Response to the Pegasus Questionnaire issued by the SC Technical Committee

April 12, 2022

By- Anamika Kundu, Digvijay, Arindrajit Basu, Shweta Mohandas and Pallavi Bedi

The Centre for Internet and Society, India

https://cis-india.org

Template designed by Saumyaa Naidu

Background

On March 25, 2022, the Supreme Court appointed Technical Committee constituted to examine the allegations of alleged unauthorised surveillance using the Pegasus software released a questionnaire seeking responses and comments from the general public. The questionnaire had 11 questions and the responses had to be submitted through an online form- which was available at https://pegasus-india-investigation.in/invitation-to-comment/. The last date for submitting the response was March 31, 2022.

CIS had submitted the following responses to the questions in the questionnaire.

Response to the Questionnaire

1. **Whether the existing boundaries of State surveillance of personal and private communications of citizens, for the purpose of national security, defence of India, maintenance of public order, and prevention and investigation of offences, are well defined and understood? Are there any other purposes for which State surveillance may be justifiable and necessary?**

The existing boundaries of state surveillance are not well defined and understood. The government can carry out surveillance as per Section 5(2) of the Indian Telegraph Act (**Telegraph Act**), 1885 and Section 69 of the Information Technology Act (**IT Act**).[1] Rule 419- A of the Telegraph Rules, 1951 and the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 ("**IT Rules**") provide for a process and procedure for the Telegraph Act and IT Act respectively.[2] Interception of messages as per the Telegraph Act is only allowed in situations of public emergency or public safety. Under Section 69 of the IT Act, the executive can issue guidelines or directions similar to that of the Telegraph Act.

These words have not been defined either under the Telegraph Act or the IT Act. They were interpreted in the Supreme Court's 1996 decision of *PUCL v. Union of India* as "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".[3] Having satisfied the above prerequisite, the purposes for interception enumerated under section 5(2) of the

[1] The Indian Telegraph Act, 1885; The Information Technology Act, 2000.
[2] The Telegraph Rules, 1951; The Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.
[3] PUCL v Union of India, AIR 1997 SC 568.

Telegraph Act are: Sovereignty/integrity of India, Security of the State, Friendly relations with Foreign States, Public Order, and Prevention of incitement to the commission of any offence. The substantive part of the IT Act includes sections 69 and 69B, and in some cases, sections 28 and section 29 of the IT Act.

Rule 419-A of the Telegraph Rules states that: only a home secretary from the central or state government can authorise 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. 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 of an interception maintained by the service provider will be destroyed every two months. A similar provision exists in the IT Rules- provision 24(1) prohibits any person from intentionally intercepting communications without authorisation. The remedy is further hindered in India's present surveillance framework as under Rule 25 of IT Rules- service providers are prohibited from disclosing information about governmental requests and orders.

Two main differences arise in the language of section 69 of the IT Act and section 5(2) of the Telegraph Act. While section 5(2) offered two prerequisites for its invocation, section 69 does away with those, and additionally, it adds two more grounds in the interest of which interception is lawful: defence of India, and investigation of any offence. As such, no safeguards have been provided for individuals being surveilled. 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.[4] Even the Standing Operating Procedure issued by the Ministry of Home Affairs on May 19, 2011, does not specify the grounds under which State interception can be carried out.[5] Moreover, there are concerns with respect to the broadly and vaguely defined powers regarding interception.

In India, the right to privacy has been almost exclusively a judicial construct. In *KS Puttaswamy v Union of India*, it was held that privacy is a constitutionally protected right.[6] The court also articulated the threshold of invasiveness concerning this right and adopted the three-pronged test required for

[4] Report of the Group of Experts on Privacy, page 46, available at https://cis-india.org/internet-governance/blog/report-of-group-of-experts-on-privacy.pdf (Last visited on April 8, 2022).
[5] Internet Freedom Foundation, Breaking: New insight into the Secret Operating Procedures of State Governments for Surveillance, September 25, 2019, available at https://internetfreedom.in/rti-on-state-surveillance/ (Last visited on April 8, 2022).
[6] Justice K.S. Puttaswamy (Retd.) & Anr. v Union of India & Ors., (2017) 10 SCC 1.

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.

