SFLC.IN
K-9, Second Floor, Birbal Road,
Jangpura Extension,
New Delhi-110014
(tel): +91-11-43587126
www.sflc.in

To,

Mr. David Kaye,

Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression,

Office of the United Nations High Commissioner for Human Rights (OHCHR).

e-mail: freedex@ohchr.org

[*Via electronic distribution*]

Date: 15 February 2019

Subject: Submission: The Surveillance Industry and Human Rights

About SFLC.in

SFLC.in is a New Delhi based not-for-profit organization that brings together lawyers, policy analysts, technologists and students to protect freedom in the digital world. We promote innovation and open access to knowledge by helping developers make great Free and Open Source Software (FOSS), protect digital civil liberties by providing pro-bono legal advice, and help policymakers make informed and just decisions with the use and adoption of technology.

In 2014, SFLC.in published a report on 'India's Surveillance State'.[1]

We hope that our submission proves useful for safeguarding the rights of people in an increasingly digital world.

Please feel free to contact us for any clarification or further information.

Surveillance in India

Multiple Indian legislations, including the Indian Telegraph Act, 1885 and Rules thereunder,

1 India's Surveillance State by SFLC.in, available at https://sflc.in/sites/default/files/wp-content/uploads/2014/09/SFLC-FINAL-SURVEILLANCE-REPORT.pdf. Last accessed on 15 February 2019.

Information Technology Act, 2000 and Rules thereunder and the Code of Criminal Procedure, contain explicit provisions that allow Central and State Governments to intercept and monitor the nation's communication networks on several grounds. A number of Lawful Interception and Monitoring (LIM) systems have been also installed into India's telephone and Internet networks in accordance with the service licenses.

1. Laws, administrative regulations, judicial decisions, or other policies and measures that impose regulations on the export, import or use of surveillance technology:

1.1 - Laws on telephone tapping:

i) Provisions regulating telephone tapping:

- Section 5 of Indian Telegraph Act, 1885 (hereinafter referred to as "Telegraph Act") empowers governments to take possession of licensed telegraphs and to order interception of messages.
- Rule 419A under Section 5(2) of the Indian Telegraph Rules, 1951 provides the procedures governing telephone tapping.

ii) Provision on unauthorized access of communications**:**

- Section 24 read with Section 23 of the Telegraph Act prescribes punishment for unlawfully learning the contents of any message.
- Section 26 of the Telegraph Act lays down punishment for unlawful interception or disclosure of messages by telegraph officer or any person performing official duties connected with any office used as a telegraph office.
- Section 43 of the Information Technology Act, 2000 (hereinafter referred to as "IT Act") lays down penalties for damage to computer, computer system, etc. in absence of permission of the owner or any other person in charge.
- Section 72 of the IT Act imposes a penalty for disclosure of information without consent of the person concerned, if such information is disclosed by a person authorized to access information under the Act, rules or regulation.

1.2 - Laws on Internet surveillance:

Internet surveillance is governed by the following provisions under the Information Technology Act, 2000 in addition to the framework for telephone surveillance:

- Section 69 is concerned with surveillance of internet. It empowers Central or State Government or officers specially authorized by the Government to issue directions for interception or monitoring or decryption of any information through any computer resource.
- Section 69B is concerned with surveillance of Internet meta-data. It empowers Central Government to authorize any agency of the Government to monitor and collect traffic data or information through any computer resource for cyber security. 'Information Technology

(Procedure and Collecting Traffic Data or Information) Rules, 2009' have been issued under this section.

- Sections 69 and 69B together set the stage for direct surveillance of Internet and internet metadata respectively. More provisions of the Act allow indirect surveillance.
- Section 28 empowers the Controller of Certifying Authorities (CCA) or authorized officers to investigate contraventions of the Act, rules or regulations made thereunder.
- Section 29 empowers CCA or authorized officers the power to access computers and their data, on a reasonable cause to suspect that contravention of the Act has taken place. Rule 3(7) of the 'Information Technology (Intermediaries Guidelines) Rules, 2011' requires that intermediaries such as ISPs and on-line portals must provide information or any assistance to authorized government agencies for the purpose of identity verification, prevention or investigation of offences, etc.
- Rule 7 of the Information Technology (Guidelines for Cyber Cafe) Rules, 2011 directs cyber cafe owner to provide every related document, register and necessary information to inspecting officer authorized to check cyber cafe and computer resources or network established therein.
- Offences relating to unauthorized access can be found under Section 43,[2] Section 43A,[3] Section 66 B,[4] Section 72,[5] Section 72A.[6]

1.3 - Other laws that facilitate surveillance:

- Section 91 of the Code of Criminal Procedure, 1973 empowers officer in charge of a police station to issue summons to produce document or other thing.

1.4 - Telecom Licenses:

Fixed-line/mobile telephone and internet services are governed under the Unified License (UL).[7] This license exists in the form of an agreement between the Department of Telecommunications (DOT) and communications service providers.

i) General conditions:

- License agreements require their licensees to furnish 'all necessary means and facilities as required' for the application of Section 5 of the Telegraph Act.[8]
- For security, licensees must provide 'suitable monitoring equipment' as per the requirement of the DOT or Law Enforcement Agencies (LEAs).

2 Penalty and compensation for damage to computer, computer system etc.
3 Liability for body corporate for failure to protect data and compensation.
4 Punishment for dishonestly receiving stolen computer resource or communication device.
5 Penalty for breach of confidentiality and privacy and other related offences.
6 Punishment for disclosure of information in breach of lawful contract.
7 Unified License, available at http://dot.gov.in/sites/default/files/Amended%20UL%20Agreement_0_1.pdf?download=1. Last accessed on 15 February 2019.
8 Condition 32.2, Part I, UL.

- Government can also issue specific orders or directions in the interests of security.[9]
- Licensees are obliged to provide all tracing facilities to trace nuisance and obnoxious/ malicious communications passing through their networks, when such information is required for investigations or detection of crimes, and in the interest of national security.[10]
- Licensees must provide 'necessary facilities' depending upon the specific situation at the relevant time, to counteract espionage, subversive act, sabotage or any other unlawful activity.[11]

ii) Telephone tapping obligations:

- Designated Central/State Government officials, apart from the DOT and its nominees, may access telephone-tapping systems installed into the licensees' networks.[12]
- If monitoring equipment is located in premises of licensee, the licensees should extend all support in this regard including Space and Entry of the authorized security personnel.[13]
- Licensees must record call details such as location, telephone numbers, date and time of call, among others.[14]

iii) Internet surveillance obligations:

- ISPs are required to maintain copies of all packets originating from their equipment and these must be available in real time to the Telecom Authority.[15]
- There are more relevant clauses in the Unified License.[16]

2. Remedies available in the event of illicit use of private surveillance technology under Information Technology Act:

2.1 - Surveillance by parties:

- Section 43 provides for a penalty and compensation for damage to computer, computer system, etc. It contains provisions against intrusion in computer systems, copying files without authorization, among others.

9 Condition 39.2, Part I, UL.
10 Condition 38.2, Part I, UL.
11 Condition 39.1, Part I, UL.
12 Condition 8.2, Part II, Chapter VIII, UL.
13 Condition 8.2, Part II, Chapter VIII, UL.
14 Condition 8.3, Part II, Chapter VIII, UL.
15 Condition 8.2, Part II, Chapter VIII, UL.
16 See Condition 39.12, Part I, UL; Condition 7.3, Part II, Chapter IX, UL; Condition 8.1.1, Part II, Chapter IX, UL; Condition 8.2, Part II, Chapter IX, UL; Condition 8.3, Part II, Chapter IX, UL; Condition 8.2, Part II, Chapter VIII, UL; Condition 39.23(x), Part I, UL; Condition 8.5, Part I, UL; Condition 7.1, Part II, Chapter IX, UL; Condition 7.2, Part II, Chapter IX, UL; and Condition 37.1, Part I, UL.

- Section 46 provides for "adjudicating officer",[17] having powers of civil court, to adjudicate whether any person has committed any contraventions under Chapter IX of the Act.[18]
- Section 66 provides a fine and imprisonment, and Section 43A provide for compensation for failure to protect data due to breach by body corporate.

2.2 - Surveillance by government:

- There is no direct remedy available. People can approach the courts under Article 32 and Article 226 of the Constitution whereby citizens can seek redressal for the violation of their right to privacy, which is a fundamental right.

3. Whether the laws, regulation, or policies identified are consistent with State obligations under Article 19 of the ICCPR, Art 19 of UDHR and other relevant human right standards:

3.1 - Human Rights concerns in Indian context:

- There is lack of transparency in India's communications surveillance and absence of independent oversight. Enabling Acts and Rules always stipulate the observance of strict confidentiality in the surveillance process, thereby significantly limiting the amount of information on surveillance practices that is available to the public. There is lack of judicial intervention at any stage of the surveillance process and no law requires judicial oversight in any capacity. As per the current procedure, the orders for interception / monitoring are issued by the Executive and the review is also conducted by the Executive. For example, Indian Telegraph Rules and the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 provide for the establishment of a Review Committee comprising solely of the Executive for reviewing surveillance directives. This severely compromises its independence and impartiality.
- Communications surveillance is currently permitted on various vaguely/broadly worded grounds, including but not limited to, protection of national security and prevention of spread of computer viruses. Several such grounds do not qualify as legitimate aims. Effectively, unrestricted communication surveillance can be conducted on anyone at any time, thereby violating the Right to Privacy.
- The nation's communication networks are effectively under perpetual surveillance. Considering the sheer volume of lawful orders issued, it is difficult to determine whether the possibility of a less intrusive alternative is considered on a case-by-case basis.
- Rule 419A(3) of the Indian Telegraph Rules 1951 and Rule 8 of the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 stipulate that 'other reasonable means' must be considered and exhausted before issuing an interception or monitoring order under the Rules. However, surveillance systems like NETRA (Network Traffic Analysis) perpetually monitor communication

17 The Information Technology (Qualification and Experience of Adjudicating officers and Manner of Holding Enquiry) Rules, 2003.
18 Chapter IX contains clauses on penalties, compensation and adjudication.

networks and call into question the whole premise of these Rules since continuous availability of intercepted data would have the effect of dispensing with the very need to resort to other less intrusive means. Despite assurances that the Central Monitoring System (CMS) operates strictly in accordance with the procedures laid down by Rule 419A, its capability for Direct Electronic Provisioning, i.e. automated instantaneous interception without involvement of service providers, runs foul of this procedure.

- Similarly, there are no provisions of law that provide for the conduct of mass surveillance of any kind, bringing into question the legality of NETRA which scans the nation's internet traffic for trigger words and phrases like "bomb", "blast" using predefined filters.[19] Media reports heightened such privacy concerns as recently as May 2018. These reports revealed the intention of the government to deploy social media analytical tool to gauge opinions of people on official policies.[20] [21] [22]
- The principle of transparency is *prima facie* violated by Indian communications surveillance. CMS and NETRA are sanctioned by high-level ministerial committees without adequate parliamentary dialogue. However, little to no information is publicly shared regarding surveillance initiatives and even purely procedural information such as internal guidelines requested under the Right to Information Act, 2005 are consistently denied citing national security. Similarly, not much is known about procedural safeguards and governing laws concerning National Intelligence Grid (NATGRID) which has been envisioned as a counter-terrorism initiative that collates data from 21 databases belonging to various government agencies including tax, travel, etc.
- There are no provisions of law whereby users are notified when their communications are subjected to surveillance, and no distinction is made between situations where such notification would defeat the purpose of surveillance and otherwise. By extension, users also lack the ability to appeal the decision to surveillance of their communications.
- Service providers are prohibited by service licenses from employing bulk encryption. This compromises the general security of communications networks by facilitating not only surveillance initiatives, but also malicious and targeted attacks from non-state parties.
- Privacy is a fundamental right[23] implicit under Article 21 of the Constitution of India but India currently does not have a data protection law. Its absence raises major privacy concerns such as those regarding The Aadhaar (Targeted Delivery of Financial and other

19 'Panel slams roping in of private firm for net snooping', available at https://www.thehindubusinessline.com/info-tech/Panel-slams-roping-in-of-private-firm-for-Net-snooping/article20406835.ece. Last accessed on 15 February 2019.

20 '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', available at http://www.becil.com/uploads/tender/TendernoticeBECIL01pdf-04836224e38fdb96422221c4e057f6c5.pdf. Last accessed on 15 February 2019. This tender was later withdrawn.

21 'Social Media Communications Hub: A Privacy Nightmare', available at https://sflc.in/social-media-communications-hub-privacy-nightmare. Last accessed on 15 February 2019.

22 '40 government departments are using a social media surveillance tool – and little is known of it', available at https://scroll.in/article/893015/40-government-departments-are-using-a-social-media-surveillance-tool-and-little-is-known-of-it. Last accessed on 15 February 2019.

23 Justice K.S. Puttaswamy (Retd.) and Another V. Union of India, 2018 (9) SCJ 224

Subsidies, Benefits and Services) Act, 2016 [24] which has the potential of being misused for surveillance.

3.2 - Recent development

- The Ministry of Home Affairs issued a circular on 20 December 2018 under Section 69 of the IT Act, authorizing ten government agencies to conduct electronic surveillance.[25] The Supreme Court on January 25th 2019 issued a notice to MHA on a plea filed by PUCL challenging the circular.

4. Relevant judicial decisions:

- KS Puttaswamy v. UOI [WP (C) 494 of 2012][1] ("Privacy Judgment"): The Supreme Court held that "*the right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III (fundamental rights) of the Constitution.*"[26]
- KS Puttaswamy v. UOI [W.P. (C) 494 of 2012] ("Aadhaar Judgment"): The Supreme Court upheld constitutionality of Aadhaar Act, 2016 barring a few provisions on disclosure of personal information, cognizance of offences and use of the Aadhaar ecosystem by private corporations.
- PUCL v. Union of India [AIR 1997 SC 568]: The Supreme Court defined the terms "public emergency" and "public safety" to mean "*the prevalence of a sudden condition or state of affairs affecting the people at large calling for immediate action"*, and *"the state or condition of freedom from danger or risk for the people at large"* respectively. The case started after a CBI inquiry on allegations from the opposition party of phone-tapping of high ranking politicians by the government. Judicial oversight of phone interception was held as unsustainable in the lack of express legal provisions that provide for such oversight, however other limitations were put in place such as a limit of two months on the validity of a phone tapping order.
- Kharak Singh v. State of Uttar Pradesh & Ors. [(1964) 1 SCR 332], Govind v. State of Madhya Pradesh [(1975) 2 SCC 148], R R Gopal & Anr. v. State of Tamil Nadu [(1994) 6 SCC 332]: The Court examined violation of privacy in these cases.

24 Upheld by the Supreme Court in Justice K.S. Puttaswamy (Retd.) and Another V. Union of India, Write Petition (Civil) No.494 of 2012. Alternate citation is 2018 (9) SCJ 224. In his dissenting judgement J. D.Y. Chandrachud warned once a biometric system is compromised, it is compromised forever.

25 These include the Intelligence Bureau, Narcotics Control Bureau, Enforcement Directorate, Central Board of Direct Taxes, Directorate of Revenue Intelligence, Central Bureau of Investigation; National Investigation Agency, Cabinet Secretariat (R&AW), Directorate of Signal Intelligence (For service areas of Jammu & Kashmir, North-East and Assam only) and Commissioner of Police, Delhi.

26 WP (Civil) No. 494 of 2012, available at https://www.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf. Last accessed on 28 January 2019.

5. The extent to which private surveillance companies offer services to States and other actors to deploy their technologies in specific circumstances, and the extent to which companies are aware of the end-use of the technologies they market:

Many private surveillance companies are involved in selling surveillance equipments in India. An RTI application filed by SFLC.in revealed that 26 companies had expressed their interest in tender floated in 2014 by Director General for Police, Logistics and Provisioning for Internet monitoring systems. The full list of these companies can be accessed on Pages 22 and 23 of SFLC.in's report "India's Surveillance State".[27]

With Regards,

Biju K. Nair,

Executive Director,

SFLC.in

27 See Footnote No. 1 above.