Response to Call for Submissions: The Surveillance Industry and Human Rights

February 15, 2019

By: Elonnai Hickok, Arindrajit Basu, Gurshabad Grover, Akriti Bopanna, Swetha Mohandas, and Martyna Kalvaityte

The Centre for Internet and Society, India

Preliminary

The Centre for Internet and Society (CIS) is a non-profit organisation that undertakes interdisciplinary research on the internet and digital technologies from policy and academic perspectives. Through its diverse initiatives, CIS explores, intervenes in, and advances contemporary discourse and practices around the internet, technology and society in India, and elsewhere.

CIS is grateful for the opportunity to submit the United Nations (UN) Special Rapporteur on call for submissions on the surveillance industry and human rights.[1] Over the last decade, CIS has worked extensively on research around state and private surveillance around the world. In this response, individuals working at CIS wish to highlight these programs, with a special focus on India.

Submission

A. Information concerning the domestic regulatory frameworks that may be applicable to the development, marketing, export, deployment, and/or facilitation of surveillance technologies by private companies, such as:

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

Import and export

India has export controls on dual-use technology. Imports and exports are regulated by the Foreign Trade (Development and Regulation) Act, 1992. The Act empowers the Directorate General of Foreign Trade (DGFT) to license items for export and control through the Indian Tariff Classification list. One of these lists - the Special Chemicals, Organisms, Materials, Equipment, and Technologies (SCOMET) list - controls the export of dual use technologies.[2]

A DGFT notification in April 2017 added "Special Materials and Related Equipment, Material, Processing, Electronics, Computers, Telecommunications, Information Security, Sensors and Lasers, Navigation and Avionics, Marine, Aerospace and Propulsion" to the SCOmet list,[3] and

[1] UN Special Rapporteur on Freedom of Expression, "Call for Submissions: The Surveillance Industry and Human Rights", UN Special Rapporteur on Freedom of Expression, January 2019, https://freedex.org/2018/12/13/call-for-submissions-the-surveillance-industry-and-human-rights/
[2] Elonnai Hickok, "Export and Import of Security Technologies", *Centre for Internet and Society,* March 2015, https://cis-india.org/internet-governance/blog/export-and-import-of-security-technologies-in-india.pdf
[3] Directorate General of Foreign Trade, "Amendment in Table A of Schedule 2 and Appendix 3 of ITC(HS) Classification of Export and Import Items", *Directorate General of Foreign Trade,* April 2017, http://dgft.gov.in/sites/default/files/Notification5-English_0.pdf

harmonised India's export control regime with the requirements in the Wassenaar Arrangement.[4] India was admitted into the Wassenaar Agreement in December 2017.[5]

However, the European Commission's approach while expanding the SCOMET list also attempts to address surveillance technologies. This is something India does not have yet.

The additional regulatory mechanisms put forward by the EU include:

(1) Proposed EU wide autonomous list for surveillance, although this reform is now being challenged.[6]

(2) Targeted catch-all control which includes additional language restricting dual use items when " there is evidence that the items may be misused by the proposed end-user for directing or implementing serious violations of human rights or international humanitarian law in situations of armed conflict or internal repression in the country of final destination"[7]

Use

State surveillance in India is governed by several legal provisions[8, 9], including:

- Sections 91 of the Code of Criminal Procedure, 1973 empowers Courts and police officers heading a station to issue summons for the "production of any document or other thing" if they deem it necessary or desirable for any investigation or trial. This provision has also been used to access stored data and request information from intermediaries.[10] Section 92 permits judicial authorities to order a "postal or telegraph authority" for interception of "any document, parcel, or thing".
- Section 5(2) of the Telegraph Act, 1885 allows the Government to intercept telephone/telegraph communication if two tests are met: (i) that there is public interest or public safety involved, and (ii) the authorised official is satisfied that the interception is necessary for maintaining public order or the security/integrity of India. Rule 419A of the Indian Telegraph Rules, issued under the Act in 2007, provides the procedure for such interception, including processes, period of interception, relevant sanctioning authority, and the review process.