The present laws are inadequate in terms of providing pre or post judicial review of interception decisions; there is also no mechanism of informing the citizen surveilled; there is no standardisation of orders; no details about which agencies are authorised to carry out interception, and there are no permissible limits set out regarding the grounds of surveillance. In *Shreya Singhal v. Union of India*, it was held that grounds ought to be 'narrowly interpreted' due to the impact on fundamental rights.[7] However, without any judicial oversight, there is no accountability in surveillance measures as to what is the 'security of the State'. State surveillance can only be permitted as per the grounds in Article 19(2) of the Indian Constitution. Any restriction should be allowed as per the proportionality requirements set out by the Supreme Court[8]

2. **Whether the procedures specified prescribed under the Telegraph Act, 1885 and Information Technology Act, 2000 and rules made thereunder for digital/telecommunication surveillance (with executive oversight measures for interception/decryption orders) are sufficient to effectively prevent (i) unwarranted excessive/routine use; or (ii) misuse; (iii) abuse of State surveillance, purportedly undertaken for the aforesaid purpose**

The existing procedures under the Telegraph Act and IT Act are not sufficient. There are no reasonable procedures that effectively prevent unwarranted/excessive use; misuse; or abuse of State surveillance even when carried out under the grounds mentioned in them. Surveillance programmes such as the National Intelligence Grid (NATGRID), the Centralised Monitoring System (CMS), Crime and Criminal Tracking Network System (CCTNS) and the proposed National Automated Facial Recognition System (AFRS) function without the presence of any law and are not covered by the Telegraph Act and IT Act.

Both the Telegraph Act and IT Act have a surveillance framework that constitutes a Review Committee. These Committees can direct the destruction of intercepted messages if not done in line with the law. The problem is that these committees only have executive members without any judicial review of the directions. Without the presence of judicial review of surveillance measures, such provisions could be held unconstitutional. The need for judicial oversight was recognised by the Supreme Court in the *Aadhaar case* when it struck down section 33(2) which vested the power to authorise the disclosure of biometric/demographic

[7] Shreya Singhal v Union of India, AIR 2015 SC 1523.
[8] Justice K.S. Puttaswamy (Retd.) & Anr. v Union of India & Ors., (2017) 10 SCC 1.

information in the interest of national security.[9] The Supreme Court stated that such disclosure required an "application of judicial mind."[10]

The concern with regards to the current laws regulating surveillance also has to do with the necessity of exclusive executive review and exclusive executive control over surveillance in India. This is where the current laws fail the proportionality test .[11] The proportionality test requires a legitimate state aim, rational nexus, necessity, and balancing. *Puttaswamy* recognised that national security and crime control are legitimate state objectives.[12] The second limb of the proportionality test delves into whether there is a rational nexus between state action and the state aim under law. Considering that the government could justify a rational nexus between state aim and the action employed, it is the necessity part of the proportionality test where the state surveillance measures fail. Necessity requires us to draw a list of alternatives and their impact on an individual, and then do a balancing analysis with regard to the alternatives. Here, judicial scrutiny of the surveillance orders either before surveillance is carried out or after surveillance has been carried out, are viable alternatives that respect individual rights while not interfering with the state's aim.

In the case of *Vinit Kumar v. Central Bureau of Investigation (CBI)*, the Bombay High Court had held that the interception orders by CBI were not backed by law and thus needed to be destroyed.[13] If there had been an effective review system, such harm would not have been caused to the petitioner. The Srikrishna Committee had also highlighted that there exists a lack of effective oversight in making decisions.[14] With surveillance functioning behind the eyes of the law and public, there is a curtailment of Articles 32 and 226 of the Indian Constitution as even if one suspects surveillance there is no method of seeking redressal.

3. If your response to Query 2 is in the negative:

(a) What substantive and procedural safeguards-involving administrative, judicial and/or independent authorities would you suggest to adequately balance individual rights with national security and public order interests?

---

[9] Justice K.S. Puttaswamy and Anr. vs. Union of India and Ors., (2019) 1 SCC 1.

[10] Ibid.

[11] Vrinda Bhandari and Karan Lahiri, The Surveillance State: Privacy and Criminal Investigation in India: Possible Futures in a Post-Puttaswamy World, 3(2) University of Oxford Human Rights Hub Journal 15 (2020).

[12] Justice K.S. Puttaswamy (Retd.) & Anr. v Union of India & Ors., (2017) 10 SCC 1.

