CENTRE FOR COMMUNICATION GOVERNANCE AT NATIONAL LAW UNIVERSITY DELHI

RESPONSE TO CALL FOR SUBMISSIONS ON 'SURVEILLANCE INDUSTRY AND HUMAN RIGHTS'[1]

The Centre for Communication Governance is an academic research centre within the National Law University Delhi and is dedicated to working on information law and policy in India. It seeks to embed human rights and good governance within communication policy and protect digital rights in India through rigorous academic research and capacity building.

We thank the United Nations Special Rapporteur on Freedom of Expression for inviting comments on the 'Surveillance Industry and Human Rights' for the report to the General Assembly in October 2018. Our response to the call for submissions is below.

1. Surveillance Powers in India

1.1. Laws enabling surveillance in India

The Indian State's powers of surveillance are primarily derived from two legislations. The first is the Telegraph Act, 1885[2] (**Telegraph Act**), which deals with interception

[1]*Authored by Gunjan Chawla and Smitha Krishna Prasad with inputs from Sarvjeet Singh and Yesha Tshering Paul.*

[2]The Telegraph Act, 1885 is the primary legislation that governs the telecommunications infrastructure in India. Telecommunication companies are permitted to operate in India on the basis of a license issued by the Department of Telecommunications, Ministry of Communications, under the Telegraph Act, 1885. The license is available at http://dot.gov.in/unified-license?page=1.

(and detention) of telephonic communications. Section 5 of the Telegraph Act provides that in certain circumstances, authorised agencies of the government may either take possession of a telegraph[3], or either prevent, intercept or detain a message or a class of messages[4]. Rule 419A of the Telegraph Rules, 1951 (**Telegraph Rules**) provides for certain procedural safeguards to be followed in the case of such interception or detention of communications.[5]

The second legislation that provides for surveillance powers is the Information Technology Act, 2000 (**IT Act**), which deals with electronic communications. Section 69 of the IT Act provides that in certain circumstances, authorised agencies of the government may order the monitoring, interception or decryption of '**any information** transmitted, received or stored through **any computer resource**'.[6] The Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 (**IT Rules**) in turn provide the process through which such action can be taken.

In addition to the above, there are certain provisions under criminal and other laws in India that also allow adjudicating and law enforcement authorities to access communications in specific circumstances.[7]

The laws and rules that regulate surveillance by Government agencies in India have been the subject of much criticism, for the lack of judicial oversight, transparency and accountability, among other things. The Supreme Court of India, and other courts in the country have looked into the conduct of surveillance on individuals many times over the years. While many of the earlier cases dealt with issues related

[3]Section 5(1), Telegraph Act 1885.
[4]Section 5(2), Telegraph Act 1885.
[5]The constitutional validity of Section 5(2) of the Telegraph Act 1885, was challenged before the Supreme Court in People's Union Of Civil Liberties v. Union Of India (UOI) and Anr., (1997) 1 SCC 301. The Supreme Court did not find Section 5(2) to be unconstitutional. However, the Court laid down certain procedural safeguards to be followed in the case of interception and detention of communications under Section 5(2). These procedural safeguards were then codified in the form of Rule 419A via amendment to the Telegraph Rules, 1951, in 2007.
[6]Section 69(1), IT Act.
[7]For instance Sections 91 and 92 of the Criminal Procedure Code, 1973.

to traditional surveillance measures, such as domiciliary visits, more recent cases have dealt with the use of technology for surveillance. For instance, the above-mentioned Rule 419A of the Telegraph Rules was brought in after the Supreme Court laid down procedural safeguards to be followed by the authorities under Section 5(2) of the Telegraph Act in *People's Union Of Civil Liberties v. Union Of India (UOI) And Anr*.[8] In *K. S. Puttaswamy v. Union of India* a landmark judgment in 2017, in which the Supreme Court upheld and affirmed the constitutionally guaranteed fundamental right to privacy, the Court also referred to the changes in the means of surveillance in recent years as a result of new/ developing technology.[9] The Court noted that while the State may have legitimate national security and other interests to monitor communications and collect and process personal data, such actions should be taken in accordance with the Constitution[10], i.e. the encroachment on privacy must be subject to law, it must be undertaken in pursuance of a legitimate state aim, and third, the means adopted for such action must be proportional to the objects and needs sought to be fulfilled by the law.[11]

The Court, in *Puttaswamy*, also recognised and affirmed the overlapping nature of fundamental rights, and held that the right to privacy not only arises under Article 21, which recognises the right to life and personal liberty, but also from the other fundamental rights guaranteed under the Indian Constitution. This includes the freedom of speech and expression guaranteed under Article 19(1)(a) of the Indian Constitution. The Court referred to previous judgments where it was held that surveillance in the form of phone tapping, for instance, would be violative of such rights under Article 19(1)(a).

The constitutionality of surveillance powers of the State including under section 5(2) of the Telegraph Act. Rule 419-A of the Telegraph Rules and Section 69 of the IT

[8] (1997) 1 SCC 301.

[9]K. S. Puttaswamy v. Union of India (2017) 10 SCC 1.

[10]Specifically, the Court referred to the procedural and content-based mandate under Article 21 of the Constitution of India which recognises the fundamental right to life and liberty.