---

[4] Sairam Sanath Kumar, "What India's New Export Control Regime Means for its Software Industry", *The Wire,* April 2018, https://thewire.in/tech/india-new-export-control-regime-software-industry

[5] Wassenaar Agreement Plenary Chair, "STATEMENT ISSUED BY THE PLENARY CHAIR ON 2017 OUTCOMES OF THE WASSENAAR ARRANGEMENT ON EXPORT CONTROLS FOR CONVENTIONAL ARMS AND DUAL-USE GOODS AND TECHNOLOGIES", *Wassenaar Agreement,* December 2017, https://www.wassenaar.org/app/uploads/2017/12/WA-Plenary-2017-Chairs-Statement.pdf

[6] https://www.accessnow.org/eu-states-push-to-relax-rules-on-exporting-surveillance-technology-to-human-rights-abusers/

[7] Ben Wagner and Stephanie Horth, " Digital Technologies, Human Rights and Global Trade? Expanding export controls of surveillance technologies in Europe, China and India" in Research Handbook on Human Rights and Digital Technology: Global Politics, Law and International Relations (EE Elgar, 2019)

[8] Vipul Kharbanda, "Policy Paper on Surveillance in India", *Centre for Internet and Society,* August 2015, https://cis-india.org/internet-governance/blog/policy-paper-on-surveillance-in-india

[9] Rishab Bailey, Vrinda Bhandari, Smriti Parsheera, and Faiza Rahman, "Use of personal data by intelligence and law enforcement agencies", *National Institute of Public Finance and Policy,* August 2018, http://macrofinance.nipfp.org.in/PDF/BBPR2018-Use-of-personal-data.pdf

[10] *Ibid, citing* Software Freedom Law Centre, "India's surveillance state: Other provisions of law that enable collection of user information", 2015, https://sflc.in/indias-surveillance-state-other-provisions-of-law-that-enable-collection-of-user-information

- Section 69 of the IT Act empowers authorised government agencies to "intercept, monitor or decrypt" information in computer resources. The scope of such interception is permitted in cases permitted by the Telegraph Act, and "defence of India" and "investigation of any crime." Most pertinently, Section 69(3) obligates online intermediaries to "extend all facilities and technical assistance" to the relevant authorised agency. Section 69B is even broader, and allows authorised agencies to "monitor and collect traffic data or information [...] for cyber security"[11] Rules issued under the IT Act under other provisions also allow for governmental agencies to access information held by private entities: the IT (Reasonable Security Practices and Sensitive Personal Data or Information Rules), 2011, Rule 3(7) of the IT (Intermediaries Guidelines) Rules, 2011, and Rule 7 of the IT (Guidelines for Cyber Cafe) allow for such access in different conditions.
- Telecom service providers are mandated under the Unified Access Services License Agreement to undertake a range of measures to facilitate state surveillance. For example all of Telecom Service Providers and Internet Service Providers operating in India have integrated Interception Store & Forward servers in their networks.[12] All voice calls, SMS, MMS, video calls, GSM and unencrypted data in transit straightforwardly and without a warrant subsequently lands in India's Central Monitoring System.[13] Service providers are also required to connect their infrastructure directly with regional centres of the Central Monitoring System (CMS). The CMS is "a centralized system to monitor communications on mobile phones, landlines and the internet in the country."[14]

2. Remedies available in the event of illicit export or use of private surveillance technology

Prohibition of unauthorized surveillance

The Central Government notified the Supreme Court's procedural safeguards as Rule 419A of the Telegraph Rules, 1951 under the Telegraph Act. The rules state that: only a home secretary from the central or state government can authorize a wiretap; requests for interception must specify how the information will be used; each order unless cancelled earlier will be valid for 60 days and can be extended to a maximum of 180 days; a review committee at the central/state level will validate the legality of the interception order; before an interception order can be approved, all other possibilities of acquiring the information must be considered;4 the review committee can revoke orders and destroy the data intercepted; records pertaining to an interception order maintained by intelligence agencies will be destroyed every six months, unless required for functional purposes, and records pertaining to an interception maintained by the service provider will be destroyed every two months. Though provision 14 and 15 of the Rules prohibit unauthorized interception by service providers and provide penalty for the same, the

