Response Submission on
TRAI's Consultation Paper on Privacy, Security and Ownership of the Data in the Telecom Sector

Amber Sinha, Elonnai Hickok and Udbhav Tiwari[1]

Centre for Internet and Society, India

November 06, 2017

Table of Contents

1. Preliminary **2**

2. About CIS **3**

3. General Comments **3**

Data as Property 4

Data Monopoly 5

Privacy Principles 5

4. Specific Comments **6**

4.1 Are the data protection requirements currently applicable to all the players in the ecosystem in India sufficient to protect the interests of telecom subscribers? What are the additional measures, if any, that need to be considered in this regard? 6

4.2 In light of recent advances in technology, what changes, if any, are recommended to the definition of personal data? Should the User's consent be taken before sharing his/her personal data for commercial purposes? What are the measures that should be

[1] The authors would like to thank Andre Jaggi, Umang Poddar and Srinivas Narasimhan for their help with this submission.

considered in order to empower users to own and take control of his/her personal data? In particular, what are the new capabilities that must be granted to consumers over the use of their Personal data? 18

4.3 What should be the Rights and Responsibilities of the Data Controllers? Can the Rights of Data Controller supersede the Rights of an Individual over his/her Personal Data? Suggest a mechanism for regulating and governing the Data Controllers. 22

4.4 Given the fears related to abuse of this data, is it advisable to create a technology enabled architecture to audit the use of personal data, and associated consent? Will an audit-based mechanism provide sufficient visibility for the government or its authorized authority to prevent harm? Can the industry create a sufficiently capable workforce of auditors who can take on these responsibilities? 23

4.5 What, if any, are the measures that must be taken to encourage the creation of new data based businesses consistent with the overall framework of data protection? 24

4.6 Should government or its authorized authority set up a data sandbox, which allows the regulated companies to create anonymized data sets which can be used for the development of newer services? 25

4.7 How can the government or its authorized authority set up a technology solution that can assist it in monitoring the ecosystem for compliance? What are the attributes of such a solution that allow the regulations to keep pace with a changing technology ecosystem? 29

4.8 What are the measures that should be considered in order to strengthen and preserve the safety and security of telecommunications infrastructure and the digital ecosystem as a whole? 31

4.9 and 4.10 What are the key issues of data protection pertaining to the collection and use of data by various other stakeholders in the digital ecosystem, including content and application service providers, device manufacturers, operating systems, browsers, etc? What mechanisms need to be put in place in order to address these issues? Is there a need for bringing about greater parity in the data protection norms applicable to TSPs and

other communication service providers offering comparable services (such as Internet based voice and messaging services). What are the various options that may be considered in this regard? 34

4.11 What should be the legitimate exceptions to the data protection requirements imposed on TSPs and other providers in the digital ecosystem and how should these be designed? In particular, what are the checks and balances that need to be considered in the context of lawful surveillance and law enforcement requirements? 35

4.12 What are the measures that can be considered in order to address the potential issues arising from cross border flow of information and jurisdictional challenges in the digital ecosystem? 40

1. Preliminary

This submission presents comments by the Centre for Internet and Society, India ("CIS") on the Consultation Paper on Privacy, Security and Ownership of the Data in the Telecom Sector published by the Telecom Regulatory Authority of India dated August 9, 2017. CIS has conducted research on the issues of privacy, data protection and data security since 2010 and is thankful for the opportunity to put forth its views. The submission was made on November 6, 2017.

This submission is divided into four main parts. The first part, 'Preliminary', introduces the document; the second part, 'About CIS', is an overview of the organization; and, the third part contains the 'General Comments' on the Consultation Paper; and the final part contains the 'Specific Comments' on the questions posed in the Consultation Paper.

2. About CIS

CIS is a non-profit organisation that undertakes interdisciplinary research on internet and digital technologies from policy and academic perspectives. The areas of focus include digital

accessibility for persons with diverse abilities, access to knowledge, intellectual property rights, openness (including open data, free and open source software, open standards, open access, open educational resources, and open video), internet governance, telecommunication reform, freedom of speech and expression, intermediary liability, digital privacy, and cybersecurity.

CIS has conducted extensive research into the areas privacy, data protection, data security, and into the telecommunications sector. CIS values the fundamental principles of justice, equality, freedom and economic development. This submission is consistent with CIS' commitment to these values, the safeguarding of general public interest and the protection of individuals' right to privacy and data protection. Accordingly, the comments in this submission aim to further these principles.

3. General Comments

The specific questions raised in the Consultation Paper are addressed below in Section 4. In this sections we provide our general comments on the paper and issues which are not addressed in the specific questions posed. The Consultation Paper calls out a number of issues challenging data governance in India. At the outset, CIS holds that there is a dire need for a robust data protection framework in India and it must be noted that a Committee of Experts has been created for this purpose by the Ministry of Electronics and Information technology. This Consultation Paper raises pertinent questions, however, some of them, we feel, may be beyond the jurisdiction of the Telecom Regulatory Authority of India, and should be addressed by the data protection legislation. We have called these questions out in our response. Below we comment on some key issues raised in the Consultation Paper.

Data as Property

The paper states in paragraph 1.4: "In the context of data protection, it is also important to establish the ownership of the data. For instance, if the data is recognized as belonging to the

user to whom it pertains, then this data becomes available for use by them to better their own lives. This brings in the dimension of empowerment to the user."

This echoes various opinions circulated recently regarding vesting the ownership of data generated on the data subjects.[2] This view seems to endorse a propertarian view of data. Though viewing data as property can enable individuals to claim physical loss or damage it can also allow individuals to trade in their own data. This can be problematic for two reasons: one, given the poor levels of awareness among consumers about the quality and quantity of data that is collected, it is likely that data trading systems will be biased in the favour the service providers in terms of *de facto* real world operation. The second problem is that given the cross border nature of data flow and jurisdictional loopholes, ensuring that regulatory rules on data trading are observed in cyberspace will be, at least in the current international status quo, a uphill task for enforcement. However, neither this paper, nor other articles[3] engage with the questions of what this entails. As opposed to a traditional understanding of property, data is a non-rivalrous good, in the the sense that there can be simultaneous users of the good and the use of data by one person does not make it less available to another. There are also certain models, such as data collection and use disclosure based on the consent principle, that can serve as indirect ways of strengthening user control and reducing data's non-rivalrous nature as a good. Therefore, while it is important to view data as having user interests vested in it, from which specific rights and privileges flow, giving it the character of property would pose various economic and legal issues. Economic issues would include those traditionally associated with the ownership and trade of goods, such as taxation while legal issues would include the need to update property rights legislation, across a broad spectrum, to account for the transient and often ephemeral nature of data.

[2] Why India needs to be a data democracy, Nandan Nilekani - http://www.livemint.com/Opinion/gm1MNTytiT3zRqxt1dXbhK/Why-India-needs-to-be-a-data-democracy.html
[3] Taking a Fresh Guard Rethinking Data in Light of the Privacy Judgment, Agnidipto Tarafder and Arindrajit Basu - http://www.epw.in/journal/2017/40/commentary/taking-fresh-guard.html

Data Monopoly

The paper raises questions about data monopoly. In Section 1.5, it states as follows: "Since the service providers, through the provision of service generate and hold the data, it gives them an advantage, which they can use to get into adjacencies (and thus extending their monopoly). This results in harm to the market. The government or its authorized agency may take steps to make this data portable, under the control of the user, thus enabling the creation of newer services."