[11]K. S. Puttaswamy v. Union of India (2017) 10 SCC 1, J. Chandrachud's opinion, para 180.

Act, and the IT Rules have been challenged before the Supreme Court and the case is currently pending.[12]

1.1.1. Consistency with International Human Rights Standards

As discussed above, the right to freedom of speech and expression has been guaranteed to all citizens of India under Article 19(1)(a) of the Indian Constitution. Article 19(2) of the Constitution provides that reasonable restrictions on this right may be imposed by law, if required 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.

We note here that the grounds on which restrictions to the freedom of speech and expression may be imposed under the Indian Constitution are slightly more elaborate than those provided for under Article 19 of the International Covenant on Civil and Political Rights (**ICCPR**). However, these restrictions could fall into the broad categories for restrictions under the ICCPR which provides that restrictions must be provided by law, and must be necessary for (a)respect of the rights or reputations of others or (b) the protection of national security or of public order (ordre public), or of public health or morals.

Specifically in the context of surveillance laws, the Indian Supreme Court has recognised that the right to privacy and freedom of speech and expression are overlapping rights. The right to privacy has also been drawn by the Supreme Court from the various fundamental rights under the Constitution, including the right to freedom of speech and expression.

As discussed above, the State's surveillance powers are largely derived from the Telegraph Act and the IT Act. Section 5(2) of the Telegraph provides that communications may be intercepted and detained upon the occurrence of a public emergency, or in the interest of public safety, if such interception is

[12] ML Sharma and Ors. v. Union of India, W.P.(Crl.) No. 1/2019. .

necessary in the interest 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. It can be argued that this provision is consistent with the requirements under Article 19(3) of the ICCPR. However, we note that other issues such as a lack of transparency and judicial oversight are cause for concern, especially given that there are few remedies available to an individual whose rights are wrongfully violated under this provision[13].

Section 69 of the IT Act provides that directions may be issued for the interception, monitoring or decryption of any information through any computer resource, if it is found to be necessary or expedient in the interest of the sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence. The grounds for undertaking surveillance activities under this provision are broader than those under Section 5(2) of the Telegraph Act, given the absence of the requirements for surveillance to be undertaken in a situation of public emergency, or where required for public safety. This is one of the grounds on which the provision has been challenged before the Supreme Court, as discussed above.[14] The actual acts of surveillance that are permitted by this provision are also more expansive, since it provides for interception, monitoring or decryption of **any information**. In addition, we note that the same issues of lack of transparency, judicial oversight and the

[13]Section 26 of the Telegraph Act provides that if a telegraph officer or other official omits to transmit or intercepts or detains, or discloses the contents of any message without authorisation, such person may be punished with imprisonment for a term which may extend to three years or with fine, or with both. Rule 419A of the Telegraph Rules in turn provides that if telecommunications service providers violate the terms of their license, including the requirement to maintain confidentiality of information or undertake unlawful interception of communications, they will be fined, and their licenses will be suspended or revoked in accordance with relevant provisions of the Telegraph Act. However, in the absence of transparent procedures, it may be difficult for an individual to even obtain knowledge of such interception to begin with.
[14] Internet Freedom Foundation v. Union of India, W.P.(C) No. 44/2019.

resulting inability to access remedial measures exist in the context of Section 69 of the IT Act as well.

It is also not clear whether the existing procedures for obtaining authorisation to undertake the acts of surveillance permitted under the Telegraph Act or IT Act are followed, given the number of surveillance orders. The Committee of Experts set up in 2017 to recommend a data protection framework for India has itself noted that there is a lack of legal and procedural safeguards in the context of surveillance, and that much of the intelligence gathering activities in the country are undertaken outside the scope of the law.[15]

1.1.2. Other issues

These laws and rules are also particularly relevant to the questions raised in the Special Rapporteur's call for submissions in the context of two issues. First, telecommunications service providers[16], internet service providers, and any person who is in charge of a 'computer resource' for the purpose of Section 69 of the IT Act, are mandated to cooperate with and assist the authorised government agencies in undertaking the acts of interception, monitoring, and decryption mentioned above. Second, specifically under the IT Act, several intelligence and law enforcement agencies have now been notified as 'authorised', with little clarity about whether or not the entire process of authorisation of interception, monitoring or decryption of information provided for under the IT Rules will need to be followed by these agencies.[17] In addition to questions about process, such a notification is also of concern since some of the agencies that have been notified as 'authorised' have been set up by executive order (in some cases prior to the formation of independent India),

[15]Committee of Experts under the Chairmanship of Justice B.N.Srikrishna, A Free and Fair Digital Economy, available at https://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report-comp.pdf.
[16] Telecommunication Service Providers are required to cooperate / provide assistance under the terms of the Unified License, available at http://dot.gov.in/unified-license?page=1.
[17]Notification dated 20.12.2018 (bearing No. 14/07/2011-T).

rather than by way of statute.[18] As a result, there is little parliamentary oversight over the functioning of these bodies and the manner in which they interact with private / non-state actors.[19]

1.2. Technological Architecture for Surveillance in India

A brief overview of some of the surveillance programs instituted by the Indian government is provided below:

1.2.1. Central Monitoring System (**CMS**)

This system is operated by the Department of Telecommunications (and its state level agencies) and aims to automate the process of lawful interception and monitoring of telecommunications. The system enables direct access to communications on mobile phones, landlines and the internet in the country, with minimum manual intervention.[20] It also provides for central and regional databases to be set up, and will allow for a system of filtering and data mining of call detail records and other information to identify specific information about targeted numbers.