[13] Vinit Kumar v Central Bureau of Investigation [2019] SCC OnLine Bom 3155.

[14] Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians, page 121, available at https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf (Last visited on April 11, 2022).

(b) In what manner can the existing procedures prescribed by law enabling (i)intelligence agencies, and (ii) law enforcement, for targeted surveillance, be further strengthened, improved on and meaningful?

In terms of safeguards, judicial oversight of surveillance orders is a necessary feature considering the exclusive executive control over surveillance mechanisms and systems. As noted above, the lack of judicial oversight in surveillance orders fails the proportionality test. The relevant safeguard would be to introduce judicial oversight either before surveillance is carried out or after surveillance has happened. Further, any communication surveillance undertaken or authorised by the Indian state must comply with the International Principles on the Application of Human Rights to Communications Surveillance (relevant parts of which are - Legality, Legitimate State Aim, Necessity, Adequacy, Proportionality, Competent Judicial Authority, Due Process, and User Notification, Transparency, Illegitimate Co-operation, and Safeguards against illegitimate access.[15] As mentioned above, the existing practices of state surveillance are not in conformity with the decision of the Supreme Court in *Puttaswamy v. Union of India.*[16] Not only is there a need to establish a rule of law but also encourage the enactment of a privacy law from a rights-based approach.

Looking at other jurisdictions, in the United Kingdom, the Investigatory Powers Act, 2016 requires all orders of surveillance to be reviewed by the Investigatory Powers Commissioner.[17] Even the Personal Data and Information Privacy Bill, 2019 introduced by Dr. Ravikumar contains provisions to create a Surveillance and Interception Review division.[18] These divisions were to be created in each High Court and have judges who would review surveillance orders. Along with judicial checks, there needs to be a check over the expenditure and deployment of surveillance mechanisms. Disclosures should be made to the Parliamentary Committee on Home affairs regarding resources, similar to what takes place during the Budget Session of the Parliament.[19]

4. What should a grievance redressal mechanism be for a person whose data is subjected to targeted surveillance by the State?

---

[15] Necessary and Proportionate, International Principles on the Application of Human Rights to Communication Surveillance, available at https://necessaryandproportionate.org/files/en_principles_2014.pdf (Last visited on April 11, 2022).

[16] Justice K.S. Puttaswamy (Retd.) & Anr. v Union of India & Ors., (2017) 10 SCC 1

[17] Investigatory Powers Act, 2016 (United Kingdom).

[18] Personal Data and Information Privacy Bill, 2019, introduced in Parliament on July 26, 2019, available at https://drive.google.com/file/d/1DReq96e-FLsSoKUvK94_-VCtu2Y1PE97/view (Last visited on April 11, 2022).

[19] For example, Ministry of Defence, *Capital Outlay of on Defence Services: Demand No. 1*, February 1, 2022, available at https://www.indiabudget.gov.in/doc/eb/sbe21.pdf (Last visited on April 11, 2022).

Where no crime or threat to national security is established from the data collection exercise?; Where involvement in a crime or a threat to national security is established from the data collection exercise? What should be the fora/forum for grievance redressal in regard to any surveillance by the State or its instrumentalities?

The User Notification section of the Proportionate and Necessity Principles of the '***International Principles on the Application of Human Rights Law to Communications Surveillance*** '[20]are relevant here. Reproducing the relevant sections below:

User Notification: Those whose communications are being surveilled should be notified of a decision authorising Communications Surveillance with enough time and information to enable them to challenge the decision or seek other remedies and should have access to the materials presented in support of the application for authorisation. Delay in notification is only justified in the following circumstance:

i. Notification would seriously jeopardise the purpose for which the Communications Surveillance is authorised, or there is an imminent risk of danger to human life; and

ii. Authorisation to delay notification is granted by a Competent Judicial Authority; and

iii. The User affected is notified as soon as the risk is lifted as determined by a Competent Judicial Authority. The obligation to give notice rests with the State, but communications service providers should be free to notify individuals of the Communications Surveillance, voluntarily or upon request.