The recognition of the need for data portability is a welcome step, and the advantages of data portability in the hands of data subjects is reflected in more detail below in Section 4. We appreciate the consultation paper for initiating the much needed discussion on the market power of data in India, and the competition issues it poses. The suggestions to create a 'data sandbox' could be a possible mechanism to address this issue by bringing data from different stakeholders in one place. However, any such step must be voluntary and any steps to compel contribution of data to curb monopolistic practices must ideally be undertaken by or in consultation with the Competition Commission of India, after taking into account the appropriate issues of competition law and economics.

Privacy Principles

We welcome the recognition in the Consultation Paper of the National Privacy Principles as formulated by the Committee of Experts led by Justice AP Shah. These principle, we believe, are key to any data protection legislation to be enacted in India. We also believe that some of these privacy principles need to be rethought in light of technological developments such as big data, and we have published a report capturing how they may be updated.[4] These suggestions are also captured below in Section 4 under relevant questions.

[4]Rethinking National Privacy Principles - Evaluating Principles for India's Proposed Data Protection Law. Amber Sinha, Elonnai Hickok and Vipul Kharbanda - https://cis-india.org/internet-governance/files/rethinking-privacy-principles

4. Specific Comments

4.1 Are the data protection requirements currently applicable to all the players in the ecosystem in India sufficient to protect the interests of telecom subscribers? What are the additional measures, if any, that need to be considered in this regard?

CIS has pointed out in its previous research, as well, that the existing framework of data protection laws in India, is inadequate to comprehensively protect the rights and interests of telecom subscribers.[5] There are a number of applicable legislation and policies that contain provisions with a bearing on the right to privacy and data security in the telecommunications sector in India. These include:

- Section 43A of the Information Technology Act and associated Rules
- Section 69 of the Information Technology Act and associated Rules
- Section 69B of the Information Technology Act and associated Rules
- Section 72A of the Information Technology Act
- Section 67C of the Information Technology Act
- Section 79 of the Information Technology Act and associated Rules
- Unified Access Service License (UASL), and Unified License (UL)
- Section 5 of the Indian Telegraph Act and the 419A Rules
- Guidelines for Protection of Critical Information Infrastructure
- Guidelines, circulars, and notifications from TRAI

[5] State of Privacy in India, Privacy International - https://www.privacyinternational.org/node/975

Depending on the services offered, a number of other sectoral legislation and policy could also be applicable such as notifications and circulars from Reserve Bank of India, the Credit Information Companies Act 2005 etc.

However, these laws and policies do not provide adequate protection with the respect of the following matters:

A. **Limited Protections for Personal Information**: Though the Rules found under section 43A define a (limited) data protection regime, the majority of this regime extends only to sensitive personal data and do not fully apply to 'personal information' - for example only Rule 4 applies to personal information and sensitive personal data or information while Rules 5, 6, and 7 apply only to sensitive personal information.

   Recommendation: It is recommended that any data protection policies formulated by the TRAI should address all forms of personally identifiable information, including both sensitive and non-sensitive personal information.

B. **Lack of Regulation of the Public Sector**: Section 43A and associated Rules apply only to body corporate. Thus, there are no clear prescribed data protection standard for collection and use of data a by the public sector. This is particularly problematic in the communications sector as the Unified Access license requires service providers to collect and retain CDRs, subscriber information, traceable identities of subscribers. and location data and to share the same with the licensor or 'designated authorities when required. [6]

[6] Licence Agreement for Provision of Unified Access Services, Ministry of IT and Communications, Government of India - http://www.dot.gov.in/sites/default/files/UAS%20license-agreement-19-12-2007.pdf?download=1

Recommendation: It is recommended that any policies formulated by TRAI apply equally to collection, access and use of communications data by both the public and private sector.

C. **Definition of Personal and Sensitive Personal Data**: Under the 43A Rules personal information is defined as *"any information that relates to a natural person, which, either directly or indirectly, in combination with other information or likely to be available with a body corporate, is capable of identifying such person."* Listed categories of sensitive personal data include "password, financial information, physical, physiological and mental health condition, sexual orientation, medical records and history, and biometric information".[7] The definition of personal data under the Rules is limited to data that is or likely to be available with body corporate. This eliminates data that may rest with other types of entities and vastly narrows the scope of the definition of personal information. Communication companies may or may not be accessing data that rest with entities beyond body corporate. Further, definitions of PI and SPDI in the Rules do not take into consideration the blurring of lines between non-PI, PI, and SPI and the sensitivity of the same.

Recommendation: Please refer to recommendation in 4.2

D. **Privacy Policy**: According to Rule 4 of the 43A rules, body corporate must provide a privacy policy that meets the following requirements:
(i) Clear and easily accessible statements of its practices and policies;
(ii) type of personal or sensitive personal data or information collected under rule
(iii) purpose of collection and usage of such information;
(iv) disclosure of information including sensitive personal data or information as provided in rule 6;

[7] Information Technology (Intermediaries guidelines) Rules, 2011, Ministry of Communications and Information Technology, Government of India - http://www.wipo.int/edocs/lexdocs/laws/en/in/in099en.pdf

(v) reasonable security practices and procedures as provided under rule 8

Recommendations: Today there is vast information asymmetry between users and service providers. Users are consenting to privacy policies and terms of service that are complicated, filled with legalese, and overly broad - not accounting for the multitude of ways in which their data is actually processed, shared, and used. Clear, accessible, comprehensive, and timely privacy policies are an important part of addressing this information asymmetry. The requirement for a privacy policy can be strengthened and improved in the following ways[8]:

- *Timing of the privacy notice The privacy notice shouble be provided at the time of collection from the data subject, and, where the personal data are obtained from another source, at the time of receipt of data from such source.[9] Tools such as 'sticky privacy policies' can be employed to ensure that users understand and control how their data is being used as a service evolves and the data travels across entities.[10]*

- *Communication of the privacy policy: The privacy policy should be accessible, easy to understand, in clear, intelligible, and concise language. Icons, visuals and other tools of communication are increasingly being used to ensure effective communication of policies.*

[8] The Ranking Digital Rights Project is an index that evaluates 22 of the world's internet, mobile, and telecommunications companies' policies and practices affecting users' freedom of expression and privacy. The index has defined a strong set of criteria for transparency of a company's privacy policy. Many of the recommendations below have been drawn from this criteria. For more information see: https://rankingdigitalrights.org/

[9] Traditionally, the notice and consent regime only involves notification from the data collector directly collecting personal data from the data subject. Given the indiscriminate sharing of data in the age of big data, we suggest introducing another layer of notice, wherein each data controller in receipt of personal data from other service providers must notify the data subject as well. This additional layer of notice is also reflected in Article 14 of the GDPR (Available here: http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf)

[10] Sticky Policies: An Approach for Managing Privacy across Multiple Parties, Siani Pearson and Marco Casassa Mont. https://documents.epfl.ch/users/a/ay/ayday/www/mini_project/Sticky%20Policies.pdf

- *Accessibility of privacy policy: In some cases companies provide a privacy policy for the website and include additional provisions and terms on privacy in their ToS that are only available to an individual after signing up for a service.*

  Recommendation: All provisions related to privacy should be located in the privacy policy and should relate to all services offered by a company. This privacy policy should be available on a company's website regardless of if a the user is a subscriber to a particular service.

