 1885, and the Information Technology Act (ITA) 2000.

Prior to 1997, there were no clear safeguards or standards for the interception of communications in India. The first safeguards are from the 1997 case *PUCL v Union of India*. In this case the Supreme Court of India held that the interception of communications was a violation of the constitutionally guaranteed right to life and personal liberty, unless permitted under the procedure established by law.[43] As part of the judgment the Supreme Court framed guidelines to be followed when intercepting telephone lines. The Central Government notified the Supreme Court's procedural safeguards as rules under the Telegraph Act. The rules state that: only a home secretary from the central or state government can authorize a wiretap;[44] requests for interception must specify how the information will be used;[45] each order unless cancelled earlier will be valid for 60 days and can be extended to a maximum of 180 days;[46] a review committee at the central/state level will validate the legality of the interception order;[47] before an interception order can be approved, all other possibilities of acquiring the information must be considered;[48] the review committee can revoke orders and destroy the data intercepted;[49] records pertaining to an interception order maintained by intelligence agencies

35 Id. sect. 3 (7).

36 ITA section 79(2). The Information Technology (Guidelines for Cyber Café) Rules 2011. Available at: <http://mit.gov.in/sites/upload_files/dit/files/GSR315E_10511%281%29.pdf> accessed 28 July 2012.

37 Id. sect. 4 (1) & sect. 4(2) At the time of registration the individual must provide an identification document. This could include: Photo Credit Card or debit card issued by a Bank or Post Office; or Passport; or Voter Identity Card; or Permanent Account Number (PAN) card issued by the Income Tax Authority; or Photo Identity Card issued by the employer or any Government Agency; Driving Licence issued by the Appropriate Government; or Unique Identification (UID) Number issued by the Unique Identification Authority of India (UIDAI).

38 Id sect. 5(2).

39 Id. sect. 4(3).

40 Id. sect. 5(3).

41 Id. sect. 5(4).

42 Id sect. 7.

43 *People's Union for Civil Liberties v The Union of India And Another*,1996, available at: <http://www.indiankanoon.org/doc/87862/> accessed 6 July 2012.

44 Rule 419-A of the Indian Telegraph Rules, as amended by the Indian Telegraph (Amendment) Rules, 2007, available at:, http://www.dot.gov.in/Acts/English.pdf> accessed 6 July 2012.

45 Id. Rule 5.

46 Id. Rule 6.

47 Id. Rule 2 & 16.

48 Id. Rule 3.

49 Id. Rule 17.

Downloaded from https://academic.oup.com/idpl/article/2/4/302/676984 by guest on 11 April 2024

will be destroyed every six months, unless required for functional purposed, and records pertaining to an interception maintained by the service provider will be destroyed every two months.[50] In the case of an emergency, immediate interception can be authorized by the Joint Secretary or any official above, provided that the Union Home Secretary is informed within three days, and receives confirmation within seven days.[51] Parts of these safeguards are reflected in the Information Technology Act's provisions for interception.

When the three legislations are compared, it clear that systematic access is facilitated the primarily by the ITA. This can be seen by:

1. the weakening of standards for legal interception between older and newer statutes. For example, under the Indian Post Office Act, interception of postal articles is permitted in the occurrence only of a public emergency, or in the interest of the public safety or tranquility.[52] Under the TA, interception of communications is permitted on 'the occurrence of any public emergency, in the interest of the public safety, and for the interests of the sovereignty and integrity of India, the Security of the State, friendly relations with foreign states, or public order, or for preventing incitement to the commission of an offence.'[53] Under the ITA, interception of electronic communications is permitted for the same reasons as stated in the TA, but is additionally permitted for preventing incitement to the commission of any cognizable offence relating to the above, or for investigation of any offence. The ITA also does not require the condition that a public emergency or public safety be in place before an interception can take place.[54] Under the ITA, authorized agencies can also monitor and collect traffic data for a range of 'cyber security' purposes.[55]
2. criminalization of non-co-operation with interception and access requests and severe punishment for non-cooperation. For example, under the ITA systematic access is enforced by holding non-compliant service providers criminally liable whereas the TA holds non-compliant intermediaries subject to civil liability.[56]
3. In 2009 two sets of rules were issued under the ITA which increased systematic access and interception dramatically. These are (1) The Procedure and Safeguards for Interception, Monitoring, and Decryption of Information Rules, 2009,[57] which allow for the interception, monitoring, and decryption of information transferred between computer resources. (2) The Procedure and Safeguards for Monitoring and Collecting Traffic Data or Information Rules, 2009,[58] which allow for the monitoring of traffic data, which includes any 'data identifying or purporting to identify any person, computer system or computer network or location to or from which the communication is or may be transmitted, and includes communications origin, destination, route, time, date, size, duration or type of underlying service and any other information'.[59]