[11] "Traffic data" is defined as "any data identifying or purporting to identify any person, computer system or computer network", and also includes metadata.
[12] Udbhav Tiwari, "The Design & Technology behind India's Surveillance Programmes," *The Centre for Internet & Society*, 20 January, 2017, <https://cis-india.org/internet-governance/blog/the-design-technology-behind-india2019s-surveillance-programmes>
[13] Maria Xynou, "India's Central Monitoring System (CMS): Something to Worry About?"*The Centre for Internet & Society*, 30 January, 2014, https://cis-india.org/internet-governance/blog/india-central-monitoring-system-something-to-worry-about.
[14] Ministry of Communications, "Centralised System to Monitor Communications", *Press Information Bureau*, August 2018, http://pib.nic.in/newsite/PrintRelease.aspx?relid=54679

provisions do not extend to intelligence agencies and the rules do not provide remedy to the individual if they are the subject of unauthorized surveillance. A similar provision exists in the Rules framed under section 69 of the IT Act - provision 24(1) prohibits any person intentionally intercepting communications without authorisation. Remedy is further hindered in India's present surveillance framework as under provision 25 of the Information Technology Act Rules - service providers are prohibited from disclosing information about governmental requests and orders. The lack of remedy in India's surveillance regime has been noted by the Justice AP Shah committee in their report recommending a privacy framework for India.[15]

History of case law

In India, the right to privacy has been almost exclusively a judicial construct. Beginning (coincidentally) with a dissenting opinion by Justice K Subba Rao in the Kharak Singh v State of Uttar Pradesh and Others (1964), the Supreme Court was initially opposed to accepting the right to privacy on the grounds that it finds no mention in the Fundamental chapter of the Constitution. However, various later benches of the Apex Court held privacy as an integral part of Article 21, the Right to Life and Personal Liberty. In the case Govind v. State of Madhya Pradesh (1975), when deliberating on the validity of police regulations that had been challenged on the grounds of violating privacy, the court held privacy was a right but was not absolute and can be curtailed by the state in an instance of 'compelling public interest'. In fact, the issue of surveillance in criminal investigation and telephone tapping was specifically addressed in this regard by the Court in People's Union for Civil Liberties v. Union of India and Another (1997), where the Court upheld the right as applicable in India. However, little or no enforcement followed, and the Information Technology Act 2000 (and the associated rules) continued the laissez-faire scenario with overarching powers to intelligence agencies to carry on surveillance exercises till the famous case of KS Puttaswamy v Union of India.

KS Puttaswamy v Union of India

The nine judges, through six concurring opinions held that privacy is a constitutionally protected right that emerges from the right to life and liberty guaranteed by Article 21 of the constitution, which is inseparable from the right to live with dignity. In doing so, it explicitly overturned the prior Supreme Court rulings in Kharak Singh to the extent that they were incompatible with this verdict.

It was clarified that the judiciary did not create a new right in this case but merely granted recognition to a right that already existed as the 'constitutional core of human dignity,' privacy, wrote Justice Chandrachud in the opinion authored by him and concurred to by Justices Kehar, Nazeer and Agarwal, is essentially the reservation of a private space for an individual founded on the autonomy of the individual. Of course, it stopped short of enumerating the variety of entitlements or interests that come within the umbrella of the right to privacy. Instead, they left it for future judges to carve out such entitlements depending on the needs of the time, given the nature of the constitution as a 'living document.'

---

[15] In 2012 the Report on the group of experts on privacy headed by Justice A.P.Shah provided recommendations and framework for India's privacy legislation. The A.P Shah report while citing the different case laws on state surveillance in India, stated that surveillance is a part of the different dimensions of the privacy that the proposed legislation should look at and that India's present surveillance framework should be brought inline with the proposed nine privacy principles. http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf pg. 60

It did, however, clarify the threshold of invasiveness with respect to this right and adopted the three-pronged test required for encroachment of any Article 21 right – legality-i.e. through an existing law; necessity, in terms of a legitimate state objective and proportionality, that ensures a rational nexus between the object of the invasion and the means adopted to achieve that object. This clarification was crucial to prevent the dilution of the right in the future on the whims and fancies of the government in power.