- Updating privacy notices: It is presently not a legal requirement or industry practice in India to notify users of changes to a privacy policy and contain an archive of the same.

  Recommendation: If a privacy policy is amended, this change should be proactively communicated by the service provider to users and an archive of the same should be available to users so as to enable a comprehensive understanding of the evolution of a company's privacy policy.

E. **Consent**: The Information Technology Act presently requires body corporate to obtain consent in *"writing, through letter or Fax or email from the provider of the sensitive personal data regarding purpose of usage before collection of such information".* Under the Unified Access license service providers are required to maintain confidentiality and privacy of users unless *"...the information relates to a specific party and that party has consented in writing to such information being divulged or used, and such information is divulged or used in accordance with the terms of that consent."*[11] This

[11] Licence Agreement for Provision of Unified Access Services, Ministry of Communications and Information Technology, Government of India - http://www.dot.gov.in/sites/default/files/UAS%20license-agreement-19-12-2007.pdf?download=1

consent can also be in the electronic format, as mentioned in the license. Inadequacies in this consent mechanism include:

- **Limited Scope:** This form of consent is limited in its scope (to sensitive personal data).
  Recommendation: As mentioned above, the requirement of consent should be extended to all forms of collection and processing of personally identifiable information.

- **Lack of Informed Consent:** The mechanism does not incorporate standards for the consent such as that it is fully informed and freely given. This can allow for practices such as pre-ticked boxes and consent through use of a service.
  Recommendation: The GDPR establishes a strong standard for consent that can be considered when formulating privacy standards in India. According to the GDPR - consent should be freely given, specific, informed, and unambiguous and should be given through an affirmative action such as ticking a box or choosing technical settings for information society services.[12]

- **One Time and Binary consent**: The consent mechanism in 43A and associated rules is a one time mechanism taken prior to the collection of information. This does not address how informed consent will be taken in an ecosystem where multiple, different, and complicated transactions take place between service providers and users on a range of platforms and across the span of a service.
  Recommendation: When the purposes for which personal data are collected are modified or expanded subsequent to its collection, consent should deemed to be specific only if it is obtained afresh in respect of that modification or expansion, prior to any use of that data for the modified or expanded purposes. Where data

[12] General Data Protection Regulation (Regulation (EU) 2016/679) - http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

being collected is merely incidental and not essential to the service being provided, then agreeing to a privacy policy that mandates collection of such data should not be a condition precedent to avail the services in question.

- **Opt-Out**: Currently Rule 5 (7) of the Section 43A Rules specifies that any time while availing the services or otherwise, also have an option to withdraw its consent given earlier. However, the Rules do not specify that the opt-out option needs to be easily implemented as the consenting to data collection. The design of data collection systems often focus on collection of data and incentivise opt-out. It is important that data subjects are able to opt-out when they choose to do so as easily as they can opt-in.

  Recommendation: The data subject should have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Technical measures can be implemented to ensure consent is contextualized and relevant to a use - such as 'just in time consent'. It is important that data subjects are able to opt-out when they choose to do so as easily as they can consent to data collection.

F. **Access and Correction**: The associated Rules to 43A provide that that body corporate permit individuals to access and correct information that they have provided. The body corporate is further not responsible for the authenticity of the data provided. This access mechanism is limited in the following ways:

  - Limited Scope: The mechanism allows individuals to only access data they have provided. This seems to assume direct collection from the individual through a form or otherwise. Yet, present day mechanisms allow data to be collected directly and indirectly from and about an individual.n.

    Recommendation: Users should be able to access all data collected and observed about them from the data controller.

- **Lack of Standards for User Control:** The mechanism only provides individuals the ability to access data but does not specify standards for this access. By not enabling individuals to obtain copies, move, or delete their data the mechanism does give users clear control over their personal data. As argued before in the submission, CIS believes that effective, continuing and enforceable ownership of data is vital to protecting user rights and consumer interest. The mechanism of access can empower the user with greater control of their data. The present mechanism only addresses correction of their data.
  Recommendation: Data collected and accessible by data controllers should be made available to the data subject in a structured, machine-readable as well as human-readable format. The received data should be portable across services. The data subject shall have the right to ensure from the data controller, the rectification of inaccurate or incomplete personal data, without any undue delay, especially in cases where the incompleteness or inaccuracy of the data has adverse impacts on the data subjects. Additionally, the data subject should be able seek the purposes of the processing, the recipients or categories of third party recipient to whom the personal data have been or will be disclosed, the intended time period of which the data would be stored, details of sources where data was not obtained directly from the data subject.

G. **Purpose and Collection Limitation**: While the 43A rules have some purpose and collection limitation principles these are confined to sensitive personal data and include a statement noting that information collected should only be used for the purpose for which it was collected and that sensitive personal data should only be collected for lawful purposes, connected to a function of the body corporate and necessary for a purpose. These standards are insufficient as they do not directly connect the purpose limitation to the purposes and use consented to and tied to the duration of a service.

Recommendations: The collection of personal data pursuant of the consent of the data subject should be valid only if it is obtained in respect of the purposes and duration strictly necessary to provide the product or service in relation to which personal data is sought to be collected, processed or disclosed. A data controller should collect, process, disclose, make available, or otherwise use personal information only for the purposes as stated in the notice after taking consent of individuals. If there is a change of purpose, this must be notified to the individual, and only after the individual has consented to the new purpose, should the data be processed for such purposes.

H. **Retention and Deletion**: There are a number of provisions in Indian law and policy that address retention of data. Under 43A and associated Rules, Body corporate should not retain sensitive personal data for longer than is required for the purposes for which the information may lawfully be used. Under the UASL, service providers are required to retain a range of information through direct requirements- such as retaining subscriber information for one year- and indirect requirements such as being able to provide traceable identities and location data of subscribers.[13] Under section 79 and associated Rules of the IT Act, intermediaries must retain unlawful content that has been removed for a period of 90 days. Section 67C of the IT Act allows the government to define the manner and duration of retention of information by intermediaries with a penalty of three years imprisonment and a fine for non-compliance. These standards are vague and, place disproportionate penalties on intermediaries for non-compliance, and do not address deletion of data.

Recommendations: After personal information has been used in accordance with the identified purpose it should be destroyed as per the identified procedures. In case of retention obligations on telecom services providers, the principles of data minimisation must be be followed and only information necessary and proportional to be retained for

[13] Licence Agreement for Provision of Unified Access Services, Ministry of Communications and Information Technology, Government of India - http://www.dot.gov.in/sites/default/files/UAS%20license-agreement-19-12-2007.pdf?download=1

the clearly identified objectives of retention must be retained, for only as long as required and reasonable.

I. **Security:** The current rules framed under Section 43A of the Information Technology Act are extremely limited in their scope. They are limited in their scope due to their non-specific obligations, lack of enforceability, failure to account for modern developments in digital security and absence of requiring independent, third party audits of measures already in force.

Recommendations: A data controller shall take measures, including, but not restricted to, technological, physical and administrative measures, to secure the confidentiality, secrecy, integrity and safety of all information collected including but not limited to personal data, including from theft, negligence, loss or unauthorised disclosure. The security measures, as appropriate may include, without limitation: a) de-identification of personal data, b) ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident, and c) ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems.