While prior to the implementation of the CMS, all telecommunications service providers in India were required, under their license terms, to install 'lawful interception systems' to carry out targeted surveillance, the license terms have

[18]Raman Jit Singh Chima and Vrinda Bhandari, When the state plays I spy, THE INDIAN EXPRESS, December 29, 2018, available at https://indianexpress.com/article/opinion/columns/snooping-computer-surveillance-it-act-mha-spying-cbi-ed-5514301/; and Explain Intelligence Bureau's legality, HC tells Centre, THE TIMES OF INDIA, March 26, 2012, available at https://timesofindia.indiatimes.com/india/Explain-Intelligence-Bureaus-legality-HC-tells-Centre/articleshow/12408605.cms.

[19]For more information on surveillance laws in India, *see* Chinmayi Arun, *Paper-Thin Safeguards and Mass Surveillance in India,* 26 NLSI REV. 105 (2014); Chaitanya Ramachandran, *PUCL v. Union of India Revisited: Why India's Surveillance Law Must Be Redesigned For The Digital Age*, 7 NUJS L .REV. 105 (2014).

[20]Centralised System to Monitor Communications, Press Information Bureau, November 26, 2009, available at http://pib.nic.in/newsite/PrintRelease.aspx?relid=54679.

since been amended to mandate integration of specific servers (which are connected to the CMS) with such lawful interception systems[21].

Development of this system started in 2008, and as of 2016, the system was reported to be live in Delhi and Mumbai, with little information on when it would be implemented fully.[22] As of early 2017, it was reported that the system would be fully operational by the first quarter of 2017.[23]

1.2.2. National Intelligence Grid (**NAT-GRID**)

Operated under the aegis of the Ministry of Home Affairs, the NAT-GRID is an integrated intelligence grid that links the stored records and databases of several government entities in order to collect data, decipher trends and provide real-time analysis of data gathered across law enforcement, espionage and military agencies. The project was approved by way of a notification after clearance was obtained from the Cabinet Committee on Security. However, there is no legislation passed by parliament to support this project.

In the initial stage, this project will allow 11 security agencies to access 21 sources of citizen data to track terror activities. These data points will include railway and air travel, income tax, bank account details, credit card transactions, visa and immigration records.[24] Additional intelligence and law

[21]Maria Xynou, India's Central Monitoring System (CMS): Something to Worry About?. January 30, 2104, available athttps://cis-india.org/internet-governance/blog/india-central-monitoring-system-something-to-worry-about.

[22]Sneha Johari, Govt's Central Monitoring System already live in Delhi & Mumbai, MEDIANAMA, May 11, 2016, available at https://www.medianama.com/2016/05/223-india-central-monitoring-system-live-in-delhi-mumbai/.

[23]Devirupa Mitra, India Gears Up to Defend Internet Rights Regime as it Operationalises Mass Surveillance Project, THE WIRE, May 3, 2017, available athttps://thewire.in/diplomacy/india-mass-surveillance-project-cms.

[24]NATGRID Gets Cabinet Approval, NDTV, June 7, 2011, available at https://www.ndtv.com/india-news/natgrid-gets-cabinet-approval-457900.

enforcement agencies and data sources will be added as the project moves forward.[25]

1.2.3. Network Traffic Analysis (**NETRA**)

This system was developed by the Centre for Artificial Intelligence and robotics at the Defence Research and Development Organisation. The system is meant to capture data from the Internet traffic, analyses it and alerts the concerned agencies in case it identifies a potential security threat. It identifies specific suspicious communications by detecting words like 'attack', 'bomb', 'blast' or 'kill' from tweets, status updates, emails, instant messaging transcripts, internet calls, blogs and other fora, as well as voice traffic on services such as Skype[26]. Reports suggest that the system serves 2 agencies[27], the Cabinet Secretariat's[28] Research and Analysis Wing[29], and the Intelligence Bureau[30].

1.2.4. Lawful Intercept and Monitoring (**LIM**)

The LIM is a secret mass electronic surveillance program operated by the Government of India for monitoring internet traffic, communications, web-browsing and all other forms of internet data.[31] The project is operated by way of installing interception, monitoring and storage programmes at international gateways, internet exchange hubs as well as ISP nodes across the country.

---

[25]NATGRID to get PAN, taxpayer data access, THE ECONOMIC TIMES, June 22, 2017, available at https://economictimes.indiatimes.com/news/economy/policy/natgrid-to-get-pan-taxpayer-data-access/articleshow/59270998.cms.

[26]Kalyan Parbat, Government to launch 'Netra' for internet surveillance, THE ECONOMIC TIMES, December 16, 2013, available at https://economictimes.indiatimes.com/tech/internet/government-to-launch-netra-for-internet-surveillance/articleshow/27438893.cms.