Law enforcement agencies should not be exempt from implementing minimum safeguards to ensure that personal data in their possession is stored safely and securely. This exemption much like the others is only a limited exemption. Law enforcement and intelligence agencies would be exempt from the requirements of Consent, Purpose Specification, Use Limitation, but would still be subject to the requirements of Transparency, Accountability Data Security, Data Quality. The rights applicable to the individuals under the data protection law such as access,

20

https://www.ohchr.org/sites/default/files/Documents/Issues/Privacy/ElectronicFrontierFoundation.pdf

rectification are also not invalid but merely suspended while the surveillance or processing activity is pending. It may also be considered that in line with its powers, the Privacy Commissioner or similar quasi judicial authority under the data protection authority, created under the Personal Data Protection Bill as well as data controllers should be able to review judicial orders that allow for surveillance and determine whether the orders meet the test for proportionality. This would allow for an additional layer of checks and balances, and allow for the data protection authority to prevent the misappropriation of personal data. Similarly, once notice has been issued to an individual post surveillance, the individual should be able to move a relevant authority for relief if the individual feels that their right to privacy was violated in a manner that is not consistent with the relevant law.

Currently, India does not have any grievance redressal mechanism to address the concerns of a person whose data has been subjected to targeted surveillance. There is no judicial or quasi judiciary regulating or overseeing the surveillance machinery or mechanism. The proposed Personal Data Protection Bill, 2019 has envisaged the creation and establishment of a Data Protection Authority (**DPA**)- and it has the power to conduct an inquiry on its own, or on a complaint received by it. However, as we are aware, unfortunately, the Bill also grants extensive powers to the government to exempt any government agency from the purview of the Bill- and this includes excluding the agency from the purview of the DPA. By virtue of the exemption granted under the bill, the government can exempt the surveillance and law enforcement agencies from the jurisdiction of the DPA. In addition, the government can also exempt such agencies from all the transparency and accountability requirements specified in the Bill. Therefore, the affected person may never be notified about the processing of their personal data by law enforcement agencies and/or surveillance agencies, and therefore will not be able to file a complaint before the DPA.

The power given to the central government to exempt any government agency needs to be drastically circumscribed and it should not extend to curtailing the power of the DPA. The DPA should have a separate wing within it which can inquire about and investigate into complaints of surveillance. Since surveillance is covert, therefore a person whose rights have been violated through illegal surveillance may (a) never become aware of the violation or (b) may be aware, but may not have any evidence to prove the allegation. The law should clearly specify that any person who believes that they have been subject to surveillance can file a complaint before the DPA's surveillance regulatory body. They do not have evidence to prove her claim before filing the complaint- it should be the responsibility of the authority to inquire and investigate into the complaint and public authorities should be under a legal duty to provide the tribunal with all required documents. In this regard, it would be pertinent to refer to the Investigatory Powers Tribunal (**Tribunal**) established under the Investigatory Powers Act, 2016 in the United Kingdom. Under the act, the Tribunal is bound to

investigate and to determine valid complaints and public authorities are under a duty to provide the Tribunal with all documents and information the Tribunal may require to assist in that investigation. Nothing can be held back from the Tribunal for reasons of secrecy or national security.[21]

5. Should there be special safeguards for the state surveillance of certain categories of persons? If so, what categories of persons should these cover and what form should these take?

The right to privacy as enumerated by the Supreme Court in *Puttaswamy 1*[22] is a fundamental right of every Indian citizen. The court did not create any special categories of persons from whom any additional or special safeguards need to be established. We do not believe that there should be any distinction between Indian citizens in the privacy protection afforded them. Further, there should be a bar on surveillance of minors below the age of 18 years. At the same time, it is also important to note the adverse impact of surveillance and the lack of any grievance redressal mechanism on the marginalised sections of society- who have historically been discriminated against on the basis of gender, caste and sexuality. Additionally, we would like to state that once an individual is no longer a person of interest, processes should be in place to stop the ongoing surveillance and measures should be taken to record the cessation of surveillance.

6. In what context and to what extent should sovereign/state immunity and State access be extended to acts of hacking of computer system, mobile devices, online accounts, telecommunication/digital networks, unauthorised access, technology backdoors, decryption of private records, and to legal mandates to share information under intermediary or data processor's obligations under intermediary rules and data protection laws, respectively?