J. **Transparency:** Transparency of company policies and practices is one of the key ways in which service providers can empower the individual to understand how their data is being collected, used, and accessed and make informed decisions on the same. Publication of transparency reports has been a growing trend with global ICT companies including Facebook, Google, Microsoft, and Vodafone. Presently, the policy ecosystem for communication service providers in India does not incentivise transparency of company practices and policies, and prohibits disclosure of information pertaining to a direction for the interception, monitoring, or decryption of communications.[14]

Recommendation: There needs to be clear reporting requirements for data controllers to publish periodic transparency reports. These reports should include information about

[14] Ranking Digital Rights - https://rankingdigitalrights.org/

data processing practices to better inform users. Further, the reports should also highlight any security incidents and steps taken by the data controllers to address the issues. Accordingly, the policies prohibiting disclosures about interception, monitoring, and decryption need to be modified.

K. **Liability:** In Indian law, the concept of liability for 'wrongful loss or wrongful gain' to any person due to the lack of 'reasonable security procedures and practices' in the handling of sensitive personal data by corporate bodies can lead to compensation being paid to the aggrieved parties depending on the extent of harm caused.[15]
Recommendations: It is recommended that a liability and redressal regime which places the onus on the individual to demonstrate the 'actual harm' caused to her may be too limiting in the the age of big data and ubiquitous data collection, as often the implications of data breaches on privacy and other rights of the individual against discrimination may not be fully demonstrable.

L. **Disclosure**: Under Rule 6 of the 43A Rules , any body corporate must take consent from the data subject before releasing or sharing any information with any organization other than the government and other authorized agencies – these administrative organizations can ask for such information by written request upon situations dealing with cybersecurity and prosecution of offences. Under Rule 6(2), any sensitive personal data can be shared with a third party by an order mandated by the law currently in force – thereby, showing that privacy of the data subject can be bypassed by a written request as well as an order under law.
Recommendations: Any policies on disclosure of personal data to third parties must clearly specify that a data controller shall not disclose personal information to third parties, except after providing notice and seeking informed consent from the individual for such disclosure. Third parties are bound to adhere to relevant and applicable privacy

[15] § 43A of the Information and Technology Act, 2008 available at - http://www.eprocurement.gov.in/news/Act2008.pdf.

principles. Disclosure for law enforcement purposes must be in accordance with the laws in force. Data controllers shall not publish or in any other way make public personal information, including personal sensitive information.

Additionally, there are matters of data protection relevant to telecom subscribers which are presently not addressed in Indian law.. They are as follows:

A. Data Portability

The concept of data portability looks to empower the individual by delivering ownership of the data to him or her – thereby, giving the power of controlling and regulating which service provider uses the data back to the person who created the data in the first place. Currently, Indian law does not provide for this right. The introduction of such as right would enable users to easily migrate to other service providers and also foster competition in the market.

B. Cookies

Cookies are universally used by websites to track browser-server interactions, and can increasingly be used to collect large amounts of data pertaining to browsing history, the frequently used pages and even other personal information depending on the kind of cookie it is.[16] These cookies are commonly used for profiling users, identifying different character traits and tendencies – and using this information for marketing through ads or processing this data for other uses.[17] Currently, the relevant legislations that cover data protection and privacy in India do not discuss the implications of cookies, and do not include basic cookie regulation law such as

[16] Bittersweet cookies. Some security and privacy considerations - Rodica Tirtea, Claude Castelluccia and Demosthenes Ikonomou. - https://www.enisa.europa.eu/publications/copy_of_cookies/at_download/fullReport
[17] *Ibid*.

whether websites must alert users of the presence of cookies and notify do-not-track options clearly.[18]

C. Automated Data Processing and Algorithms

In the case of service providers employing automated or algorithmic decision making that has a direct bearing on users, regulation should ensure that

- Appropriate statistical techniques are used
- Transparency of algorithmic logic,
- Measures are in place to correct inaccuracies and risks of errors;
- Security is ensured and
- Discriminatory effects prevented and addressed if they arise.

To minimize concerns of unauthorised data usage, organizations should make attempts disclose the logic underlying their decisionmaking processes to the extent possible without compromising their trade secrets or intellectual property rights.

4.2 In light of recent advances in technology, what changes, if any, are recommended to the definition of personal data? Should the User's consent be taken before sharing his/her personal data for commercial purposes? What are the measures that should be considered in order to empower users to own and take control of his/her personal data? In particular, what are the new capabilities that must be granted to consumers over the use of their Personal data?

A. Personal data

The use of technologies which lead to ubiquitous and continuous collection and processing of data has led to significant changes both in the scale and nature of data

[18]Internet Privacy in India - https://cis-india.org/telecom/knowledge-repository-on-internet-access/internet-privacy-in-india

collection and use. Personal data processed by the data controllers usually includes the following kinds of data:

a) Data actively provided by the data subject: This includes data such as mailing address, user name, age, etc.)

b) Observed data: This includes data which are "provided automatically" by the data subject by virtue of the use of the service or the device. For example, a person's search history, preferences and choices, traffic data and location data. It could also include other raw data such as the heartbeat tracked by fitness or health trackers, which is observed and not actively provided each time by the user.

c) Inferred data and derived data: This includes data about the data subject created by the data controller/processor on the basis of the data provided by the data subject. This would include building of profile of individuals by data controllers based on inferences made by them on data collected.

Recommendation

The definition of personal data should be clarified to include all three of the above kinds of data. This clarification could be a subset of the broader definition of personal data which includes any data which relates to a natural person if that person can, whether directly or indirectly in conjunction with any other data, be identified from it and includes sensitive personal data.

Further, certain categories of data ought to be defined as sensitive personal data and must include the following (based on the GDPR)[19]: (i) biometric data; (ii) deoxyribonucleic acid data (iii) sexual preferences and practices; (iv) medical history and health; (v) political affiliation; (vi) ethnicity, religion, race or caste; and (vii) financial and credit information, including financial history and transactions.

[19] General Data Protection Regulation (Regulation (EU) 2016/679) - http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

B. User Consent

Consent should be taken before sharing a data subject's personal data for commercial purposes and the names of the type/names of the third parties should be disclosed. Furthermore, companies should be prohibited from refusing to offer services to customers who choose not to share information for commercial purposes. Consent should not be a tool of coercion, ie., if data being collected is merely incidental and not essential to the service being provided, then agreeing to a privacy policy that mandates collection of such data should not be a condition precedent.

Plans that offer reduced plans for blanket consent from the user for access and use of their personal data should be disallowed. Such plans risk creating divides between those who can afford privacy and those who cannot and risk inflating the price of plans that provide greater privacy control.

C. Rights to Empower Users

We see the following as essential rights for users:

- Right to an easy-to-understand privacy notice: All persons must be afforded an easily accessible, simple to understand and clear privacy notice that will serve to resolve any discrepancies or doubts that may be possessed by potential data subjects before they give consent.

- Right to Withdraw: The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.

- Right against unfair denial of service: All persons shall have the right against unfair denial of services on the grounds that such persons do not agree to

share data, not essential but merely incidental to the provision of service, being made a precondition to the provision of services.

- Right to Access: The data subject shall have the right to obtain from the controller access to the personal data collected and/or being processed. Additionally, the data subject can seek the purposes of the processing, the recipients or categories of third party recipient to whom the personal data have been or will be disclosed, the intended time period of which the data would be stored, details of sources where data was not obtained directly from the data subject. The data should be made available by the controller in a structured, machine-readable as well as human-readable format. This should include both data directly collected from the data subject as well as data observed about the data subject.