Procedure and safeguards for Interception, Monitoring, and Decryption of Information Rules

Under the Interception, Monitoring, and Decryption Rules, legal access to information begins with permission granted by the Secretary in the Ministry of Home Affairs in the case of the Central Government, and the Secretary in charge of the Home Department in the case of a State Government.[60] To enable this access, the Rule requires that:

1. Intermediaries must provide all facilities, cooperation, and assistance for the interception, monitoring, and decryption of information to authorized agencies.[61] The extent of the assistance required under the ITA is extensive, and includes assisting in the installation of equipment of the authorized agency, the maintenance, testing, or use of such equipment, the removal of such equipment, and any action required for accessing stored information under the direction.[62]

50 Id. Rules 18 & 19.

51 Id. Rule 2.

52 Indian Postal Act 1898 Section 26.

53 The Indian Telegraph Act 1885 Section 5(2). Under the Telegraph Act offence refers to an offence that requires a warrant from a magistrate for investigation.

54 Information Technology Act 2008 Section 69.

55 The Information Technology Act 2008 Section 69B.

56 The Information Technology Act 2008 Section 69A (3), The Telegraph Act Rules under section 419A 2007. sect. 15.

57 Information Technology Act Procedure and Safeguards for Interception, Monitoring, and Decryption of Information Rules. 2009, available at: <http://deity.gov.in/sites/upload_files/dit/files/downloads/itact2000/Itrules301009.pdf> accessed 27 August 2012.

58 Information Technology Act Procedure and Safeguards for Monitoring and Collecting Traffic Data or Information Rules, 2009.

59 As defined under Explanation ii of Section 69B, Information Technology Act, 2000 (as amended).

60 Sect. 4. ITA. Procedure and Safeguards for Interception, Monitoring, and Decryption of Information Rules. 2009.

61 Id. sect. 13.

62 Id. sect. 19.

Downloaded from https://academic.oup.com/idpl/article/2/4/302/676984 by guest on 11 April 2024

2. Mandatory key escrow of Decryption Key Holders, who are required to disclose both the decryption key and provide assistance in decrypting information to authorized agencies.[63] Key escrow allows for systematic access.
3. Sharing intercepted material internally and between authorized agencies. Although authorized agencies are prohibited from using or disclosing the contents of intercepted communications for any purpose besides investigation, they are permitted to share the contents with other security agencies for the purpose of investigation or in judicial proceedings.[64] For example, a Central Government agency can access all information collected and intercepted by a State security agency.[65]

Procedure and safeguard for Monitoring and Collecting Traffic Data or Information Rules

These rules contain similar procedural instructions to the Interception, Monitoring, and Decryption rules, as they also require intermediaries to extend all facilities to authorized agencies on request.[66] But, unlike the Decryption, Interception, and Monitoring rules, orders for monitoring of traffic data are allowed to be issued for matters related to cyber security including:

- forecasting of imminent cyber incidents;
- monitoring network application with traffic data or information on computer resources;
- identification and determination of viruses or computer contaminants;
- tracking of cyber security breaches or cyber security incidents;
- tracking computer resources breaching cyber security or spreading viruses or computer contaminants;
- identifying or tracking of any person who has breached, or is suspected of having breached or being likely to breach cyber security;
- undertaking forensics of the concerned computer resource as part of an investigation or internal audit of information security practices in the computer resource;
- accessing stored information for enforcement of any provisions of the laws relating to cyber security for the time being in force;
- and any other matter relating to cyber security.[67]

Internet and telecom licences

Directions as to how and what extent intermediaries are to assist the government in interception are also found in the ISP licence and the UASL—Unified Access Service Licence, both of which are legally grounded in the Telegraph Act. It is unclear whether the licences conform strictly to the privacy safeguards of the Indian Telegraph Act.[68] Each licence facilitates extensive systematic access by the following means.

(a) Providing monitoring, tracing, and interception facilities and infrastructure to security agencies.

(b) Prohibiting service providers from using bulk encryption.

(c) Mandating data retention which is accessible in real time to security agencies through online portals. Minimum retention periods are specified in some cases, but no clear requirement for deletion or anonymization exists.

(d) Requiring the provision of information for varying reasons including: 'to trace . . . obnoxious calls', to 'detect crime', prevent 'cyber terrorism', and '. . . in the event of low intensity conflict'.

(e) Changing the timeframe and periodicity of access requests including 'on request', 'from time to time', 'at all times', and 'in real time'.

(f) Expanding of authorized authorities to include 'security agencies', 'officers of the Government of India', 'The Government', 'designated person of the Government/State', 'The Telecom Authority', and 'the licensor or authorized representatives'.

(g) Providing access to extensive information, such as: 'all information on the system', 'location details', 'a complete list of subscribers', 'call record details', 'time charges of internet telephony calls', 'profiles of all users connected to the service', 'copies of packets originating from the customer premise', 'all commercial records', 'all location details of equipment provided', 'traceable identities of subscribers', 'data records for even failed call attempts', and 'list of calling line identification restriction subscribers with their complete address and details.'