In the context of data protection, the Court also looked at the "International Principles on the Application of Human Rights to Communication Surveillance" (hereinafter referred to as the "Necessary and Proportionate Principles"), which were launched at the U.N. Human Rights Council in Geneva in September 2013,

The judgement also references Daniel Solove's problem of aggregation and states that "where data gathered through the ordinary citizen's veillance practices finds its way to state surveillance mechanisms, through the corporations that hold that data" is a cumulative violation of the Right to Privacy.

Punitive provisions under foreign trade act 1992

There are punitive penal provisions in the Foreign Trade (Development and Regulation) Act, 1992 and its 2010 amendment which imposes civil and criminal prosecution for violation of export laws with fines for civil violations ranging from Rs. 3 lakhs to Rs. 20 Lakhs.

Proposed Data Protection Framework

In 2018 the SriKrishna Committee released the draft Personal Data Protection Bill of 2018 (PDP Bill). Importantly, if the Bill is enacted in its' current form, individuals will have an avenue to seek redress for violations related to surveillance. The Bill recognises any restriction on actions due to the fear or surveillance and surveillance that is not reasonably expected as two harms for which individuals can seek judicial remedy for. The Bill also requires that the processing of personal data in the interests of the security of the State must be authorised by law and necessary and proportionate for the interests sought to be achieved.

Further, The PDP Bill also requires the data fiduciary[16] to undertake an impact assessment before undertaking any processing involving new technologies or large scale profiling or use of sensitive personal data.[17] Following the impact assessment if the Authority under the legislation has a reason to believe that such processing is likely to cause harm then the authority might direct the data fiduciary to cease such processing or direct that such processing be subject to certain conditions.

[16] The proposed Personal Data Protection Bill defines a Data fiduciary" as any person, including the State, a company, any juristic entity or any individual who alone or in conjunction with others determines the purpose and means of processing of personal data;
[17] Section 33 of the proposed Personal Data Protection Bill

3 .Whether the laws, regulations, or policies identified are consistent with State obligations under Article 19 of the International Covenant on Civil and Political Rights, Article 19 of the Universal Declaration of Human Rights, and other relevant human rights standards.

The two key provisions in international human rights law which any surveillance measure needs to comply with are Articles 17 (Right to Privacy) and 19 (Right to Freedom of Speech and Expression)

Article 19

Data collection and mass surveillance regimes that are excessively intrusive combined with a lack of adequate remedies can have a potential negative impact on the freedom of speech and expression as it can dissuade people from speaking freely as it may cause individuals to feel like their private lives and conversations are subjects of constant surveillance. [18]Therefore, any surveillance measure needs to be in line with the requirements of Article 19.

Article 19 articulates the freedom of speech and expression.The restrictions clearly demarcate situations when free speech may be legitimately restricted

(a) Provided by a law that is clear, predictable and certain

(b) Grounds for restriction are specific:

1. Respect of the rights of others,
2. Protection of national security,
3. National Security and public order
4. Necessary for a democratic society and is proportionate

[18] European Court of Justice. (2016). *Tele2 Sverige AB v Post-och telestyrelsen; Secretary of State for the Home Department v Watson and others* (C-203/15 and C-698/15), EU:C:2016:970, 99-100

Article 17

Article 17 of the ICCPR protects the Right to Privacy against interferences that are 'unlawful' and 'arbitrary'. In General Comment No. 31, the UNHRC has specified that it can take place only on the basis of a law that is well-defined and specifies the precise circumstances under which surveillance may be permitted. [19]The notion of arbitrary interference essentially refers to the principle of proportionality and states that any intrusion must be proportionate to the end sought. [20] The UN High Commissioner's Report stated that the law enabling a surveillance measure must be:

(a) Accessible to the public;

(b) Pursues legitimate aims,

(c) Precise enough in terms of detailing the limits of this interference and

(d) Provides for effective remedies against abuse of that right. Any policy that impinges on the Right to Privacy must never be applied in a manner that impairs the 'essence of that right.' [21]

PROVISION	**CONSISTENCY WITH ART 19 ICCPR**	**CONSISTENCY WITH ART 17 ICCPR**
Sec 69 IT Act and Associated rules	Complies with substantive and the parameters for restrictions delineated in 19 (3)requirements of reasonable restrictions but does not contain any remedies for violation	Does not contain substantive or procedural frameworks delineating limits of permissible interference by the state
Telegraph Act section 5 and 419A rules	The criteria listed in 19(3) is "public order or public interest" whereas the criteria included here is 'public safety' which seems to be over-reaching	While a clear procedure has been delineated in the Rules, remedies available either against the state or private actor are unclear
Section 91,92 CrPc	Excessive and outdated provision that gives carte	In the absence of any checks and balances or remedies,

[19] Human Rights Comm.,' General Comment no. 31, Nature of the General Legal Obligation on State Parties to the Covenant,' para 6, U.N. Doc. CCPR/C/21/Rev.1/Add.13 (May 26, 2004)
[20] Sarah Joseph, Jenny Schultz & Melissa Castan,*The International Covenant on Civil and Political Rights* 476-77 (3rd ed,2013).533.
[21] High Commissioner for Human Rights, 'Rep. on the Right to Privacy in the Digital Age', para 28, U.N. Doc. A/HRC/27/37 (June 30, 2014)

	blanche' powers to the police, including access to private sector held data without considering any of the reasonable restrictions, thereby acting as a clear mode of stifling dissent	this does not comply with the requirements of Article 17
UASL Telecom Licenses	Requirements placed on service providers are not clear or predictable and require service providers to monitor, trace, and aggregate data and users without consent, thereby stifling free speech	Aims of the UASL Telecom Licenses and the CMS monitoring system are not clearly defined and no remedies against abuse of the right

B. Information concerning the use of such surveillance technologies:

1. Details of emblematic cases of State use of private surveillance technology against individuals or civil society organizations.

As outlined in previous questions, the Government is legally capable of surveilling its citizens in the form of interception, monitoring, decryption, retention and collection of traffic data. Though the Indian government has developed a number of surveillance projects in-house and in collaboration with the private sector, it is not clear that the state has targeted individuals or civil society through the unauthorised use of private surveillance technology. At the sametime, the presence of surveillance technologies that have been used by other governments to target individuals and civil society have been documented in India. In 2011, a company knows as Blue Coat came under the scanner for supplying governments around the world with equipment that were being used as a part of surveillance infrastructure.[22] Specifically, these were devices that categorized web pages to permit filtering of unwanted content; and one that could establish visibility of over 600 web applications and control undesirable traffic. The technology was first identified in Syria which was known to proactively contain dissent and clamp down on opposition. However, as many as 50 of their specific devices were incorporated within public or government networks, including in India and surrounding countries such as Singapore and Thailand. It has been reported that in a number of these countries, these technologies aided government ability to censor content even beyond what the legislation permitted.[23] As per research published by Citizen Lav, FinSpy servers were recently found in India, which means that Indian law

[22] Morgan Marquis-Boire, Jakub Dalek, Sarah McKune, Matthew Carrieri, Masashi Crete-Nishihata, Ron Deibert, Saad Omar Khan, Helmi Noman, John Scott-Railton and Greg Wiseman, "Planet Blue Coat", Citizen Lab, Januar 2013, https://citizenlab.ca/2013/01/planet-blue-coat-mapping-global-censorship-and-surveillance-tools/
[23] Ibid

enforcement agencies may have purchased this spyware from Gamma Group and could potentially be using it to conduct surveillance s in India.[24]

2. Company policies to ensure that the development and sale of surveillance technologies meets human rights standards, particularly those articulated in the UN Guiding Principles on Business and Human Rights.

From research undertaken by the Centre for Internet and Society, it does not appear that companies selling surveillance technologies in India have in place policies and practices that are purposefully inline with the Guiding Principles on Business and Human Rights. In 2013, CIS conducted research on surveillance technology companies based in India. A randomised sample of 100 companies working in the security sector was selected, out of which 76 companies were found to sell surveillance technologies.[25] The research was narrowed by randomly selecting 50 companies for further analysis.[26] Out of 50 enterprises' sample only 19 companies had their privacy policies published on their websites.[27] Even though the privacy policies were not further investigated, and the research is limited in scope, the trend of enterprises not publishing privacy policies could be observed and highlights the need for further investigation into how policy and practice of such companies align with the UN Guiding Principles.

Further, it does not appear that Indian companies have adopted practices similar to those that are being adopted by foreign global tech companies. For example, Google and Microsoft publicly announce their commitments to respect human rights,[28] and publish social responsibility reports.[29] In the case of the development of facial recognition technologies, Google limits access to some of their tools,[30] and Microsoft calls for putting regulation mechanisms in place while outlining their ruling principles in the development process.[31]

Such a requirement is also not included in the evaluation criteria for importing dual use technologies into India. Applications for licenses to export equipment on the SCOMET list are evaluated on a case to case basis, but some aspects that the committee takes into consideration include:

1. Credentials of end-user, credibility of declarations of end-use of the item or technology, integrity of chain of transmission of item from supplier to enduser, and the potential of item or technology, including timing of its export, to contribute to end uses that are not in

---

[24] Morgan Marquis-Boire, Bill Marczak, Claudio Guarnieri & John Scott-Railton, *For Their Eyes Only: The Commercialization of Digital Spying,* Citizen Lab and Canada Centre for Global Security Studies, Munk School of Global Affairs, University of Toronto, 01 May 2013, http://bit.ly/ZVVnrb

[25] Maria Xynou, "The Surveillance Industry in India," *The Centre for Internet and Society*, March 2014, https://cis-india.org/internet-governance/blog/surveillance-industry-india.pdf, 2.

[26] Ibid., 23.

[27] Maria Xynou, "Spreadsheet data on sample of 50 security companies," *The* Centre *for Internet and Society*, 28 February 2014, http://cis-india.org/internet-governance/blog/data-on-surveillance-technology-companies.

[28] "Microsoft Global Human Rights Statement," *Microsoft Corporation*, https://www.microsoft.com/en-us/corporate-responsibility/human-rights-statement.

[29] "Sustainability,"*Google LCC*, https://sustainability.google/reports/.

[30] Kent Walker, "AI for Social Good in Asia Pacific," *Google LCC*, 13 December 2018, https://www.blog.google/around-the-globe/google-asia/ai-social-good-asia-pacific/.

[31] Brad Smith, "Facial recognition: It's time for action,"*Microsoft Corporation*, 6 December 2018, https://blogs.microsoft.com/on-the-issues/2018/12/06/facial-recognition-its-time-for-action/.

conformity with India's national security or foreign policy goals and objectives, objectives of global non-proliferation, or its obligations under treaties to which it is a State party.
2. Assessed risk that exported items will fall into hands of terrorists, terrorist groups, and non-State actors;
3. Export control measures instituted by recipient State;
4. The capabilities and objectives of programmes of recipient State relating to weapons and their delivery;
5. Assessment of end-uses of item(s);
6. Applicability to an export licence application of relevant bilateral or multilateral agreements to which India is a party.

3. 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.