- Right to Portability: The concept of data portability allows for data that is collected and stored by one data controller, to be transmitted (including but not limited to the original collected data, but also any results that may have been unearthed) to another controller without any hindrance from the former.

- Right to access when data is indirectly obtained: All persons shall have a right to obtain access to data that has indirectly come into the possession of a data controller from a third party, and that is personally identifying of an individual.

- Right to access data about previous breaches: All data subjects should possess the right to enquire about any previous breaches that may have occurred with respect to that specific service provider, and any other instances of security being undermined. The steps taken by the data controller to curb the previous breaches, and to ensure that it doesn't happen again should also be accessible by the subject.

- Right to Deletion: All subjects should be allowed to ask for and verify the complete erasure of all data held by the service provider about them, including data that is explicitly provided by the user as well as indirect data that the service provider can 'create' by observing, analysing and correlating data and patterns.

4.3 What should be the Rights and Responsibilities of the Data Controllers? Can the Rights of Data Controller supersede the Rights of an Individual over his/her Personal Data? Suggest a mechanism for regulating and governing the Data Controllers.

- **Scope of Powers of Data Controllers**

  The scope of powers that data controllers have should be strictly limited by the nature of consent provided to the data subject or as otherwise required in the law.[20] A data controller shall collect, process, disclose, make available, or otherwise use personal information only for the purposes as stated in the notice after taking consent of individuals. If there is a change of purpose, this must be notified to the individual, and only after the individual has consented to the new purpose, should the data be processed for such purposes. After personal information has been used in accordance with the identified purpose it should be destroyed as per the identified procedures.

- **Legitimate Interest Exception**

[20] For example, the Report of the Group of Experts defines the following exceptions to the right to privacy: national security, public order, disclosure in public interest, prevention, detection, investigation, and prosecution of criminal offences,and protection of the individual or of the rights and freedoms of others. http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf The Information Technology Act, UAL, and Indian Telegraph Act also lay out a number of requirements for service providers that they need to comply with.

Where legitimate interests of data controllers can supersede rights of individual - The data controller may be allowed to process data for purposes other than those expressly consented to by the data subject in cases where it can demonstrate the existence of a legitimate interest. This legitimate interest of the data controller shall be limited by the interests of the data subject which require protection of data. Factors relevant for determining the existence of a legitimate interest shall include the the reasonable expectations of data subject, whether processing leads to an adverse impact on the data subject, overriding public interest, nature of the data that are processed (sensitive or not), the relationship between the data subject and the controller and their respective positions of power, and the measures that the controller has taken to reduce the impact on the privacy of the individuals.[21]

4.4 Given the fears related to abuse of this data, is it advisable to create a technology enabled architecture to audit the use of personal data, and associated consent? Will an audit-based mechanism provide sufficient visibility for the government or its authorized authority to prevent harm? Can the industry create a sufficiently capable workforce of auditors who can take on these responsibilities?

- **Audit as a Mechanism of Data Protection**

  Data protection regimes globally have recognised the value of audit in educating and assisting organisations to meet their obligations. For instance, the UK Data Protection Act provides powers for the the UK ICO to assess any organisation's processing of personal data for the following of 'good practice', with the agreement of the data controller. This includes, but is not limited to, compliance with the requirements of

[21] Moerel, Lokke and Prins, Corien, Privacy for the Homo Digitalis: Proposal for a New Regulatory Framework for Data Protection in the Light of Big Data and the Internet of Things (May 25, 2016). Available at SSRN: https://ssrn.com/abstract=2784123.

the regulator. This is known as a consensual audit. Further, there can also be provisions to conduct compulsory audits. This would enable the regulator to serve government departments, designated public authorities and other categories of designated persons with a compulsory 'assessment notice' to evaluate their compliance with the data protection principles.

- However, it is important to recognise that audits have limited utility as they can only look at aspects of procedural compliance and thus need to be complemented with robust mechanisms for redress and comprehensive policy . It is unclear from this question how the TRAI envisages the use of a technological infrastructure for audits to see if consent has been appropriately taken.

4.5 What, if any, are the measures that must be taken to encourage the creation of new data based businesses consistent with the overall framework of data protection?

No detailed suggestions or comments apart from the suggestions made on Data Sandboxes in Section 4.6, suggestions made for incentivizing privacy protecting tools and compliance software in Section 4.7 and general measures that can be taken to create regulatory sandboxes[22] (independent of data sandboxes) to allow for rapid innovation to occur unhindered excessive regulation but without putting users as risk .

[22] Regulatory Sandboxes – How, Who and Why? - Pavel Shoust. http://pubdocs.worldbank.org/en/770171476811898530/Session-4-Pavel-Shoust-Regulatory-Sandboxes-21-09-2016.pdf

4.6 Should government or its authorized authority set up a data sandbox, which allows the regulated companies to create anonymized data sets which can be used for the development of newer services?

When considering the creation of a data sandbox it is important to define how the sandbox will operate. For example access standards to the sandbox, purposes for which the information can be used, security standards, anonymization standards etc. t Towards defining the above we have laid out key aspects of data sandboxes, along with key policy questions that will need to be resolved while setting up such a sandbox.

- **What is a data sandbox?**

  A Data Sandbox is a non-operational environment where the analyst can model and manipulate data inside the data management system. Data sandboxes have been envisioned as a secure area where only a copy of the company's or participant companies' data is located.[23] In essence, it refers to the scalable and creation platform which can be used to explore an enterprise's information sets. The distinction between a Sandbox and a Warehouse is that an analytic sandbox can be thought of as an area carved out of the existing data warehouse infrastructure. It provides the environment and resources required to support experimental or developmental analytic capabilities. It is a place where these new ideas, hypotheses, data sources, and tools can be utilized, tested, evaluated, and explored. Meanwhile, the data warehouse stands as the prerequisite data foundation containing the historically-accurate enterprise data that the analytic sandbox efforts spin around and against.

  Given the emerging regulatory trends globally and conversation around the same in India, it important to note that a data sandbox is entirely different from a regulatory

[23] A Data Sandbox for Your Company - http://terrificdata.com/2016/12/02/3221/.

sandbox. While the primary purpose of a data sandbox is to analyze and perform operations on data, regulatory sandboxes are controlled environments where firms can introduce innovations to a limited customer base within a relaxed regulatory framework, after which they may be allowed entry into the larger market after meeting certain conditions. This purportedly encourages innovation through the lowering of entry barriers by protecting newer entrants from unnecessary and burdensome regulation. Regulatory sandboxes can be interpreted as a form of responsive regulation by governments that seek to encourage innovation – they allow selected companies to experiment with solutions within an environment that is relatively free of most of the cumbersome regulations that they would ordinarily be subject to, while still subject to some appropriate safeguards and regulatory requirements.

Examples of Data Sandboxes

- Sandbox Proposal by the Singapore Government[24]

  The government of Singapore is planning to roll-out a data sandbox in late 2017 to facilitate experimentation and innovation. The idea behind this sandbox is to align the data sets so there are more opportunities for data to be discovered and enable interested, qualified, parties to come together to create data driven solutions to existing problems.