(h) Not differentiating between metadata and payload data, that is user logs are subjected to the access standard as the geographical location of an individual.

63 Id. sect. 17.
64 Id sect. 25 (2).
65 Id. sect. 25 (6).
66 Sect. 4.7 ITA. Procedures and safeguards for Monitoring and Collecting of Traffic Data Information Rules, 2009.
67 Id. sect. 3.
68 ISP License Clauses 34–35, UASL License Clauses 39–41.

Downloaded from https://academic.oup.com/idpl/article/2/4/302/676984 by guest on 11 April 2024

In comparison to international interception and access best practices, the Indian regime on the whole is lacking. Missing safeguards, include: redress to individuals who were unduly implicated by interception activities,[69] internal restrictions on access to intercepted material,[70] requiring a court order for interception.[71]

Laws requiring proactive/systematic disclosure of private sector

In India there are three categories of legislation, policy, and practice that we examined that require broad disclosures of information to the government: banking laws, health laws, and practices concerning travel. The broad disclosure that takes place is often of information collected by the 'monitoring' of irregular behaviour in databases, and is augmented through broad and generic mandatory data retention. It is important to note that in many traditional Indian legislations, although proactive disclosure does take place, there are also safeguards in place to minimize misuse.

Banking laws

Acting as the regulating body for banking in India is the Reserve Bank of India (RBI). The RBI was established under the Reserve Bank of India Act 1934, and is considered to be a branch of the government.[72] Under the Act, the RBI can require financial institutions, non-banking companies, and corporations to furnish information on a regular basis as may be specified by the RBI through general or special order.[73] This includes the ability to collect and require disclosure of information relating to: credit,[74] deposits,[75] assets,[76] investments, and statements[77] from banking and non-banking institutions. The RBI is allowed to inspect any non-banking or financial institution to verify the correctness and completeness of information furnished, or to obtain information that the institution failed to furnish.[78] The RBI is not allowed to further disclose this information, except if it is considered necessary in the public interest, with permission from the bank, or if it is required under any other law.[79]

Further defining the powers of the RBI is the Banking Regulations Act 1949, which was enacted to allow the RBI to regulate, control, and inspect banks in India.[80] The Act requires that banking companies submit to the Reserve Bank a return showing its assets and liabilities on a monthly basis. At the same time the Reserve Bank may direct a banking company to furnish any information relating to its business or affairs.[81] The RBI also has the power, if directed by the Central Government or a High Court, to inspect the books and accounts of any bank. If directed, reports of the inspection are to be disclosed to the Central Government.[82] This information is otherwise allowed to be disclosed only when it is considered to be in the public interest.[83]

As a mechanism to both correctly identify clients, hold clients accountable, and increase the effectiveness of banks detecting illegal transactions, the Banking Regulations Act 1949 established the Know Your Customer (KYC) norms.[84] Under the norms, banks must report to controlling officers all cash deposits and withdrawals over INR 1,000,000 in fortnightly statements,[85] and proactively disclose 'suspicious transactions' to the RBI and 'appropriate law enforcement authorities'.[86] Through this requirement, the KYC norms enable banks, the RBI, and law enforcement to monitor customer transactions in order to detect illegal activities such as ghost accounts (Benami),[87] tax fraud, money laundering, financing of terror, and phishing. According to the KYC norms banks should obtain 'all information necessary' to establish the identity of each new customer.[88] This violates the data minimization principle. Banks must also keep documentation on customer relationships and transactions to enable the reconstruction of any transaction. These records are to be preserved and maintained for at least five years, and should be available for audit, and 'when required'.[89]

69 As is the case under the UK RIPA Act.
70 As is the case under the UK RIPA Act.
71 As is the case under the US Wiretap Act.
72 The Reserve Bank of India Act 1934 sect. 3, available at: <http://www.vakilno1.com/bareacts/reserve1934/reserve.html> accessed 28 July 2012.
73 Id. sect. 45 (K)& (L).
74 Id. sect. 45(B)&(C).
75 Id. sect. 45 (K).
76 Id. 45(IB).
77 Id. 45(l) & (M).
78 Id. sect. 45 (N).
79 Id. sect. 45 (NB).
80 The Banking Regulations Act 1949, available at: <http://cooperation.ap.nic.in/pdf/BR%20Act%201949.pdf> accessed 27 August 2012.
81 Id. sect. 27.
82 Id. sect. 35.
83 Id. sect. 28.
84 Guidelines on 'Know Your Customer' 2002. sect. 8 KYC norms are issued under Section 35A of the Banking Regulations Act 1949, available at: <http://www.rbi.org.in/scripts/NotificationUser.aspx?Id=819&Mode=0> accessed 28 July 2012.
85 Id. sect. 4.3.
86 Id. sect. 5.4.
87 Benami means 'without name'.
88 Id. sect. 2.2.
89 Id. sect. 6.