The development of surveillance technologies and solutions is done by both the private companies and government entities such as C-DOT and C-DAC. Private companies specializing in providing data and/or surveillance technologies to the Indian government such as social media monitoring, analysis, crowdsourced data mining tools are accommodating the end-use purposes of facilitating state-led surveillance. Importantly, such companies are not necessarily 'surveillance companies' and the use of the technology is not explicitly 'state surveillance' . In many ways, the use of techniques like monitoring and sentiment analysis are expanding the scope of legalized surveillance and thereby increasing its scope beyond traditional forms, authorization processes, and authorities. The impact on freedom of expression and privacy of these techniques is currently undocumented. As of 2017, CIS has documented the below publicly known instances of private companies' collaboration with the state, which included but are not limited to:

- Pricewaterhouse Cooper aided the Indian government in mining the data obtained from the MyGov.in e-governance project.[32] The data from MyGov.in platform, social media content and blogs is managed with an aim to monitor public discourse.[33] It is currently unclear from publicly available data how collected information is used and stored.
- SocialAppsHQ conducted sentiment analysis, behavioural patterns identification and provided real-time alerts on social media platforms for government's Social Media Lab project, which began in Mumbai and since expanded to other cities.[34]
- FaceTagr, an Indian company created a software that analyzes CCTV footage in real time to check for individuals with criminal history. It is being used by the local police who are alerted when criminals are identified in the area. The company is also collaborating with

[32] Amber Sinha, "Social Media Monitoring," *The Centre for Internet and Society*, 13 January, 2017, http://cis-india.org/internet-governance/files/social-media-monitoring/at_download/file, 1.
[33] Ibid., 3.
[34] Ibid., 2.

the Indian Railways, along with deploying its software at 24 checkpoints of the Indian-Nepal border for the purpose of monitoring human trafficking.[35]

Social media platforms can also cooperate with the Indian government by providing information on their users when law enforcement agencies approach them for disclosure of information during an investigation. Facebook, Google and Twitter produce transparency reports outlining the number of requests being satisfied.[36] Transparency reports of tech companies such as Google and Facebook are the only formal points of reference on Indian surveillance mechanisms apart from journalistic inquiries and granted right to information requests.[37]However, the extent to which social media platforms are familiar with how the government is using their technologies and platforms is unknown.

In the case of facial recognition technology the leaders in this field such as Microsoft and Google have shown that they recognise the potential harms that this technology can cause. Microsoft, for example has published a blog laying down principles that guide their facial recognition work. These principles include Fairness, Accountability, Transparency, Non-discrimination, Notice and consent and Lawful Surveillance.[38] Similarly Google has also announced that Google Cloud would not be offering general-purpose facial recognition APIs before understanding the important working through questions of technology and policy.[39] However such steps have not been taken by Indian companies. On the contrary one of India's largest multinational companies, Tech Mahindra has rolled out their facial recognition software to record employee attendance without open and public discourse around potential implications or risks of the same.[40]

4. Company standards or policies to monitor the use of their technology after it is sold to governments.

Though there are initiatives that focus on company policies and practice and their impact on human rights including freedom of expression and privacy that CIS is aware of, such as the Global Network Initiative - companies in India do not appear to have adopted such practice and do not appear to actively monitor the use of their technology after it is sold to governments.

---

[35] Anand Murali (2018)"The Big Eye: The Tech is Ready for Mass Surveillance in India" <https://factordaily.com/face-recognition-mass-surveillance-in-india/>

[36] Vipul Kharbanda, "Transparency in Surveillance," *The Centre for Internet & Society*, 23 January, 2016, https://cis-india.org/internet-governance/blog/transparency-in-surveillance.

[37] Centre for Internet and Society, "State of Surveillance in India" *Privacy International*, 29 March 2016, https://www.privacyinternational.org/feature/1165/state-surveillance-india.

[38] Rich Sauer, "Six principles to guide Microsoft's facial recognition work" Microsoft Blog, 17, December, 2018,https://blogs.microsoft.com/on-the-issues/2018/12/17/six-principles-to-guide-microsofts-facial-recognition-work/

[39]Kent Walker, "AI for Social Good in Asia Pacific," Google in Asia, 13 December, 2018, https://www.blog.google/around-the-globe/google-asia/ai-social-good-asia-pacific/

[40] Supriya R, "Tech Mahindra's Moodometer Gauges Employees' Mood to Uplift Work Environment," Data Quest, 10 August, 2018
https://www.dqindia.com/tech-mahindras-moodometer-gauges-employees-mood-uplift-work-environment/