[27]Udhav Tiwari, The Design & Technology behind India's Surveillance Programmes, January 20, 2017, available at https://cis-india.org/internet-governance/blog/the-design-technology-behind-india2019s-surveillance-programmes.

[28]More information about the Cabinet Secretariat is available at https://cabsec.gov.in/.

[29]The Research and Analysis Wing is India's primary foreign intelligence agency.

[30]The Intelligence Bureau is India's internal intelligence agency.

[31]Shalini Singh, Govt. violates privacy safeguards to secretly monitor Internet traffic, THE HINDU, August 21, 2016, available at https://www.thehindu.com/news/national/govt-violates-privacy-safeguards-to-secretly-monitor-internet-traffic/article5107682.ece.

1.2.5. Crime and Criminal Tracking Network and System (**CCTNS**)

This system is slightly different from the others described above, and provides for the integration of all existing law enforcement records into one core application software (**CAS**) accessible by police stations and law enforcement authorities across the country. This system was developed as an e-governance initiative, and aims to use ICT to improve police functions.

Based on our research and the limited information available on these programs, we note that this is also one of the few systems where the technology, the core application software in this case, has been developed by a private corporation, namely Wipro Infotech.[32]

Other surveillance systems include the Telephone Call Interception System, and the New Media Wing.[33] In addition, there has been a proliferation of CCTV use in India, both by the public sector, for the purpose of policing activities, and by private individuals / entities.

1.3. Regulation of Private Sector Actions

Regulation of the private sector in the context of development, manufacturing, sale or use of surveillance technology in India is limited. No Government regulations exist to regulate the procurement and production[34], by private agencies and domestic

[32]Wipro to digitise India's crime records under e-governance plan, Governance Knowledge Centre, August 3, 2010, available at http://www.indiagovernance.gov.in/news.php?id=211.

[33]Privacy International, State of Privacy in India, January 2019, available at https://privacyinternational.org/node/1002.

[34]Industrial licenses are required for a select category of items specially designed for military use. Namely, electronic Equipment used for electronic counter measure (ECM) and electronic counter countermeasure (ECCM), surveillance, intelligence, Command and Control systems, Global Navigation satellite systems (GNSS) jamming equipment. Data processing, storage and transmission security equipment, identification and authentication equipment (including identification Friend or Foe and non-Cooperative Target Return Identification systems), guidance and navigation equipment' Troposcatter-radio communications equipment' and Military Information Security assurance systems and equipment (like cryptographic devices including military Cryptographic key management and Cryptanalytic systems), communication equipment, frequency modules and secrecy devices, specially designed for Military use. Dual use items which are not present in the above mentioned list are also not licensable under Industries (Development and Regulation) Act, 1951.See https://services.dipp.gov.in/lms/ilServices.

manufacturers, of surveillance technology that is not specially designed for military use. We have also been unable to find any regulation in the form of licensing requirements or otherwise, that are applicable to research and development efforts, or production and manufacturing of surveillance equipment in India. The only form of formal control that the State appears to exert in this regard is by way of issuing requests for proposals, and entering into formal contractual arrangements for specific projects that the Government undertakes.

However, India is a member of the Wassenaar Arrangement, and the Foreign Trade Policy (**FTP**) regulates the export of certain types of surveillance goods and technology, in compliance with India's obligations under the Arrangement. Regulations have been formulated to place restrictions on the import and export of such technology in compliance with India's international obligations under the Wassenaar Arrangement.

1.3.1. Export of dual-use surveillance goods and technology

India was admitted into the Wassenaar Arrangement framework, which regulates the export conventional arms as well as dual-use goods and technologies[35]. Since India's induction into the Wassenaar Arrangement the export of dual-use surveillance technology covered under the Wassenaar Arrangement has been incorporated into Indian law by amending the ITC-HS classification system under the FTP through a notification issued by the Directorate General of Foreign Trade (**DGFT**) in April 2017.[36] The FTP (the latest formulated for 2015-20 and revised in December 2017[37]) as well as the ITC-HS Classifications are formulated and notified by the DGFT under the

[35]Martand Jha, India and the Wassenaar Arrangement, LIVE MINT, February 5, 2018, available at https://www.livemint.com/Sundayapp/AETSo9p0H9Dii7ou9WRvrO/India-and-the-Wassenaar-Arrangement.html.

[36]Government of India, Ministry of Commerce and Industry, Directorate-General of Foreign Trade, Notification No. 5/2015-20 dated 24th April 2017, http://dgft.gov.in/sites/default/files/Notification5-English_0.pdf.

[37]Available at http://dgft.gov.in/sites/default/files/ft17-051217.pdf.

statutory authorization provided by Section 5 of the Foreign Trade (Development and Regulation) Act, 1992 (**FTDR Act**).