The State derives its power and authorisation to conduct surveillance from Section 69 of the IT Act read with the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information Rules), 2009 (I**nterception Rules**). The Interception Rules lay down the procedure to be followed by the government agencies to undertake electronic surveillance. It is pertinent to note that the IT Act — under Section 43 read with Section 66 — penalises any unauthorised access to computer systems, and the government has not been granted any exception. Section 43 of the IT Act prohibits, without the permission of the owner, accessing or securing access to a computer, computer system or computer network or a computer resource; or downloading, copying or extracting any data, or information from such computer system. It also prohibits

[21] https://www.ipt-uk.com/
[22] (2017) 10 SCC1

the introduction of any 'computer contaminant' or 'computer virus' into any computer system; or damaging or causing damage to any computer system. The penalty is prescribed under Section 66- which could either be (a) imprisonment for a maximum period of 3 years; (b) a fine which could extend to a maximum of 5 Lakh; or (c)both.

The State cannot/should not be able to claim sovereign immunity for illegal acts done by such as hacking of computer systems, mobile devices, online accounts, telecommunication networks or unauthorised access to computer systems and personal records. This lack of sovereign immunity also extends to agencies/private entities working on behalf of the State- such agencies/entities can also not claim immunity for an illegal act under the garb of sovereign/state immunity.

State hacking operations are based on known backdoors in commonly used software products. However, there is no such thing as a secure backdoor – stockpiling software vulnerabilities for use in government hacking operations leaves *all* digital infrastructure vulnerable to abuse and is not sustainable in the long run. An example of this is the WannaCry ransomware attack[23], which was based on an exploit stolen from the US National Security Agency (NSA). It led to a massive global cyberattack affecting around 2,00,000 computers across 150 countries. Another example is the breach of Juniper Networks Inc. and its many government and corporate customers[24]. This was attributed to hackers linked to the Chinese government, who found and exploited a backdoor planted by the NSA in a cryptographic standard. The State should disclose software vulnerabilities to software vendors in order to protect itself and its citizens from hostile powers and criminal entities, and not exploit them for short-term surveillance objectives.

7. Should the State be obliged to record or disclose surveillance technology/access that is procured by it, available with it or used by it for the purpose of national security, or defence of India? To whom should such disclosures be made and in what form? Should these records be accessible under Right to Information or otherwise made public once a certain amount of time has elapsed?

Yes, the State (at the Central and state level) should be under an obligation to record and disclose the surveillance technology that is procured by or used by it for the purposes of national security, or defence of India. We suggest that all records of purchase/consignment of the surveillance mechanism must be maintained in a digital form. This includes the terms of service of the provider, the contract, the amount paid, the responsible person within the company and

[23] https://en.wikipedia.org/wiki/WannaCry_ransomware_attack

[24] https://www.bloomberg.com/news/features/2021-09-02/juniper-mystery-attacks-traced-to-pentagon-role-and-chinese-hackers

the government ect. Once a contract is over there should be proper record of the same as well data that was handed over to the government.The laws regulating the surveillance architecture in the country should mandate the State to proactively/periodically disclose the details of the surveillance technology which it has procured or to which it has access.

While making the disclosures, it should disclose (a) whether any data impact assessment study was conducted prior to accessing/procuring the surveillance technology, and if yes, then the result of the study should also be disclosed; (b) the number of people of were/are under surveillance; and the reason thereof; and © how long will the data be retained; and (d) the personnel who have/will have access to the technology.

The disclosures should be made to the Rajya Sabha Standing Committee on Home Affairs- the ambit of the standing committee includes looking into police training and modernisation, prison conditions, national security and intelligence coordination. It is worthwhile to note that in 2020, New York passed the Public Oversight of Surveillance Technology (POST) Act. The act mandates the New York Police Department (NYPD) to **publicly** disclose the technology tools it currently possesses – and going forward, technology that it plans to acquire – along with the policies that govern their use. NYPD released its surveillance technology information to the public in January 2021 and the public was invited to give comments.

It is important to determine what could/would constitute a reasonable length of time. However, we believe that the records should be accessible under the Right to Information Act after a certain time has elapsed.

8. Would your suggestions be practical and feasible to implement under the Indian federal constitution framework, with States having control over state law enforcement agencies?

Yes, our suggestions regarding regulating the surveillance mechanism in the country are practical and feasible and can be implemented under the Constitutional framework.Our recommendations are in line with the three tier test laid down by the Supreme Court to satisfy any encroachment into the right to privacy.