- Alibaba-NUS-EZlink[2][25]

  Alibaba Cloud, the National University of Singapore and the cashless transaction firm, EZlink, have planned to set up a big data initiative. With Alibaba Cloud's global technological prowess, NUS' growing digital know-how and EZ-Link's cashless

[24] Singapore government plans to roll out a 'big data sandbox' this year - Kevin McSpadden. https://e27.co/singapore-government-plans-roll-big-data-sandbox-year/

[25] Alibaba Cloud, NUS and EZ-Link tie-up for big data initiative in Singapore - Kevin McSpadden. https://e27.co/alibaba-cloud-nus-and-ez-link-tie-up-for-big-data-initiative-in-singapore/

expertise, a framework is to be set up in order to convert usage pattern data into actionable intelligence. Alibaba Cloud will also contribute US$500,000 in cloud credits to allow NUS students and researchers to use the service for academic and research purposes.

- Singapore-London Data Sharing Initiative[26]

  A global data sharing initiative was launched to build and provide managed access to a rapidly increasing number of data points provided by the public and private sector between Singapore and London, synchronized by time and location.

Open Questions and Recommendations

The sandbox must aim to be an environment in which analysts and data scientists can test new tools, see what approaches their peers are taking, share their work, get help, and develop effective business cases to procure relevant software.

- **Access:** The primary issue in the case of any state controlled data sandbox is that of how access is controlled and granted to the data sandbox. There could be three different models of access that may be followed: a) Access is restricted to Governmental bodies and entities only; b) Access is given to authorized private companies and entities, which involves formulating a justifiable criteria for such authorisations; or c), Access to the database can be given to the general public with possible limitations in the form of license conditions or requisite permissions. Ideally, all three of these forms of access should be incorporated into the framework for the sandbox towards achieving data democracy.

  In the case that the access is granted to the public or companies, the next questions is the level of access these parties will have to the data. In essence, it must be decided

[26] *ibid*

whether the entirety of the data is accessible to every entity or the data is fragmented into portions to which different entities have access to.

We recommend that access to data is not absolute, i.e., not all entities can be allowed to gain access to all kinds of data that can be accessed through the sandbox. To solve this issue, a multi-tiered system can be adopted with regard to access to data. Certain types or "tiers" of data can be accessed only by entities specifically authorized to do so. For example, access to the most sensitive of data will only be given to entities with the highest level of authorization and so on. Importantly, this allows for any potential misuse of data to be checked.

- **Ownership:** There are also questions regarding the ownership of the sandbox platform, or more accurately, the structure of the ownership of the platform, whether it is solely owned and operated by a Governmental organization/regulator, whether it is a joint venture or if it is to be run wholly by a private entity, or a special purpose vehicle created for this purpose.

- **Security and De-Identification:** It needs to be noted such an initiative can be potential 'honeypot' for fraudulent activities, and it is imperative that only de-identified datasets be included in the data sandbox. For this purpose, the regulator must collaborate with the academia and industry to prescribe robust data de-identification and security measures that are followed by all participants.

- **Standards for Use:** It is possible that the data sandbox may be misused or used for purposes that do not support the goals of the sandbox. It is important that the goals of the sandbox and appropriate use are defined and could include for example: innovation, public good, public interest, development etc. The use of the sandbox could also serve as an additional mechanism for defining access. For example, a

proposed use of the sandbox for public good could take priority over business innovation.

4.7 How can the government or its authorized authority set up a technology solution that can assist it in monitoring the ecosystem for compliance? What are the attributes of such a solution that allow the regulations to keep pace with a changing technology ecosystem?

The use of privacy enhancing technological solutions is key to the governance of privacy in any jurisdiction. There are softwares now available that can be implemented by companies to ensure, monitor, and report on statutory compliance and whose use may be incentivised by the regulator.[27] There are also technological solutions which will preserve and enhance user privacy, and whose use may be incentivised by regulators in India are listed below:

- **Sticky Privacy Policies**

  Sticky privacy policies involve cryptographic solutions in which policies can stick to data to define allowed usage and obligations as it travels across multiple parties, enabling users to improve control over their personal information. They allow the data subject to decide on a set of conditions and constraints which unambiguously lay down how her/his PII is to be used by the party receiving the data. As the data moves across multiple parties, these policies define an allowed usage and obligations, thus enhancing the control of the data owners over their personal information. They impose prohibitions and obligations such as access of third parties and the purpose for which the data is being used. These policies also allow the data owners to blacklist certain parties from gaining access to their personal information along with laying down rules such as a notice of disclosure and the deletion or minimization of data after a specified period of time.

[27]For Example: https://www.nymity.com/products.aspx, https://www.trustarc.com/, https://privacyperfect.com/

- **Personal Data Stores**

  A Personal Data Store or PDS helps you gather, store, manage, use and share the information. It gives the user a central point of control for their personal information (e.g. interests, contact information, affiliations, preferences, friends). For instance, openPDS can be installed on any server under the control of the individual (personal server, virtual machine, etc) or can be provided as a service (SaaS by independent software vendors or application.

- **DND Options**

  In the case of implementing the principle of Opt Out, data subjects should be provided with options such as a.) no further collection of data, b.) erasure of all previously collected data and the results of processing of such data. In certain cases, it may not be in the public interest to allow erasures of decisions already made on the basis of data collected. This could be facilitated by a system such as a Centralised website/service/phone number/email number - where an individual can withdraw consent easily, for instance through a single SMS for which the syntax is easy to use. Services providers could be automatically informed of such choices, or they could access the details of the users who have opted out periodically (daily or bi-weekly basis) and effect changes. In order to prevent mistaken removal of users, an additional layer of confirmation through email/SMS can also be built in.

- **Standardized Privacy Policies**

  The form in which notices are presented is extremely important. Therefore, summaries, infographics, highlighting relevant and actionable information can go a long way in making notices much more intelligible to laypersons. Some existing models of standardized formats for simple and easy to use privacy notices include the following: i) National Telecommunications and Information Administration (NTIA)

developed a code of conduct for standardized short-form privacy notices for smartphone app. ii) Private Parts is a web based service to simplify privacy notices

- **Privacy by Default**

  Privacy by default is a principle intended to counter the wide use of privacy policies and terms of conditions by services providers to nudge users towards least privacy preserving choices by having maximum data collection and blanket consents as defaults. Implementation of privacy by default would entail that the strictest privacy settings automatically apply when a user signs up for a service. This would be done by ensuring that the default privacy settings would always lean towards privacy enhances choices and technological implementation of the data minimisation principle by automating deletion of data once the purpose has been fulfilled

The above mentioned softwares and technological tools can be developed and incentivised by the regulator through use of co-regulatory steps in collaboration with the industry, the academia and the civil society. However, it recommended that the regulator does not take the responsibility of creating a technological solution for this purpose, as other stakeholders are better suited to perform that role. Through incentivizing these technological tools the regulator will be ensuring that the sector can remain compliant in a technologically evolving ecosystem.

4.8 What are the measures that should be considered in order to strengthen and preserve the safety and security of telecommunications infrastructure and the digital ecosystem as a whole?