Surveillance technology is covered under the category of SCOMET (Special Chemicals, Organisms, Materials, Equipment and Technology) that itemises goods, services and technologies used for civilian and military applications, or 'dual-use items'. The current SCOMET list has nine categories, of which Category 8 is most relevant to harmonizing domestic law with the Wassenaar Arrangement. It is entitled 'Special Materials and Related Equipment, Material, Processing, Electronics, Computers, Telecommunications, Information Security, Sensors and Lasers, Navigation and Avionics, Marine, Aerospace and Propulsion'. Export of dual-use items and technologies under India's Foreign Trade Policy is regulated. It is either prohibited or is permitted under an Authorisation by the DGFT.[38]

1.3.2. Compliance Requirements

Any person who intends to engage in the export of dual-use surveillance goods and technology listed under Category 8 of SCOMET is required to obtain an Importer-Exporter Code (**IEC**) number from the DGFT first, in order to obtain an authorization to export such technology.[39] An entity claiming status as a manufacturer-exporter must establish their credentials as such to the concerned authority.[40]

Exemptions from obtaining IEC are not applicable for export of SCOMET category items as listed in Appendix - 3, Schedule 2 of ITC (HS) except in case of exports by Ministries/Departments of Central or State Government.[41] An

[38]Foreign Trade Policy, Government of India, Ministry of Commerce and Industry, Department of Commerce, (as updated on 02.12.2017), https://dgft.gov.in/sites/default/files/ft17-051217.pdf at para 9.49.
[39] India's Export Control System for SCOMET, Department of Industrial Policy and Promotion, Ministry of Commerce and Industry, http://dgft.gov.in/sites/default/files/SCOMETHelp04092018.pdf at para 2.07. the DGFT is the licensing authority for all items, except 'Category 6' of SCOMET, or the 'Munitions list'. For Category 6, the Ministry of Defence is the licensing authority.
[40]Ibid at para 2.15.
[41] Ibid at para 2.07.

export license is also required for replacement goods or parts thereof for SCOMET items.[42]

The application must be made on the DGFT's online portal[43] along with the requisite documents, including an End-User Certificate in the prescribed proforma.[44] The application is then forwarded by the DGFT to an Inter-Ministerial Working Group (**IMWG**) composed of members from the:

1. Ministry of External Affairs
2. Department of Defence Production
3. Department of Space (through ISRO)
4. Defence Research and Development Organisation (DRDO)
5. Department of Chemicals and Petrochemicals
6. National Authority of Chemical Weapons Convention and
7. Cabinet Secretariat

The IMWG meets on a monthly basis under the Chairmanship of the Additional DGFT to decide on applications.[45] The IMWG decides, by consensus, on whether to approve an export authorization.[46] Pre-license checks are conducted through relevant agencies and India's missions abroad.[47] Post-shipment verifications are also part of licensing conditions.[48]

[42]Ibid at para 2.48.
[43]http://dgftcom.nic.in/CallModule.asp?sch=SCOMET.
[44] Appendix 2S(i), End Use cum User Certificate in Case of Export of SCOMET Items, India's Export Control System for SCOMET, Department of Industrial Policy and Promotion, Ministry of Commerce and Industry, Government of India, http://dgft.gov.in/sites/default/files/SCOMETHelp04092018.pdfat p. 51.
[45] India's Export Control System for SCOMET, Department of Industrial Policy and Promotion, Ministry of Commerce and Industry, Government of India, http://dgft.gov.in/sites/default/files/SCOMETHelp04092018.pdfat p. 3.
[46]Ibid.
[47]Ibid.
[48]Ibid.

In permitting or rejecting the export authorization, the Handbook of Procedures requires that the IMWG take the following criteria into account to arrive at its decision[49]:

a) Credentials of end-user, credibility of declaration of end-use of the item or technology, integrity of chain of transmission of item from supplier to end- user, and the potential of the item or technology, including timing of its export, to contribute to end-uses that are not in conformity with India's national security or foreign policy goals and objectives, goals and objectives of global non-proliferation, or India's obligations under International treaties/Agreements to which it is a State party.
b) Assessed risk that exported items will fall into hands of terrorists, terrorist groups, and non-State actors;
c) Export control measures instituted by the recipient State;
d) Capabilities and objectives of programmes of the recipient State relating to weapons and their delivery;
e) Assessment of end-use(s) of item(s);
f) Applicability of provisions of relevant bilateral or multilateral Agreements and Arrangements, to which India is a party, or adherent. This is including but not limited to the control lists of the Nuclear Suppliers Group, Missile Technology Control Regime, Australia Group (and its Warning List or Awareness Raising Guidelines) and Wassenaar Arrangement (and its Sensitive List and Very Sensitive List) as amended from time to time.

Ordinarily, IECs allotted have permanent validity unless cancelled.[50] However, for SCOMET Items an authorization is valid only for a period of 24 months,[51] subject to alteration at the discretion of the IMWG where a shorter/longer duration authorization may be required in specific cases.[52]

[49]Ibid at para 2.74.
[50]Ibid at para 2.10.
[51]Ibid at para 2.16.
[52]Ibid at para 2.19.

1.3.3. Remedies for Breach of Export Control Regulations

There are penal provisions in the FTDR Act for violation of export laws. Apart from suspension or cancellation of the IEC by the DGFT pursuant to Section 9 the FTDR Act, Section 11 prescribes a fine of upto one thousand rupees (approximately USD 14), or five times the value of goods,[53] whichever is more for any export or import of goods carried out in contravention of the Act, its rules or the export-import policies declared by the Government. This fine may be imposed by the Adjudicating Authority[54] after giving notice in writing to the concerned party.[55] Should a criminal offence be made out, the imposition of such a penalty does not act as a bar to criminal prosecution under other penal statues.[56]

1.4. Other regulations

In addition to the FTP, private actors engaging in security related work may also be governed by the Private Security Agencies (Regulation) Act, 2005 (**PSARA**). This law governs the provision of private security services. *Prima facie*, this law does not regulate those companies that develop and produce surveillance technology, but only those that use it in the ordinary course of their business activities, i.e. provision of security services.[57]

However, it is relevant given that the private security industry is amongst the largest employers in India, employing almost 8.9 million people, with the potential to employ

[53]Section 11(2), Foreign Trade (Development and Regulation) Act, 1992.
[54]The DGFT or any other person authorized by the Central Government to do so on his behalf.
[55]Sections 13 and 14, Foreign Trade (Development and Regulation) Act, 1992.
[56]Section 12, Foreign Trade (Development and Regulation) Act, 1992.
[57] According to Section 2(f) of PSARA, "private security" means security provided by a person, other than a public servant, to protect or guard any person or property or both and includes provision of armoured car service. Section 2(g) defines a "private security agency" means a person or body of persons other than a government agency, department or organisation engaged in the business of providing private security services including training to private security guards or their supervisor or providing private security guards to any industrial or business undertaking or a company or any other person or property. Section 2(h) defines a "private security guard" as a person providing private security with or without arms to another person or property or both and includes a supervisor.

3.1 million more by 2022[58], and the low police to population ratio is likely to facilitate exponential growth in this sector in the coming years.[59]

Human rights obligations of private security agencies (**PSAs**) under the PSARA are restricted to ensuring robust training of private security personnel, and ensuring that any such personnel hired by the PSA do not have any criminal history or antecedents.[60] While there is some provision for training security personnel in 'electronic security', the PSARA provides no definition of surveillance activity or set any standards/ boundaries of what the PSAs may or may not do in the provision of security services. In the absence of comprehensive data protection laws in India, this could mean that these agencies have unfettered power to undertake surveillance activities, whether for intelligence agencies (which as described above are not subject to much parliamentary oversight) or otherwise.

2. Case Studies

2.1. Private companies and State Surveillance

2.1.1. Surveillance systems for law enforcement

As discussed above, our research suggests that among the major surveillance programs that we have information about, only the CCTNS was developed by a private corporation. The Wipro Group is one of India's leading multinational IT companies, and is a signatory to the United Nations (**UN**) Global Compact and supports the UN Guiding Principles on Business and Human Rights.[61] The company does also have a human rights policy, although this policy is largely

[58]http://www.skilldevelopment.gov.in/assets/images/annual%20report/Annual%20Report%202016-2017%20-%20English.pdf as cited in the FICCI and BDO report.

[59]PwC, Indian private security industry: preparing for the next leap, November 2017, at p.6, http://ficci.in/spdocument/20966/FICCI-PwC-Report-on-Private-Security-Industry.pdf accessed on 13.02.2019.

[60]Section 10(1)(c), PSARA 2005.

[61]Wipro Human Rights Policy Statement, https://www.wipro.com/content/dam/nexus/en/sustainability/pdf/Human-Rights-Policy.pdf.

limited to labour / employment practices, and privacy practices in the context of its employees, customers and suppliers.[62]

However, it is doubtful whether the company has any control over the manner in which the CCTNS is utilized by law enforcement agencies. The stipulations of the Request For Proposal under which the company was allotted the contract to develop the CCTNS required that the CAS (Centre) and CAS (State) would be developed by a professional software development agency as the Systems Integrator at the National Crime Records Bureau (**NCRB**) under the overall guidance and supervision of the Ministry of Home Affairs.[63] However, there is no further discussion on the terms of the contract in the context of human rights obligations, and it seems unlikely that a private corporation applying for such a project with widespread applications would be able to negotiate such terms with the Government.

A 2014 study by the Centre for Internet and Society shows that there are however, several other private companies, both Indian and foreign, that develop and sell security solutions in India.[64] The most popular of these solutions appear to be biometric technologies, access control systems, video surveillance and phone monitoring systems.[65] Although limited information is available about government use of the systems developed or manufactured by such private companies, given the pervasive use of complex technology in government surveillance in the face of declining public expenditure on scientific

[62]Wipro Human Rights Policy Statement, https://www.wipro.com/content/dam/nexus/en/sustainability/pdf/Human-Rights-Policy.pdf.

[63] See, for example, E-Governance Mission Mode Project (MMP) for the Crime & Criminal Tracking Network and Systems (CCTNS): Request for proposal for Selection of System Integrator for Implementation, Commissioning and Maintenance of CCTNS in Maharashtra state, Volume I: Techno-Functional Requirements, http://www.ncrb.gov.in/BureauDivisions/CCTNS/All%20State%20RFP/Maharashtra/Tender1.pdfat p. 42, para 3.1.

[64]Maria Xynou, The Surveillance Industry in India, March 2014, available at https://cis-india.org/internet-governance/blog/surveillance-industry-india.pdf.

[65]Maria Xynou, The Surveillance Industry in India, March 2014, available at https://cis-india.org/internet-governance/blog/surveillance-industry-india.pdf.

R&D, private IT companies in the country have demonstrated their openness to collaborating with, and marketing their products and services to government agencies.

This Government on its part also promotes the use of many of these systems from a law enforcement perspective. In particular, it has begun to promote the use of security and surveillance through various initiatives, for instance, the Ministry of Home Affairs has issued guidelines for the security of children within school premises through CCTV cameras.[66] The installation of CCTV cameras in public areas and public transport has also been pushed as a solution to issues around women's safety.[67]

2.1.2. Social media and encrypted communication services

Between 2008 and 2012, the Indian Government engaged in discussions with telecommunication services providers and Research in Motion (**RIM**), the makers of the 'Blackberry' phones, on the interception of encrypted messages and communication on Blackberry devices.[68] The Government stated that telecom services would not be permitted on these devices, if the lawful interception requirements could not be met. The Indian government demanded that servers or facilities be set up in India, that would allow them access to otherwise secure communications, a demand that was amplified after reports that RIM had agreed to do the same in countries like China and Saudi Arabia.

[66]MHA, cops blamed for CCTV project 'failure', THE HINDU, December 20, 2018, available at https://www.thehindu.com/news/cities/Delhi/mha-cops-blamed-for-cctv-project-failure/article25785377.ece.

[67]Jatin Anand, State-run buses to be equipped with CCTV cameras soon, THE HINDU, March 26, 2018, available at https://www.thehindu.com/news/cities/Delhi/state-run-buses-to-be-equipped-with-cctv-cameras-soon/article23350840.ece.

[68]Chris Velazco, Indian Government To Launch BlackBerry Messenger Snooping System 'Soon', TECH CRUNCH, available at https://techcrunch.com/2012/04/09/indian-government-to-launch-blackberry-messenger-snooping-system-soon/.

In 2012, RIM conceded to the Indian government's requests and set up a server in Mumbai to permit lawful interception.[69]

Currently, with reports of increasing use of social media and private communication services to spread misinformation, often with violent consequences, the Indian Government is once again looking into measures to trace the sharing of such information.[70] The Government has been in discussions with representatives of Whatsapp since mid-2018 to find technology based solutions to the problem. It has also proposed controversial changes to the laws that provide intermediaries with safe harbour from liability for content shared by their customers, with the aim of addressing this issue[71], as well as requirements for all companies that collect or process the personal data of Indian citizens to maintain local copies of such data to assist law enforcement activities[72].

At the same time, reports suggest that the Central Bureau of Investigation has issued a notice requiring social media platforms to use Microsoft's Photo DNA software (primarily meant for detection of child pornography), for the purpose of regular criminal investigations.[73]

It remains to be seen whether these private entities will cooperate with the Government, and what kind of measures they implement if they do.

We note that discussions with both RIM and Whatsapp were / are on the basis of requirements for lawful interception under the Telegraph Act and IT Act

[69]Sanjay Singh, No secrets on BlackBerry: Govt gets its way on tapping popular messenger service, INDIA TODAY, April 7, 2012, available at https://www.indiatoday.in/business/india/story/govt-to-tap-blackberry-messenger-security-privacy-98321-2012-04-07.

[70]Surabhi Agarwal, WhatsApp executives meet government to discuss traceability, , THE ECONOMIC TIMS, December 7, 2018, available athttps://economictimes.indiatimes.com/tech/internet/whatsapp-executives-meet-government-to-discuss-traceability/articleshow/66979532.cms.

[71]Draft Information Technology [Intermediary Guidelines (Amendment) Rules] 2018.

[72]Draft Personal Data Protection Bill, 2018.

[73] Sushant Singh, CBI asks social media firms to use intrusive photo tech to track suspects, THE INDIAN EXPRESS, December 31, 2018, available at https://indianexpress.com/article/india/cbi-surveillance-photodna-microsoft-facebook-youtube-twitter-5516347/.

discussed above. Other service providers are required to and have reported compliance with such lawful interception requests as well.[74] However, we note that efforts such as publication of transparency reports, which are now common among the large multinational companies, are limited in the context of Indian companies. One possible reason for this is the confidentiality requirements imposed on service providers under the IT Rules.[75] However, reporting that is not barred by these rules is also limited.

2.2. Private companies providing other services

2.2.1. Biometric identity system – Aadhaar

The use of biometric technologies in the government's favoured national identity project – Aadhaar, has also led to a proliferation of technology used to read and authenticate fingerprints. The Aadhaar system also currently captures irises of enrolled individuals and has also commenced the use of facial recognition technology[76].

The Aadhaar project was challenged before the Supreme Court in 2012, on the grounds that it violated the privacy of enrolled individuals, and was cause for security concerns, among other things. As the case remained before the Supreme Court for over 5 years, one of the other issues that became increasingly apparent was the involvement of the private sector in the development of Aadhaar infrastructure with limited transparency, as well as the growing number of private companies that based their business models almost entirely on the use of Aadhaar related personal data. These concerns were exacerbated by the fact that the same individuals moved in and out of the

[74]See for instance Transparency Reports published by Google and Facebook.

[75]Rules 21, 24 and 25 of the IT Rules impose confidentiality requirements on intermediaries that are involved in interception or monitoring or decryption of any information.

[76]Pankaj Doval, Face recognition to be must for all Aadhaar authentications, TIMES OF INDIA, August 24, 2018, available at https://timesofindia.indiatimes.com/india/face-recognition-to-be-must-for-all-aadhaar-authentications/articleshow/65522828.cms.

regulatory authority and these private companies in a sort of 'revolving door' set up.[77]

In 2018, the Supreme Court's judgment in relation to the constitutional challenge against the Aadhaar project upheld the identity system as used by the Government as valid, but restricted private sector use of the Aadhaar number and related information.[78]However, much of the technology behind the Government's use of Aadhaar is / was supported by services and products offered by private companies. For instance, 4G Identity Solutions, L-1 Identity Solutions are providing multiple biometric authentication services[79], and iris recognition technology[80] and BioEnable Technologies provided scanners at passports offices and Aadhaar enrolment centres[81].It is not clear what role these service providers will continue to play in the Aadhaar ecosystem. Since the Supreme Court's judgment on the matter, the Government has also proposed amendments to the Aadhaar Act, 2016, to allow for limited private sector use of Aadhaar related personal information, among other things.[82] While the majority of the 5 judge bench of the Supreme Court upheld the constitutional validity of the Aadhaar project, Justice Chandrachud, in his dissent noted the potential for surveillance by the use of Aadhaar related personal data.[83]

[77]Aria Thaker, The New Oil: Aadhaar's mixing of public risk and private profit, THE CARAVAN, May 1, 2018, available at https://caravanmagazine.in/reportage/aadhaar-mixing-public-risk-private-profit.
[78]K. S. Puttaswamy v. Union of India, (2018) 12 SCALE 1.
[79]World's Largest Civil ID, 4G Identity Solutions, http://www.4gid.com/civilachievements.html
[80]World's Largest 1:N Real-time Identification System, 4G Identity Solutions, http://www.4gid.com/citizenachievements.html.
[81]Aadhaar Solutions, BioEnable, https://www.bioenabletech.com/aadhaar-solutions.
[82]Namita Singh, What does the Aadhaar and Other Laws (Amendment Bill), 2018 do?, MEDIANAMA, January 3, 2019, available at https://www.medianama.com/2019/01/223-what-does-the-aadhaar-and-other-laws-amendment-bill-2018-do/.
[83]K. S. Puttaswamy v. Union of India, (2018) 12 SCALE 1.

2.2.2. Social Media Monitoring

In April 2017, the Ministry of Information and Broadcasting issued a bid document for the creation of a social media analytical tool, to monitor and gauge citizen's opinions about government policies.[84] The information collected using this tool was to be used to target individuals with personalised campaigns to promote "positive" opinions and to neutralise "negative sentiments" about government schemes.[85] The bid document suggested that the tool would be used to monitor all communication, on social media websites, as well as on private communication services including email.[86]

While this tool was not meant to be used for intelligence or law enforcement purposes, it did nonetheless raise significant privacy concerns, given that India does not have comprehensive data protection or surveillance laws. This bid document was questioned before the Supreme Court, where the bench observed that this could lead to the creation of a 'surveillance state', post which the Central Government informed the Court that the notification for setting up the system had been withdrawn.[87]

It is relevant to note however, that prior to being withdrawn, the timeline for submitting bids in response to the document had been extended multiple times

[84]Kumar Sambhav Shrivastava, Government plans to monitor individual social media users to gauge opinion about official policies, SCROLL.IN, May 25, 2018, available at https://scroll.in/article/879833/government-plans-to-monitor-individual-social-media-users-to-gauge-opinion-about-official-policies.

[85]Kumar Sambhav Shrivastava, Government plans to monitor individual social media users to gauge opinion about official policies, SCROLL.IN, May 25, 2018, available at https://scroll.in/article/879833/government-plans-to-monitor-individual-social-media-users-to-gauge-opinion-about-official-policies.

[86]Request for Proposals (RFP) invited for Selection of Agency for SITC of Software and Service and Support for function, operation and maintenance of Social Media Communication Hub, Ministry of Information and Broadcasting, Government of India, RFP Ref No: BECIL/Social Media/MIB/02/2018-19, April25 2018, available at www.becil.com/uploads/tender/TendernoticeBECIL01pdf-04836224e38fdb96422221c4e057f6c5.pdf.

[87]Social media hub: Centre tells SC it is withdrawing plan, will review the policy, SCROLL.IN, August 3, 2018, available at https://scroll.in/latest/889083/social-media-hub-centre-tells-sc-it-is-withdrawing-plan-will-review-the-policy.

because of a lack of proposals. The bid was opened to Indian companies only, and reports suggest that Indian companies were not clear on whether the project was sustainable given the nature of resources and capacity available to them at the time.[88]

[88]Kumar Sambhav Shrivastava, Government plans to monitor individual social media users to gauge opinion about official policies, SCROLL.IN, May 25, 2018, available at https://scroll.in/article/879833/government-plans-to-monitor-individual-social-media-users-to-gauge-opinion-about-official-policies.