We recommend amending the Information Technology Act and its affiliated rules as well as the Telegraph Act and its rules. We also recommend either a complete abrogation of Section 35 of the proposed Data Protection Bill or a significant dilution of it so that it is in conformity with the principles enumerated by the Supreme Court in the right to privacy judgement. State governments will also need to accordingly amend the laws in their states which permit surveillance.

9. What steps can be taken to improve and increase the cyber security of the Nation and its assets? Is there a need for a separate authority or organisation to (i) investigate cyber security vulnerabilities for threat assessment relating to cyber-attacks; and (ii) to ensure cybersecurity of public and private digital infrastructure?

An institutional overhaul is not needed and at present the cybersecurity institutional architecture is sufficient to work towards safeguarding both public and private digital infrastructure. Over the past two decades, India has made a notable effort towards creating institutional machinery focussing on cyber resilience.[25] The Prime Minister's Office has several portfolios within it. This includes the National Security Council,usually chaired by the National Security Adviser (NSA) and plays an important role in implementing India's cybersecurity ecosystem.The National Critical Information Infrastructure Protection Centre (NCIIPC) under the National Technical Research Organisation was set up to facilitate the protection of critical information infrastructure and in 2015, the Prime Minister established the office of the National Cyber Security Co-ordinator who advises the Prime Minister on key cybersecurity issues and also leads some of India's diplomatic engagement on cybersecurity.India's Computer Emergency Response Team (CERT-IN) which deals with threats to non-critical infrastructure deals falls within the Ministry of Electronics and Information Technology. The Ministry of Defence has set up the Defence Cyber Agency, a tri-service command of the Indian armed forces and the Ministry of Home Affairs has several organisations within its remit to further law enforcement efforts.

This institutional architecture is robust and India does not need a seperate authority or organisation. Instead, efforts must be made to foster coordination both within government institutions and with key external stakeholders,such as security researchers.

Software security audits from independent security researchers can help improve the cybersecurity of government services and assets. We suggest reform around the operation of the Indian Computer Emergency Response Team (**CERT-IN)** and how it handles responsible disclosures from ethical hackers:

(1) Safe harbour provisions for ethical hackers

Ethical hackers, i.e. security researchers who independently audit government IT infrastructure for vulnerabilities and responsibly disclose them so that they can be fixed, are playing an increasingly important role in the cybersecurity strategies. Many private and public entities run programs for ethical hackers to

[25] See Arindrajit Basu and Pranesh Prakash "Patching the gaps in India's cybersecurity,"*The Hindu*,March 06,2021,https://www.thehindu.com/opinion/lead/patching-the-gaps-in-indias-cybersecurity/article34000336.ece

connect with them and some even offer monetary rewards[26,27]. While CERT-IN provides a point of contact for responsible disclosure of vulnerabilities, its policies do not allow for protecting ethical hackers from legal liability for unauthorised access to computer systems[28] — an activity which is a natural byproduct of their work. This discourages people acting in good faith from examining government systems. Such policies must be amended to grant reasonable immunity to ethical hackers to enter systems in the context of discovering and demonstrating vulnerabilities as per industry standards[29,30]. Access monitoring tools should ideally already be in place to ensure that ethical hackers are complying with the boundaries set in place for them.

(2) Timely fixes and acknowledging issues

Researchers who have reported security issues to CERT-IN have said that issues are not acknowledged (publicly or privately) and not addressed in a timely manner[31], which is concerning given the criticality of the security issues in question. Appropriate changes to the functioning of CERT-IN should be made to ensure that reported issues are acknowledged and fixed in a timely manner that is in line with industry standards[32].

(3) Incentivising ethical hackers

While providing monetary compensation for responsibly disclosing security issues may or may not be feasible for the government, there are other incentives that can be set up to incentivise ethical hackers. Allowing public disclosure of issues once they have been completely resolved or simply making a public acknowledgment of their contribution without mentioning sensitive details enables ethical hackers to claim credit for their work and encourages them to do more.

10. What laws and safeguards should be put in place by the State to protect its citizens from targeted surveillance by non-State/private entities and foreign agencies?

---

[26] https://hackerone.com/directory/programs
[27] https://hackerone.com/deptofdefense
[28] https://internetfreedom.in/dont-penalise-cybersecurity-researchers/
[29]https://portswigger.net/daily-swig/safe-harbor-needs-to-be-built-to-provide-haven-for-ethical-hackers
[30]https://www.hackerone.com/vulnerability-disclosure/whats-vulnerability-disclosure-program-do-ou-need-one
[31]https://www.huffpost.com/archive/in/entry/election-commission-website-leaked-phone-number-email-address_in_5df9b653e4b0d6c84b7588c8
[32] https://googleprojectzero.blogspot.com/p/vulnerability-disclosure-faq.html

Non-State actors

For private sector actors processing data belonging to individuals,urgently implementing a data protection law is the best way of protecting Indian citizens. The current draft of the Data Protection Bill defines harm to include "any observation or surveillance that is not reasonably expected by the data principal, and psychological manipulation which impairs the autonomy of the individual";these provisions could be used by a data principal when they become aware that they are being surveilled by private entities. Clause 29(7) of the Bill also states that the Data Protection Authority may direct a data fiduciary to conduct an audit in case the data fiduciary is processing data in such a manner that is likely to cause harm to a data principal. The data principal under Clause 32 can make a complaint to the data protection officer in event that the processing of a data principal has or is likely to cause harm.

In terms of foreign non-state actors there are a range of actors including Advanced Persistent Threat Groups,private software and technology companies that either work in collusion with government agencies to help them access data or manufacture surveillance technologies sold to client governments,and several erstwhile private military and security companies that are developing in-house capabilities enabling large scale surveillance. To protect citizens from such activities, India must have clear,transparent and accountable procurement practices to ensure that adversarial foreign actors do not end up undertaking critical functions that may undermine human rights.

There is also a concern of state backed extraterritorial surveillance by intelligence agencies. To protect from this, a two step approach is needed:

1. Ensure that India's surveillance architecture (both legal and technical) is constitutionally sound and in line with international human rights standards

2. In line with the approach taken by the EU, approve cross border flows only to countries that have equivalent and adequate surveillance standards for any citizens data that might flow there.

11. Do you have any other suggestions or comments relating to the Terms of Reference?

Surveillance reform in line with India's constitutional standards and international human rights law is imperative from a geopolitical and global economic standpoint. From an economic standpoint, Cross border-flows with the European Union, the world's single-largest common market remains a priority for several key stakeholders in India's digital economy. Recent decisions coming from the European Union, including the Schrems II decision of the European Court of

Justice that invalidated an agreement enabling data flows to the US ,indicate that safeguards against state surveillance are a priority for the EU. [33]From a security standpoint, Indian law enforcement agencies face a cumbersome process (through Mutual Legal Assistance Treaties or MLATs) to access data stored in foreign jurisdictions such as the United States that is required for conducting legitimate criminal investigations.[34]A solution to this problem lies in signing an executive data sharing agreement with the United States and other jurisdictions along the lines of the CLOUD Act. To boost the confidence of partners in the privacy and security of data in India, a transparent and accountable surveillance regime with judicial oversight is critical.[35]

Finally, from a political and normative standpoint, much of the consternation against Chinese products and China's technological advances have been driven by a narrative around a lack of security safeguards. India has often used its democratic credentials and in foreign policy posturing such as the restriction of Chinese applications in India, which were justified on the grounds of sovereignty as well as data security and privacy.[36] To maximise the foreign policy dividends of its democratic credentials, a reformed surveillance architecture is the need of the hour.

[33] Arindrajit Basu, " Unpacking US Law and Practice on Extraterritorial mass surveillance in light of Schrems II," Medianama,Aug 24 2020,https://www.medianama.com/2020/08/223-american-law-on-mass-surveillance-post-schrems-ii/

[34] Amber Sinha et al, Cross Border data-sharing and India: A study in processes,content and capacity, The Centre for Internet&Society,27 September 2018,https://cis-india.org/internet-governance/files/mlat-report/view

[35]Smriti Parsheera and Prateek Jha," Cross border data access for law enforcement: What are India's strategic options," Carnegie India, November 23,2020,https://carnegieindia.org/2020/11/23/cross-border-data-access-for-law-enforcement-what-are-india-s-strategic-options-pub-83197

[36] See https://pib.gov.in/PressReleseDetailm.aspx?PRID=1635206