In India, the responsibility to ensure a network and associated infrastructure and content is secure and remains confidential lies with the service provider. There are a number of security provisions and standards that service providers must adhere to in India. These include:

- Standards: Adoption of ISO 27001 or developed and approved sectoral standard (43A); network elements must meet ISO/IEC 15408 (UL 39,7); management must meet ISO 27000 (UL 39.7), telecom elements must meet 3GPP2 security standards (UL 39.7). Certification must be done by certified labs in India (UL 39.7) All contemporary security standards must be incorporated when procuring equipment (UL 39.9)
- Annual audits, inspection, and scrutiny: (Section 43A Rules, UL s. 39.2 and s. 39.6)
- Provision of facilities to government: (UL s. 39.1 69)
- Security clearance for foreign personnel: (Ul 39.3)
- Organizational security policy and management including network forensics, hardening, penetration test, and risk assessment (UL 39.5)
- Maintaining records of software details, operation and maintenance command procedure and logs, User ID linked with name and details by the system administrator, software updates and changes, supply chain of hardware and software. (UL 39.9)
- Monitoring facilities for attacks and fraud (UL 39.10)
- Ensure that vendor/supplier allows for security inspection of hardware, software, design, development, manufacturing, and supply chain during the supplies of equipment (UL 39.10)
- Penalty up to 50crore for security breach due to inadvertent inadequacies
- Certain officers like Chief security officer to be resident Indian citizen (UL 39.32)
- Adequate and timely measures to ensure information transacted through a network by subscribers is secure and protected (UL 39.23)
- Accounting and user information relating to a subscriber should not be transferred outside of India (UL 39.32)
- Remote Access network should be provided only to approved locations (UL 39.23)
- Controls: (NCIIPC guidelines)[28]
    - Planning Controls: Identification of CII PC2: Vertical and Horizontal Interdependencies PC3: Information Security Department PC4: Information Security Policy PC5: Integration Control PC6: VTR Assessment and Mitigation

[28] Guidelines for Protection of CII - http://nciipc.gov.in/documents/NCIIPC_Guidelines_V2.pdf

Controls PC7: Security Architecture Controls including configuration Management and Mitigation Controls PC8: Redundancy Controls PC9: Legacy System Integration PC10: Supply Chain Management – NDA's, Extensions and Applicability PC11: Security Certifications PC12: Physical Security Controls

- Implementation controls: Asset and Inventory Control IC2: Access Control Policies IC3: Identification and Authentication Control IC4: Perimeter Protection; Physical and Environmental Security IC6: Testing and Evaluation of Hardware and Softwares
- Operational controls: OC1: Data storage: Hashing and Encryption OC2: Incident Management - Response OC3: Training, Awareness and Skill up-gradation OC4: Data Loss Prevention OC5: Penetration Testing OC6: Asset and Inventory Management OC7: Network Device Protection OC8: Cloud Protection OC9: Critical Information Disposal and Transfer OC10: Intranet Security OC11: APT protection
- Disaster recovery controls: DR1: Contingency Planning – Graceful degradation DR2: Data Backup and Recovery Plan, Disaster Recovery Site DR3: Secure and Resilient Architecture Deployment

The following additional steps need to be taken to ensure the security of telecommunications infrastructure and the digital ecosystem as a whole:

- Companies should have mechanisms for users to report security vulnerabilities in the form of incident reporting and vulnerability disclosures.
- Companies should have in place and disclose information about its process for responding to data breaches, and must publish periodic reports about any security incidents and how they have been responded to.
- All user communications should be encrypted and this should be enabled by default.

- Advanced authentication mechanisms should be used to secure accounts, users should be able to see account activity and companies should notify users about unusual account activity.
- Companies should regularly publish educational material on security for users.[29]

4.9 and 4.10 What are the key issues of data protection pertaining to the collection and use of data by various other stakeholders in the digital ecosystem, including content and application service providers, device manufacturers, operating systems, browsers, etc? What mechanisms need to be put in place in order to address these issues? Is there a need for bringing about greater parity in the data protection norms applicable to TSPs and other communication service providers offering comparable services (such as Internet based voice and messaging services). What are the various options that may be considered in this regard?

The data protection law in India should be neutral to technology and platform, and must apply equally to all data controllers including telecom companies, and OTT content and application service providers. The obligations of telecom companies are addressed in the Unified Licenses entered into the Department of Telecommunications, and there is no need to extend these contractual obligations to any other stakeholders. Instead, the mechanism for regulating other stakeholders should be the data protection legislation. It is recommended that the Unified License is harmonized with the data protection legislation. It is further recommended that any data protection norms applicable to communication service providers such as telecom companies, and OTT service providers which provide comparable services such as messaging and VOIP services, must be privacy preserving and

[29] Ranking Digital Rights: https://rankingdigitalrights.org/

enhancing but not limiting in any way. Therefore, any regulations regarding communication encryption must only specify minimum thresholds, and not limit the level of privacy protection that these services may provide.

4.11 What should be the legitimate exceptions to the data protection requirements imposed on TSPs and other providers in the digital ecosystem and how should these be designed? In particular, what are the checks and balances that need to be considered in the context of lawful surveillance and law enforcement requirements?

Any legitimate exception to the data protection requirements imposed on TSPs and other providers in the digital ecosystem should be clearly defined in law. CIS supports the exceptions recommended in the Report of the Group of Experts on Privacy which include national security, public order, disclosure in public interest, prevention, detection, investigation, and prosecution of criminal offences, protection of the individual or of the rights and freedoms of others. These exceptions should be guided by the principles of proportionality, legality, and necessary in a democratic state.[30]

Further CIS strongly supports the International Principles on the Application of Human Rights to Communications Surveillance and has recommended that laws in India comply with them [31] to ensure that surveillance carried out in the country complies with safeguards and protects human rights. The principles are as follows:

[30] http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf

[31] https://cis-india.org/internet-governance/blog/policy-recommendations-for-surveillance-law-in-india-and-analysis-of-legal-provisions-on-surveillance-in-india-and-the-necessary-and-proportionate-principles.pdf/view

- "**Legality:** Any limitation to privacy rights must be prescribed by law and there should be no interference with these rights in the absence of an existing publicly available legislative act, which meets a standard of clarity and precision that is sufficient to ensure that individuals have advance notice of and can foresee its application. Therefore, lawful surveillance can only be carried out under procedures laid down by legislative provisions.
- **Legitimate Aim:** Laws should only permit Communications Surveillance by specified State authorities to achieve a legitimate aim that corresponds to a predominantly important legal interest that is necessary in a democratic society. Any measure must not be applied in a manner that discriminates on the basis of race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.
- **Necessity:** Surveillance laws, regulations, activities, powers, or authorities must be limited to those which are strictly and demonstrably necessary to achieve a legitimate aim. Communications Surveillance must only be conducted when it is the only means of achieving a legitimate aim, or, when there are multiple means, it is the means least likely to infringe upon human rights. The onus of establishing this justification is always on the State.
- **Adequacy:** Any instance of surveillance authorised by law must be appropriate to fulfil the specific Legitimate Aim identified.
- **Proportionality:** Communications surveillance should be regarded as a highly intrusive act that interferes with human rights threatening the foundations of a democratic society. Decisions about Communications Surveillance must consider the sensitivity of the information accessed and the severity of the infringement on human rights and other competing interests.This requires a State, at a minimum, to establish the following to a Competent Judicial Authority, prior to conducting Communications Surveillance for the purposes of enforcing law, protecting national security, or gathering intelligence:

1. there is a high degree of probability that a serious crime or specific threat to a Legitimate Aim has been or will be carried out; and
2. there is a high degree of probability that evidence of relevant and material to such a serious crime or specific threat to a Legitimate Aim would be obtained by accessing the Protected Information sought; and
3. other less invasive techniques have been exhausted or would be futile, such that the techniques used is the least invasive option; and
4. information accessed will be confined to that which is relevant and material to the serious crime or specific threat to a Legitimate Aim alleged; and
5. any excess information collected will not be retained, but instead will be promptly destroyed or returned; and
6. information will be accessed only by the specified authority and used only for the purpose and duration for which authorisation was given; and
7. that the surveillance activities requested and techniques proposed do not undermine the essence of the right to privacy or of fundamental freedoms.