Downloaded from https://academic.oup.com/idpl/article/2/4/302/676984 by guest on 11 April 2024

The Prevention of Money Laundering Act, 2002 (PMLA) is India's most comprehensive anti-money laundering legislation.[90] The legislation mandates all banking companies, financial institutions, and intermediaries to maintain transaction and client identity records as 'prescribed' for ten years.[91] These records are to be furnished to appointed directors as may be prescribed by Central Government in consultation with the RBI.[92] In turn, the Director, through a general or special order, may disclose the information to tax, foreign exchange, or duty or cess authorities. The Director may also disclose information to any officer, authority, or body functioning under any law as the Central Government if it is in the public interest, or needed to enable an officer to carry out his/her duties.[93] Powers of search, seizure, and summons are permitted under the Act, but justification must be recorded in writing, and an established procedure for the acquiring and retaining of data must be followed.[95] Furthermore, search and seizure through the Act is subjected to the provisions of the CrPc.[95]

Intermediaries that fall under the ambit of the Securities and Exchange Board of India Act 1992[96] are held accountable to the monitoring and disclosure standards found in the PLMA. In guidelines specifically addressing money laundering in the securities sector, intermediaries must have in place a system for reporting suspicious transactions, and be able to disclose relevant information to 'law enforcement agencies' in a timely manner.[97]

Health Legislation

Broad disclosure requirements of health related information apply to both private and public institutions. The rationale for broad disclosure in the health sector, unlike banking or telecommunications, has primarily to do with public safety, order, and health—as in the case of tracking epidemics. For example, the Epidemic Diseases Act 1947 contains broad provisions which require the government to be informed if any part of the state is 'visited by, or threatened with, an outbreak of any dangerous epidemic disease'.[98] In order to prevent the outbreak of a disease, the government can authorize authorities to inspect persons travelling within the country or across national borders. The authorities must inform the government of the findings of such inspections.[99] The type and amount of information allowed to be collected through these inspections, and to be subsequently disclosed to the government or by the government, is unclear. Thus, in this case, broad disclosure of information is accompanied by broad and indiscriminate collection of information for the purposes of 'preventing an outbreak of disease'.

In 1992, the Government of India established the National AIDS Control Organization (NACO) for the prevention and control of AIDS. One of many programmes initiated by NACO are Community Care Centers,[100] which are intended to serve as a transitioning point between hospital and home care for patients. The programme facilitates proactive disclosure through its systematic monitoring and reporting of district level activities to the state level, where the information is compiled into state reports and shared with 'stakeholders'.[101] Information that is monitored and reported includes, but is not limited to, aggregate data such as the number of patients tested for HIV, the number of HIV positive clients, the number of pregnant women found HIV positive, and personal information such as specified client information.[102]

The Pre-Conception and Pre-Natal Diagnostic Techniques Act (PNT) 1994,[103] meant to criminalize female foeticide in India, requires extensive retention of personal information pertaining to pregnant women. For example, 'all registers, records, charts, consent letters, forms, books, pamphlets, advertisements, material objects, equipment records, and any other material required to be maintained under the Act', must be retained for a period of two years. These records must be made available at all reasonable times for inspection

90 Prevention of Money Laundering Act, 2002, available at: <http://finmin.nic.in/law/moneylaunderingact.pdf> accessed 27 August 2012.

91 Id. sect. 12 (a).

92 Id. sect. 15.

93 Id. sect. 66.

94 Id. sects 16&17.

95 Id. sect. 65.

96 Under the SEBI Act an intermediary includes: stock-broker, sub-broker, share transfer agent, banker to an issue, trustee to a trust deed, register, merchant banker, underwriter, portfolio manager, investment adviser.

97 Guidelines for Anti Money Laundering Measures. SEBI. 3.2.3 Available at: <http://www.sebi.gov.in/cms/sebi_data/attachdocs/1292487332332.pdf> accessed 28 July 2012.

98 *The Epidemic Diseases Act*. (1897). Section 2(1), available at: <http://www.maha-arogya.gov.in/actsrules/EPIDEMIC-DISEASES-ACT.pdf> accessed 28 July 2012.

99 Id. sect. 2(2)(b).

100 NACO, Operational Guidelines for Community Care Centres, 2007, available at: <http://nacoonline.org/upload/Policies%20&%20Guidelines/22,%20Guidelinesfor%20Community%20Care%20Centre%20-.pdf> accessed 28 July 2012.

101 Id. p. 41.

102 Id. p. 45.

103 The Pre-Conception & Pre-Natal Diagnostic Techniques Act 1994, available at: <http://rajswasthya.nic.in/PCPNDT%2005.12.08/PCPNDT%20Act%20%282%29.pdf> accessed 28 July 2012.

Downloaded from https://academic.oup.com/idpl/article/2/4/302/676984 by guest on 11 April 2024

by the appropriate authority,[104] who is appointed by the Central Government.[105]

Proactive disclosure of health information also takes place through real-time monitoring of pregnant women under projects such as the 'Save the Baby Girl (STBG)' project. STBG was launched to curb female foeticide and improve the sex ratio. The system includes an online portal, and the installation of video capture devices called the 'Silent Observer' (SIOB), which are connected to ultrasound machines. The SIOB, also known as the 'active tracker' monitors ultrasound tests and records images of each sonography conducted. This information is submitted by sonography centres through the online portal where it is centralized and used to generate statistics and reports. The recorded sonography video and centralized records are accessible to 'concerned authorities',[106] which the press notes and project descriptions have not clearly specified. Given the skewed sex ratios in India, this is perhaps one area where disclosure is warranted.

Travel

In India, there is no specific legislation that addresses disclosure of travel data to the government, yet there is an undocumented obligation on relevant private-sector companies to collect, maintain, proactively disclose, and allow access to information on travellers. The absence of explicit policy results in the exact practices around disclosure and access to travel information is ambiguous. Perhaps the most innocuous of these practices is the disclosure of aggregate travel information to the Directorate General of Civil Aviation.[107] On the other hand, hotels in India are required to maintain ID record of all guests staying on the premises, which must be submitted to the police. Yet, how often these records are submitted, and if officials can come to a hotel and request access to the records at any point of time is unclear.[108]

The same ambiguity exists around passenger records. There seem to exist two conflicting practices. According to anonymous senior officials at the Director General of Civil Aviation, passenger information that is collected and held by the airlines is not submitted to any body or organization under any circumstance. This fact was supported by an anonymous source in a budget airline. Yet, according to an anonymous source the Indian Income Tax Department requests lists of passengers who fly over a set number of times per year to crack down on tax fraud from travellers.

The role of the courts for major categories of data

Historically, the courts played a limited role in authorizing the interception of communications or payload data. For example, section 92 of the CrPc, which applies to 'any document, parcel or thing in the custody of a postal or telegraph authority' or in other words analogue letters and telegrams, requires judicial authorization, as a court order must be issued before accessing information.

However, this safeguard is no longer relevant in today's information society. Section 91 of the CrPc, which is commonly used to access basic subscriber information and other metadata, especially from telecom and internet companies, does not require judicial authorization. Nor do the various interception and access provisions for meta data and payload data under the ITA, TA, or ISP licences. To summarize, Indian courts do not have any role in the authorization or oversight of interception and access to metadata or payload data.[109]

The absence of courts in the authorization process has resulted in diverse practices. For example, according to some security experts based in Delhi and in Mumbai who provided anonymous interviews for this paper: (1) all phone calls in sensitive cities like Mumbai are recorded for two or three days, these records are reviewed by the police and specific numbers are then retained for longer durations, and (2) all international voice traffic is retained for two or three days. However, representatives of Indian telecos speaking under conditions of anonymity have given assurances that such blanket voice retention measures are neither technically nor economically possible. The truth, perhaps, lies somewhere in between, as it appears that Telecos engaged in data retention of voice and Internet traffic and metadata have rolled out legal interception equipment based upon the big data business opportunity, and

104 Id. sect. 29.

105 Id sect. 17(2).

106 Id. Save the Baby Girl Project. Press Note. February 2010, available at: <http://savethebabygirl.com/news/pressnote-stbg1.pdf> accessed 28 July 2012.

107 For example, passenger Data statistics can be found on the DGCA website, available at <http://www.dgca.nic.in/reports/pass-ind.htm,http://tourism.gov.in/TourismDivision/AboutDivision.aspx?Name=Travel%20Trade> accessed 27 August 2012.http://tourism.gov.in/TourismDivision/AboutDivision.aspx?Name=Market%20Research%20and%20Statistics>.

108 Bureau of Immigration. General Requirements for Registration of a Foreign National. <http://www.immigrationindia.nic.in/reg_req2.htm#rhk101>. section 'Report to be made and by Hotel Managers' accessed 28 July 2012.

109 Payload data refers to the content of a message or communication.

Downloaded from https://academic.oup.com/idpl/article/2/4/302/676984 by guest on 11 April 2024

the frequency of intercept or information requests. By examining media coverage of crime, one can make an informed guess about the scope and nature of data retention. During the investigation of the Arushi murder, it was clear that Internet traffic logs detailing search engine queries and details of when the modem was turned on and switched off could be recovered weeks after the incident.[110] In contrast, during the investigation of Sister Valsa John's murder it was not possible to recover her call records without finding the device.[111]

Standards for use

Standards for governmental use of accessed information vary across sectors, and in most cases are non-existent. Apart from the safeguards for telephonic interception established as a result of the *PUCL v Union of India* ruling, few other explicit standards for use or safeguards against abuse are mentioned in sectoral law. One of the safeguards notified in the Telegraph Act rules as a result of the Supreme Court's verdict in *PUCL v Union of India* impacts the use of intercepted information: 'all copies of the intercepted material must be destroyed as soon as their retention is not necessary under the terms of the Act.'[112] Reflecting similar safeguards to those found under the TA, the ITA Interception, Monitoring, and Decrpytion Rules, prescribe the maintenance of records by the designated officer to include 'the name and other particulars of the officer or the authority to whom the intercepted or monitored or decrypted information has been disclosed, the number of copies, including corresponding electronic records of the intercepted or monitored or decrypted information made and the mode or method by which such copies, including corresponding electronic record are made, the date of destruction of the copies.'[113] However, in contrast, the 'Guidelines for Anti-Money Laundering Measures' issued by SEBI do not mention any similar privacy safeguards under the sections dealing with 'record keeping' and 'retention of records.'[114]

Cross-border and multi-jurisdictional issues

The ITA 2008 in its preliminary chapter clarifies that it does not only apply to the India jurisdiction; it says it 'applies also to any offense or contravention there under committed outside India by any person'.[115] This is in contrast with the Telegraph Act, which only 'extends to the whole of India'.[116] Thus, when information leaves the Indian jurisdiction it is most often subjected to other countries laws and regulations, unless otherwise stated in a contract.

Recent controversies and/or pending unresolved issues

BlackBerry

The four years of negotiations between the Indian government and Research in Motion (RIM) demonstrate how the Indian Government is seeking both systematic access to, and proactive disclosure of, information held by the private sector. Since March 2008, the Indian Government has threatened to ban RIM's BlackBerry services, unless given real time and direct access to communication traffic.[117] The Indian Government during negotiations has proposed six solutions to allow for direct access to the BlackBerry network. These are: (1) physically locating the servers (Network Operating Centres) within India, thus giving the Government clear jurisdiction;[118] (2) enforcing a blanket data retention requirement on all Internet data and email for a minimum period of six months;[119] (3) lowering RIM's encryption to 40 bit from the current 256 bit to allow easy interception of communications;[120] (4) encryption key escrow for both BIS and BES with the Indian

110 *Times of India*, Aarushi murder case: Only Talwars no one else in house, says CBI, March 1st 2011m available at: <http://articles.timesofindia.indiatimes.com/2011-03-01/delhi/28642981_1_nupur-talwar-rajesh-talwar-aarushi-murder-case> accessed 28 July 2012.

111 The Indian Express. Nun's mobile to give lead in investigation: Police. November 19th 2011. Available at: <http://www.indianexpress.com/news/nuns-mobile-to-give-lead-in-investigation-police/877993/> accessed 27 August 2012.

112 PRS. April 27th 2010. FAQS on Telephone Tapping, available at: <http://www.prsindia.org/theprsblog/2010/04/27/faqs-on-telephone-tapping/> accessed 28 July 2012.

113 The Information Technology Interception, Monitoring, and Decryption Rules 2009, Section 16. A similar safeguard is found under section 8 of sect. 419A Telegraph Act Rules 2007.

114 Guidelines for Anti-Money Laundering Measures, available at: <http://www.sebi.gov.in/guide/antimoney.pdf> accessed 28 July 2012.

115 S. 1 Information Technology Act 2000, available at: <http://eprocure.gov.in/cppp/sites/default/files/eproc/itact2000.pdf> accessed 28 July 2012.

116 S. 1 Indian Telegraph Act 1885, available at: <http://www.dot.gov.in/Acts/telegraphact.htm> accessed 28 July 2012.

117 Philip, Joji. BlackBerry maker Research in Motion agrees to hand over its encryption keys to India. Economic Times. August 2nd 2012. Available at: <http://articles.economictimes.indiatimes.com/2012-08-02/news/33001399_1_blackberry-enterprise-encryption-keys-corporate-emails> accessed 12 September 2012.

118 Economic Times. RIM gives in, BlackBerry server to be located in India. August 30th 2010. Available at: <http://articles.economictimes.indiatimes.com/2010-08-30/news/27624905_1_blackberry-encrypted-services-rim> accessed 27 August 2012.

119 *Economic Times*, DoT Bats For Blackberry, Wants Updated Technology, July 10th 2008, available at: <http://articles.economictimes.indiatimes.com/2008-07-10/news/27719369_1_blackberry-services-blackberry-smartphones-encryption-solutions> accessed 28 July 2012.

120 Id.

Downloaded from https://academic.oup.com/idpl/article/2/4/302/676984 by guest on 11 April 2024

Government;[121] (5) negotiating a 'Government to Government' solution where legal interception orders will be routed through the US or Canadian government, who will then comply and carry out interception on behalf of the Indian Government;[122] (6) complying with the requirements of the Central Monitoring System (CMS), an interception network that allow Security Agencies to intercept emails, cyber chats, monitor voice calls, SMS, MMS, GPRS, fax communications on landlines, and CDMA and GSM networks—from New Delhi in real time.[123]

Solutions 4 and 6 proposed by the Indian government imply proactive disclosure, allowing the government to bypass the private sector and legal safeguards.

In the standoff, RIM made several counter offers to the Indian government, which did not directly correlate to their demands. For example, most recently, RIM has opened a facility NOC in Mumbai.[124] This arrangement will allow for interception of Black Berry messages, and BIS traffic (not BES traffic). Access at this level can only be resolved via proactive disclosure or key-escrow. The policy and practice emerging from the stand-off between RIM and the Indian government is commonly understood within and outside government to set the standard for data access and interception for other private-sector companies offering similar cloud-based encrypted communication services like Google Mail and Skype.[125]

The Central Monitoring System

As mentioned, the government is presently looking to build a Centralized Monitoring System (CMS) to enable comprehensive and legal interception. The CMS will allow Security Agencies to intercept, in real time, emails, cyber chats, monitor voice calls, SMS, MMS, GPRS, fax communications on landlines, and CDMA and GSM networks.[126] The new system will specifically exclude service providers from carrying out interceptions, thus creating a system where the government will not need to require disclosure, but will be able by pass the private sector, and access this information on its own.

NATGRID

In 2011, the National Intelligence Grid (NATGRID) was established as an attached office of the Ministry of Home Affairs, and facilitates governmental systematic access by providing authorized agencies with the ability to connect 21 databases from government and private-sector organizations such as tax, travel, Internet, and phone records.[127] NATGRID complicates the picture of governmental access to information, because it does not operate under legislation, and claims only to connect databases to allow tracking. Since, regulations and procedures have not been made public, this means that ten intelligence/law enforcement agencies could potentially access any information held by a private-sector company without authorization or notification.

Corruption

Although Indian interception legislation does have some safeguards in place to protect against systematic access by the government, in practice the government often ignores these safeguards. Recently, in Mumbai, two city assistant police commissioners were accused of selling call details from the conversations of high-profile individuals.[128] The police commissioners allegedly used their position to gain access to the communication records from telecos. Only one of the telecos responded when the investigating police officers approached seeking the names of the officers to whom details had been disclosed.[129] This incident reveals that law enforcement officials abuse their positions to dilute data access safeguards, and demonstrates the loose implementation of the interception safeguards. In addition, it is clear that service providers are not transparent about data disclosures because it is not required by law, and in some cases the disclosure was not legal. Thereby reiterating the lack of redress and

121 D Kutty, Indian Government Asks RIM For Blackberry Keys, *Topnews*, 9 July 2011, available at <http://www.Topnews.In/Indian-Government-Asks-Rim-Blackberry-Keys-2333827> accessed 28 July 2012.

122 *Economic Times*, Blackberry To Open Code For Security Check, August 3rd 2010, available at: <http://articles.economictimes.indiatimes.com/2010-08-03/news/27620028_1_rim-executives-blackberry-corporate-email> accessed 28 July 2012.

123 Time of India. Soon agencies to intercept email, chats in real time. May12th 2011. Available at: <http://articles.timesofindia.indiatimes.com/2011-05-12/india/29535755_1_security-agencies-cms-intercept> accessed 27 August 2012.

124 Sharma, A. RIM Facility Helps India in Surveillance Efforts. The Wall Street Journal. October 28th 2011. Available at: <http://online.wsj.com/article/SB10001424052970204505304577001592335138870.html> accessed 27 August 2012.

125 Rediff. India wants access to Google, Skype, Twitter data. July 13th 2011. Available at: <http://www.rediff.com/money/slide-show/slide-show-1-tech-india-wants-access-to-google-skype-twitter-data/20110713.htm> accessed 11 September 2012.

126 Times of India (n 117).

127 *The Wall Street Journal*, Q&A: NATGRID Chief Raghu Raman, June 29th 2011, available at: <http://blogs.wsj.com/indiarealtime/2011/06/29/qa-natgrid-chief-raghu-raman/> accessed 28 July 2012.

128 Id. *The Times of India*, Two Delhi cops may land in the dock for selling cell call records. March 11th 2012, available at: <http://articles.timesofindia.indiatimes.com/2012-03-11/mumbai/31144815_1_delhi-officers-delhi-cops-service-providers> accessed 28 July 2012.

129 Id.

Downloaded from https://academic.oup.com/idpl/article/2/4/302/676984 by guest on 11 April 2024

protection for service providers if there is misuse of access rights by government entities.

CCTV

CCTV is an area where proactive disclosure and systematic access to private-sector data is growing rapidly in the absence of any regulatory framework. For example, in New Delhi, other metro cities, and state capitals, the police have been insisting on the installation of CCTV cameras in private-sector businesses.[130] Hotels are asked to install CCTV cameras at reception desks, front entrances, car parks, and all lobbies of the hotel.[131] Most recently, the police have been encouraging private establishments to make CCTV camera feeds available in real time by using web-streaming technologies.[132] In practice, the use of technology to deliver footage in real time requires the private sector to proactively disclose information, and allows the police systematic access to information about the day to day goings-on of private-sector establishments.

Concluding observations

The practices around the reactive, proactive, and systematic access to private-sector data by the Indian Government remain unclear, as few members of the private sector are willing to comment on the topic, even under conditions of anonymity. Furthermore, applicable and explicit policy is limited. Where applicable policy does exist, it is based on vague language with insufficient safeguards in place, thus leading to a wide range of interpretations and practices regarding governmental access. For example, data retention regimes employed by the private sector often do not adhere to safeguards like breach notification, transparency, internal record-keeping, and deletion/obfuscation policies; thus the extent of information that the government could potentially access is never clear.

As a result of this vague policy vacuum, there is no adherence to a uniform standard by the private sector, and practices are inconsistent across different organizations, geographic regions, market segments, and sectors in India. Indigenous private-sector organizations do not publicly resist data access or disclosure demands from the government. For example, in its annual report, Bharati Airtel alleges that 'in the Lawful Interception domain, we have received 422 appreciation letters from various Law Enforcement agencies in the last one year alone'.[133] The report is not clear as to the total number of interceptions facilitated by the company.

The lack of clarity in policy, and the gap between policy and implementation, has three implications: (1) unclear liability when personal data fall into the wrong hands; (2) lack of a redress system available to the private sector in case of abuse by government officials; (3) a tendency for collusion between government actors and private-sector actors which can additionally result in tampering with cyber-evidence.

In India health and banking legislation allow proactive disclosure and reactive access for reasons that impact the public interest such as access to information related to epidemics and transactions that could be fraudulent in nature. These legislations have some safeguards in place, and facilitate disclosure and access predominantly through requirements for broad data retention, and monitoring of abnormal patterns in the databases, that are explicitly described in the legislation. On the other hand policy around the disclosure and access to travel data is for the most part unclear, and seems to take place through unspoken practices.

A clear weakening of safeguards for access and disclosure has happened over time through Internet and communication legislation. For example, systematic access by the government, through interception legislation, has diluted safeguards, increased the scope of permitted interception, and created harsher penalties for non-compliance. The disclosure and access under these provisions is justified for reasons of national security and crime detection, and is facilitated by a lack of safeguards and failure to implement those in place.

The government's growing demand for proactive disclosure of, and systematic access to, private-sector data for reasons of national security and crime detection can also be seen through the BlackBerry controversy, the increased and varied uses of CCTV, and the government's routine development of 'bigger and better' surveillance systems such as UID, NATGRID, and the CMS. These projects have been implemented without waiting for enabling and safeguarding legislation.

130 *Hindustan Times*, CCTV cameras to keep an eye on parts of Old Delhi, July 5th 2012 available at: <http://www.hindustantimes.com/India-news/NewDelhi/CCTV-cameras-to-keep-an-eye-on-parts-of-Old-Delhi/Article1-883463.aspx> accessed 28 July 2012.

131 Madaan, Neha. Hotels shop for CCTV cameras, metal detectors. The Times of India. August 8th 2012. Available at: <http://articles.timesofindia.indiatimes.com/2012-08-08/pune/33099780_1_cctv-cameras-metal-detectors-sayaji-hotels> accessed 11 September 2012.

132 *The Indian Express*, Gang rape effect: Don't let women work beyond 8pm in pubs, mall, March 14th 2012, available at: <http://www.indianexpress.com/news/gangrape-effect-dont-let-women-work-beyond-8-pm-in-pubs-malls/923453/0> accessed 28 July 2012.

133 Bharati Airtel Annual Report. Year 2010–11. Pg.15. Available at <http://www.airtel.in/AnnualResults/Bharti_Airtel_annual_report_full_2010-2011.pdf> accessed 27 August 2012.

Downloaded from https://academic.oup.com/idpl/article/2/4/302/676984 by guest on 11 April 2024

Thus, the Government of India does not seem to exercise a scientific temper or adopt principles of natural justice when it comes to the systematic access to and disclosure of private-sector data. It appears to be sold on a techno-utopian vision of 'surveillance for surveillance's sake'.

doi:10.1093/idpl/ips028

Downloaded from https://academic.oup.com/idpl/article/2/4/302/676984 by guest on 11 April 2024