- **Competent Judicial Authority:** Determinations related to Communications Surveillance must be made by a competent judicial authority that is impartial and independent. The authority must be:
  1. separate and independent from the authorities conducting Communications Surveillance;
  2. conversant in issues related to and competent to make judicial decisions about the legality of Communications Surveillance, the technologies used and human rights; and
  3. have adequate resources in exercising the functions assigned to them.
- **Due Process:** Due process requires that States respect and guarantee individuals' human rights by ensuring that lawful procedures that govern any interference with human rights are properly enumerated in law, consistently practiced, and available to the general public. Specifically, in the determination on his or her human rights, everyone is entitled to a fair and public hearing within a reasonable time by an

independent, competent and impartial tribunal established by law,10 except in cases of emergency when there is imminent risk of danger to human life. In such instances, retroactive authorisation must be sought within a reasonably practicable time period. Mere risk of flight or destruction of evidence shall never be considered as sufficient to justify retroactive authorisation.

- **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:
  1. Notification would seriously jeopardize the purpose for which the Communications Surveillance is authorised, or there is an imminent risk of danger to human life; and
  2. Authorisation to delay notification is granted by a Competent Judicial Authority; and
  3. 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.
- **Transparency:** States should be transparent about the use and scope of Communications Surveillance laws, regulations, activities, powers, or authorities. They should publish, at a minimum, aggregate information on the specific number of requests approved and rejected, a disaggregation of the requests by service provider and by investigation authority, type, and purpose, and the specific number of individuals affected by each. States should provide individuals with sufficient information to enable them to fully comprehend the scope, nature, and application of the laws permitting Communications Surveillance. States should not interfere with service providers in their efforts to publish the procedures they apply when assessing and complying with State requests for Communications Surveillance, adhere to those procedures, and publish records of State requests for Communications Surveillance.

- **Public Oversight:** States should establish independent oversight mechanisms to ensure transparency and accountability of Communications Surveillance.11 Oversight mechanisms should have the authority to access all potentially relevant information about State actions, including, where appropriate, access to secret or classified information; to assess whether the State is making legitimate use of its lawful capabilities; to evaluate whether the State has been comprehensively and accurately publishing information about the use and scope of Communications Surveillance techniques and powers in accordance with its Transparency obligations; to publish periodic reports and other information relevant to Communications Surveillance; and to make public determinations as to the lawfulness of those actions, including the extent to which they comply with these Principles. Independent oversight mechanisms should be established in addition to any oversight already provided through another branch of government.Integrity of Communications and Systems: In order to ensure the integrity, security and privacy of communications systems, and in recognition of the fact that compromising security for State purposes almost always compromises security more generally, the policies should not compel service providers or hardware or software vendors to build surveillance or monitoring capabilities into their systems, or to collect or retain particular information purely for surveillance purposes.
- **International Co-operation:** In response to changes in the flows of information, and in communications technologies and services, States may need to seek assistance from foreign service providers and States. Accordingly, the mutual legal assistance treaties (MLATs) and other agreements entered into by States should ensure that, where the laws of more than one state could apply to Communications Surveillance, the available standard with the higher level of protection for individuals is applied. Where States seek assistance for law enforcement purposes, the principle of dual criminality should be applied. States may not use mutual legal assistance processes and foreign requests for Protected Information to circumvent domestic legal restrictions on Communications Surveillance. Mutual legal assistance processes and

other agreements should be clearly documented, publicly available, and subject to guarantees of procedural fairness.

- **Safeguards against Illegitimate Access:** States should enact legislation criminalising illegal Communications Surveillance by public or private actors. The law should provide sufficient and significant civil and criminal penalties, protections for whistleblowers, and avenues for redress by those affected. Laws should stipulate that any information obtained in a manner that is inconsistent with these principles is inadmissible as evidence or otherwise not considered in any proceeding, as is any evidence derivative of such information. States should also enact laws providing that, after material obtained through Communications Surveillance has been used for the purpose for which information was given, the material must not be retained, but instead be destroyed or returned to those affected."[32]

4.12 What are the measures that can be considered in order to address the potential issues arising from cross border flow of information and jurisdictional challenges in the digital ecosystem?

Cross-border flow of information has important benefits that include, but are not limited to:

- Business activities such as monitoring supply chains, tracking of delivery and pick-up of goods in real time: all of this requires the free-flow of locations, customer information and other related data, which can be difficult depending on the laws prevalent in the country of operation.
- With regard to innovation and progressive technology, the flow of data across borders is imperative. Without access to information and big data spanning over a large number of countries, the effectiveness of new technology and innovative standards will stagnate, or at the very least, slow down.

[32] https://necessaryandproportionate.org/about

Law Enforcement Access

With respect to law enforcement, the cross-border flow of information can prove vital as there are many cases that circumvent domestic authorities, and require information about possible threats from other countries that may possess a repository of relevant knowledge. The concept of mutual legal assistance treaties (MLATs) are bilateral agreements that enable sharing of information between law enforcement agencies and governments, but are considered to operate slowly due to bureaucratic hurdles. CIS recognizes that there is a need to reform the MLAT process so that law enforcement agencies are not unreasonably thwarted by delays in cross border data transfer. As a baseline, CIS recommends that MLATs be formulated in accordance with the principle of "Safeguards for International Cooperation", as mentioned above. Accordingly, the mutual legal assistance treaties (MLATs) and other agreements entered into by States should ensure that, where the laws of more than one state could apply to communications surveillance, the available standard with the higher level of protection for individuals is applied. Where States seek assistance for law enforcement purposes, the principle of dual criminality should be applied. States may not use mutual legal assistance processes and foreign requests for protected information to circumvent domestic legal restrictions on communications surveillance. Mutual legal assistance processes and other agreements should be clearly documented, publicly available, and subject to guarantees for procedural fairness.

Interoperability between Legal Regimes

There is a need for interoperability to be introduced between jurisdictions by way of trade agreements that bridge the gaps between data protection policies across nations. The possibility of achieving harmonization of privacy and data protection policies between nations may not always be feasible, but, if interoperability is achieved, then the global community can aim for shared principles that exist within different privacy systems – thereby, promoting mutual acceptance of privacy norms but also ensuring that 'data protection flows

with the data, wherever it is stored.'[33] There are various mechanisms such as model contracts, data adequacy, safe harbor and binding corporate rules which need to be explored for interoperability between different jurisdictions and facilitating trade while also preserving privacy.

Need for a Data Protection Authority

Globally, cross border data flows are facilitated and governed through dialogue between data protection authorities. Data protection authorities can enter into bilateral or multilateral arrangements with the DPAs of other jurisdictions to co-operate in the implementation of privacy laws. Such arrangements facilitate trade in services by ensuring regional or international consistency. The existence of a DPA allows participation in and leveraging networks such as the Global Privacy Enforcement Network.

[33]Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost? - Nigel Cory. https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost