mozilla

November 6, 2017

To:
Shri RS Sharma
Chairman, Telecom Regulatory Authority of India

Shri Arvind Kumar
Advisor (BB&PA), Telecom Regulatory Authority of India

RE: Mozilla comments on the Telecom Regulatory Authority of India's consultation paper on Privacy, Security, and Ownership of the Data in the Telecom Sector

Dear Sirs,

Thank you for the opportunity to provide comment on the important topic of privacy, security, and ownership of data. We have long argued that the enactment of a baseline data protection law should be a national policy priority for India, and we welcome your thoughtful and thorough analysis of these issues in this consultation paper. The Supreme Court of India's recent landmark ruling on the right to privacy and the ongoing debate around the Aadhaar highlight the need for policymaking in this arena.

Mozilla is a global community of technologists, thinkers and builders -- including thousands in India -- working together to keep the internet open, accessible, and secure. We are the creators of Firefox, an open source browser that hundreds of millions of people around the world use as their window to the web. To fulfill the mission of keeping the web open and accessible to all, we are constantly investing in the security of our products and the privacy of our users.

Our commitment to user security and privacy can be seen both in the open source code of our products as well as in our policies. Consider, for example, Mozilla's Data Privacy Principles,[1] which guide the development of our products and services:

1. **No surprises**
   Use and share information in a way that is transparent and benefits the user.

2. **User Control**
   Develop products and advocate for best practices that put users in control of their data and online experiences.

3. **Limited data**
   Collect what we need, de-identify where we can and delete when no longer necessary.

4. **Sensible settings**

[1] https://www.mozilla.org/en-US/privacy/principles/
[2] https://blog.mozilla.org/netpolicy/files/2016/07/Mozilla-Submissions-TRAI-Consultation-on-Cloud-

Design for a thoughtful balance of safety and user experience.

5. **Defense in depth**
   Maintain multi-layered security controls and practices, many of which are publicly verifiable.

We have answered the consultation paper's questions in detail below, and we remain at your disposal for any further information or clarification on any of these points. We look forward to working with TRAI throughout this critical process.

Q.1 Are the data protection requirements currently applicable to all the players in the eco-system 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?

As we have articulated in the past,[2] we believe that data protection is well served when it rests upon a comprehensive framework rather than solely technology or sector specific regulations. Given due respect and consideration to differences in products and business models, we believe that a purely technology or sector specific approach risks inconsistent law and could obscure the path forward for new technology. Moreover, all actors, both public and private, need to provide for user privacy and choice, and technology and sector specific regulations risk the potential for gaps in protection and oversight. Adopting general standards also has the added benefit of providing a more future-proof approach, allowing new companies and entrepreneurs to understand and apply these standards as new technologies develop.

We note that while India has many laws and regulations that speak to the responsibilities of various actors in the Indian ecosystem to protect user privacy including the Telegraph Act, the IT Act, the IT Rules, and the Unified License, these are fairly high level provisions that do not amount to comprehensive data protection requirements. While these provisions provide a good normative basis to build from, further articulation of data protection rules and requirements is needed in order for users to be meaningfully protected. As we have urged on several occasions in filings submitted to TRAI, enacting a comprehensive data protection law should be a national policy priority.

In establishing new measures to ensure adequate data protection, we would recommend TRAI and the Government of India build from the recommendations[3] developed by the honorable Group of Experts headed by the learned Justice A.P. Shah, former Chief Justice of the Delhi High Court. As this consultation paper notes, these recommendations include the following National Level Principles:

1. ***Notice:*** *A data controller, which refers to any organization that determines the purposes and means of processing the personal information of users, shall give simple to understand notice of its information practices to all individuals, in clear and concise language, before any personal information is collected from them. Such notices should include disclosures on what personal information is being collected; purpose for collection and its use; whether it will be disclosed to third parties; notification in case of data breach, etc.*

2. ***Choice and consent:*** *A data controller shall give individuals choices (opt-in/opt-out) with regard to providing their personal information, and take individual consent only after providing notice of its information practices.*

[2] https://blog.mozilla.org/netpolicy/files/2016/07/Mozilla-Submissions-TRAI-Consultation-on-Cloud-Computing.pdf
[3] http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf

3. ***Collection limitation:*** *A data controller shall only collect personal information from data subjects as is necessary for the purposes identified for such collection.*

4. ***Purpose limitation:*** *Personal data collected and processed by data controllers should be adequate and relevant to the purposes for which they are processed.*

5. ***Access and correction:*** *Individuals shall have access to personal information about them held by a data controller and be able to seek correction, amendments, or deletion of such information, where it is inaccurate.*

6. ***Disclosure of Information:*** *A data controller shall only disclose personal information to third parties after providing notice and seeking informed consent from the individual for such disclosure.*

7. ***Security:*** *A data controller shall secure personal information using reasonable security safeguards against loss, unauthorised access or use and destruction.*

8. ***Openness****: A data controller shall take all necessary steps to implement practices, procedures, policies and systems in a manner proportional to the scale, scope, and sensitivity to the data they collect, in order to ensure compliance with the privacy principles, information regarding which shall be made in an intelligible form, using clear and plain language, available to all individuals.*

9. ***Accountability****: The data controller shall be accountable for complying with measures which give effect to the privacy principles. Such measures should include mechanisms to implement privacy policies, including training and education, audits, etc.*

While these principles provide a strong foundation, we respectfully recommend that inclusion of a few additional provisions in order to foster a strong data protection framework.

1. **Data breach notification** -- Data breaches represent a visceral loss of control of users over their data and a violation of the expectations that they have when they entrust their data to a third party. When affected users are not informed about data breaches, they are at an increased risk of abuse and attack as they don't know to take action to mitigate the threats to their privacy and security. We would recommend that there should be a requirement to promptly notify users and the data protection authority and/or other appropriate regulatory body after any breach that impacts the privacy of data subjects.

2. **Enforcement and oversight** -- We believe that a strong data protection framework requires a strong enforcement framework. To this end, we would recommend the creation of an empowered and resourced data protection authority (DPA)[4] with the following responsibilities:

    - Trainings, education, and other capacity building efforts with relevant actors in the Indian ecosystem to ensure adequate data protection.
    - Oversight of compliance with data protection requirements.
    - Oversight and, at times, provision of redress and remedy for users whose privacy and security have been violated.
    - Investigations and punitive measures to create the appropriate incentives to abide by the data protection framework.

[4] We recommend throughout this consultation the creation of an independent and well resourced Data Protection Authority (DPA). We note, however, that given the substantial size of India, it may also bbe necessary to create a DPA in each state.

It is critical that the DPA be independent from government and have sufficient resources to fulfill these responsibilities.

3. **Right to object --** A right to object to having one's data processed is a protection enshrined in many data protection laws around the world. As data profiling and big data analytics becomes ever more prolific, often without the full knowledge or consent of the user, a right to object is critical to ensuring that users remain in control of their data.

4. **Data portability** -- Users should have the right to take their data from one service and bring it to another service provider, and generally to make use of it for their own benefit and interest. In addition to ensuring that the user remains in control of their data, this right also helps to foster competition in the digital ecosystem.

5. **Privacy by design**[5] -- Ensuring that privacy is part of the design of processes, products, and services -- and not tacked on at the end -- will ensure more seamless integration of these data protection principles into the Indian ecosystem. Moreover, in a country with low levels of literacy and digital literacy, it is especially important that the privacy, security, and dignity of these citizens are protected as part of the engineering of products and systems.

Q. 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?

Definition of personal data
The IT Rules of 2011 enacted pursuant to Section 43A of the IT Act provide strong definitions of "personal information" and "sensitive personal data or information."

> *"Personal information" means any information that relates to a natural person, which can be used, either directly or indirectly for identifying such person. "Sensitive personal data or information" is defined to be a sub-category of this information.*
>
> *"Sensitive personal data or information" is defined to be a sub-category of this information, including information relating to:*
> *(i) password;*
> *(ii) financial information such as Bank account or credit card or debit card or other payment instrument details;*
> *(iii) physical, physiological and mental health condition;*
> *(iv) sexual orientation;*
> *(v) medical records and history;*
> *(vi) Biometric information;*
> *(vii) any detail relating to the above clauses as provided to body corporate for providing service; and*
> *(viii) any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise.*

[5] https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pd

We see great value in using these definitions which are already codified in law as the basis for a forthcoming data protection framework. However, we would also commend for your attention and consideration two other international examples of how personal data could be defined. We note that these examples have robust international backing and foundation in international law, and could help to enrich the legal definitions already found in Indian law.

First, the EU's General Data Protection Regulation (GDPR)[6] definition of personal data, which is particularly valuable for its detailed articulation of indirect identification (which is increasingly possible through big data analysis).

> *"'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); **an identifiable natural person is one who can be identified, directly or indirectly**, in particular **by reference to an Identifier** such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;" (emphasis added)*

Second, the International Principles on the Application of Human Rights to Communications Surveillance[7] -- also known as the Necessary and Proportionate Principles -- contain a definition of "protected information." These Principles have been endorsed by more than 400 international civil society organizations, and Navi Pillay, the former UN High Commissioner for Human Rights has stated in her landmark report *The Right to Privacy in the Digital Age*[8] that they can be considered persuasive interpretive guidance of Article 12 of the International Covenant on Civil and Political Rights (ICCPR) which India is a signatory to.

> *"Protected Information" is information that includes, reflects, arises from, or is about a person's communications and that is not readily available and easily accessible to the general public. Traditionally, the invasiveness of Communications Surveillance has been evaluated on the basis of artificial and formalistic categories. Existing legal frameworks distinguish between "content" or "non-content," "subscriber information" or "metadata," stored data or in transit data, data held in the home or in the possession of a third party service provider.[9] However, these distinctions are no longer appropriate for measuring the degree of the intrusion that Communications Surveillance makes into individuals' private lives and associations. While it has long been agreed that communications content deserves significant protection in law because of its capability to reveal sensitive information, it is now clear that other information arising from communications – metadata and other forms of non-content data – may reveal even more about an individual than the content itself, and thus deserves equivalent protection. Today, each of these types of information might, taken alone or analysed collectively, reveal a person's identity, behaviour, associations, physical or medical conditions, race, color, sexual orientation, national origins, or viewpoints; or enable the mapping of the person's location, movements or interactions*

---

[6] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&qid=1490179745294&from=en
[7] https://necessaryandproportionate.org/
[8] http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf
[9] "People disclose the phone numbers that they dial or text to their cellular providers, the URLS that they visit and the e-mail addresses with which they correspond to their Internet service providers, and the books, groceries and medications they purchase to online retailers . . . I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection." United States v. Jones, 565 U.S. ___, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring).

over time,[10] or of all people in a given location, including around a public demonstration or other political event. As a result, all Protected Information should be given the highest protection in law.

Consent

In regards to the question of consent, users should generally have to give explicit, informed, affirmative consent for their personal data to be used/processed/etc. This is manifested in the GDPR for example as: "consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her..."

It is important to see consent as the beginning and not the end of data protection. Consent is one of the first links of a security chain that includes, but is not limited to, additional links like privacy by design, storing and transmitting data securely, collection and purpose limitation, oversight by the data protection authority, data breach notification, etc. Of course, if the link of consent is weak or broken, the integrity of the rest of the chain is compromised.

Consent must also be meaningful. The example of the EU's "cookie banners" is illustrative. As part of the 2002/58/EC Electronic Privacy Directive update in 2009 in the EU, all websites in Europe have had to implement a notice to users that their site uses cookies. While implementation varies significantly from Member State to Member State, these notices regrettably do not deliver the promise of control, transparency, and choice as per the spirit and intent of the e-Privacy framework. Rather, the user "consents" by clicking on the banner, or in some implementations, consent is interpreted by scrolling down the page, but they do not have a meaningful choice in the case they object to the data collection processes, nor do they have real information about how many parties can access their data and for what purposes. Users must be given a real choice, and should not be forced into a "take it or leave it" approach where their only option is to accept a given service or site's terms of not use it at all.

Information to the user

Privacy notices can be a powerful tool to communicate to users how their data will be processed, stored, accessed, etc, but it is imperative that they be written in clear, accessible language. This privacy notice should also be provided in each language that the service is offered. So if a service is offered in Gujarati, for example, all notices, terms of service, etc should be offered and legally binding in Gujarati, not just English or Hindi.

Consideration of mobile communications

It is also important for a data protection framework to specify when consent must be obtained, and what types of data processing actions require consent once versus at every instance of access, storage, or processing. This is important as some types of data (e.g., communications data and data stored on the user's device) are especially sensitive, and warrant a higher level of user control and consent. For particularly sensitive information, we would recommend that the user's consent be obtained every time such information is processed. Data processing actions should be permitted with (1) the consent of the data subject or (2) when it is necessary for the provision a service. Examples of the latter exemption include:

[10] "Short-term monitoring of a person's movements on public streets accords with expectations of privacy" but "the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy." United States v. Jones, 565 U.S. ___, 132 S. Ct. 945, 964 (2012) (Alito, J. concurring).

- *Security:* This includes scanning, filtering, and ultimately processing both communication content and metadata for the detection and prevention of malware, phishing, and spam, other forms of abuse of networks, services and users.
- *Filtering out illegal or unacceptable content:* that would include automated tools deployed by services providers used to identify illegal content, such as child exploitation imagery.
- *Product features:* those that are not possible without access to the communications content itself, such as translators, group video callings, message syncing across devices, or assistive technologies that automatically copy hotel reservations, travel itineraries, and so forth.

Grounds for processing
While seeking and obtaining user consent is generally considered the preferred basis for processing data, other jurisdictions have recognized the need for data processing on alternative grounds. For example, we would commend for TRAI's attention here too the provisions of the GDPR, which allows for data processing on six grounds:

1. The data subject has consented
2. Processing is necessary for performance of contract[11]
3. Compliance with a legal obligation
4. To protect vital interests of the data subject or other persons
5. For a task carried out in the public interest
6. The legitimate interest of the controller

A note on "legitimate interest"
We note that while the concept of "legitimate interest" can be used to process data in a way that does not pose substantial risks to the user, companies and governments can also easily abuse this concept. A frequent justification for legitimate interest is to allow for innovation and testing of new products and services. While innovation and testing of new products are important, we believe there are other ways to protect these activities without putting the privacy at users at risk with such an open-ended exemption. For example, when Mozilla seeks to conduct research or test browser features that might reveal sensitive information about users, we utilize several experimentation platforms that require users to opt into tests. For example, users can join the *Test Pilot* program,[12] which will install new add-ons with additional browser features. Those add-ons will often provide Mozilla with additional data to understand users' experience with new features. Alternatively, Mozilla also conducts opt-out tests of new features in cases that represent minimal privacy risk to users and where measuring interactions with new features allows us to improve the product for users.

We respectfully recommend that legitimate interest either not be included in any forthcoming regulation or that strict safeguards are enacted in order to ensure that legitimate interest does not become a loophole that renders data protection meaningless.

Q.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.

In keeping with the fundamental right to privacy guaranteed by the Indian Constitution as recognized recently by the Supreme Court of India, the rights of the individual over his/her personal data must be

[11] We note that in the EU context, Terms of Service, which can typically be changed arbitrarily and unilaterally by the service provider, are not considered a contract for this purpose.
[12] https://testpilot.firefox.com/experiments/

treated as paramount. As discussed above, at no time should the rights of the data controller be able to supersede the rights of the individual over his or her personal data.

To realize this right in practice, we respectfully recommend there must be several responsibilities and obligations placed on data controllers and codified in law, including:

1. Offering users meaningful notice, choice, and consent mechanisms
2. Collection and purpose limitation
3. Facilitation of access, correction, and the right to object
4. Security and role based access control and protections against unlawful disclosure
5. Training of employees and contractors

These recommendations are consistent with the Principles developed by the honorable Group of Experts headed by the learned Justice A.P. Shah, former Chief Justice of the Delhi High Court as well as the EU's GDPR.

We would further recommend that at all times, data controllers must be able to demonstrate that any data processing has been done in compliance with the data protection framework. Practically, this should include taking appropriate technical and organizational measures, publishing policies, and ensuring adequate documentation of all data processing decisions and actions, all of which can and should be reviewed by the data protection authority or other appropriate regulatory body. We reiterate here our strong recommendation that an empowered and independent data protection authority should be created for the purposes of regulation, training, oversight, and enforcement pursuant to the data protection framework.

Q. 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?

Given significant differences in business models, products/services, data collection practices, and the complexity of algorithms in use today, a singular technology enabled architecture to audit the use of personal data for all actors in the digital ecosystem seems infeasible to impossible.

While a strong DPA should be established and should have the power to audit the practices of data controllers, whether they are public or private entities, the creation of a workforce of auditors seems inadvisable.

Consider, for example, the role of credit agencies in the global financial crisis of 2007-2010. Credit agencies are supposed to be neutral, independent third parties who rate the riskiness of debt instruments and securities. Yet, the structured finance, collateralized debt obligations, and other complex financial instruments that underpinned the subprime mortgage crisis in the United States would not have been possible without the credit agencies. The Financial Crisis Inquiry Commission (FCIC) set up by the US Congress and President to investigate the causes of the crisis found in their report that the "failures" of the Big Three rating agencies were "essential cogs in the wheel of financial destruction" and "key enablers of the financial meltdown."[13] Credit agency Standard & Poor's, the world's largest credit agency paid a fine

[13] https://www.gpo.gov/fdsys/pkg/GPO-FCIC/pdf/GPO-FCIC.pdf

of $1.375 billion for its role;[14] Moody's, the second largest rating agency, paid $864 million to settle with US federal and state authorities over its ratings.[15]

This should serve as a cautionary tale on the wisdom of relying so heavily on third parties to investigate complex systems and algorithms, whether in the realm of structured finance or technology products and services. While audits can certainly be useful tools in enforcing data protection requirements, they are not a substitute for actually empowering users with transparency, choice, and consent or a properly resourced, independent regulator.

As an alternative, we would respectfully recommend:

- The creation of an empowered and independent data protection authority.
- Strong documentation requirements around data processing, access, use, and storage actions in order to assist the data protection authority and other relevant regulatory bodies in the fulfillment of their mandates.
- Reporting obligations (e.g., for changes in rules, processes, or in the instance of a data breach).
- Capacity for dialogue with and determinations from DPA on pre-market entry or new products/features.

Finally, we would recommend that given the incredible sensitivity and intimate nature of biometric data, the data protection authority should be notified before market entry of any and all products, services, and features that collect, store, process, or use biometric data.

Q. 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?

Consistent with the fundamental right to privacy, data processing should only occur on the basis of the user's consent or the other aforementioned legitimate grounds for processing articulated in our answer to Question 2. The era of big data and the dawn of an age in which all things are connected to the internet and where databases are increasingly linked pose real danger to privacy and data protection.

A data protection framework should spell out the specific requirements for obtaining consent and managing purpose and collection limitation so as to ensure both that new data based businesses are developing their products/services in accordance with the right to privacy and in a way that provides legal clarity to those business wishing to build data based products/services.

Q.6 Should government or its authorized authority setup a data sandbox, which allows the regulated companies to create anonymized data sets which can be used for the development of newer services?

We do not believe this is an appropriate action for government nor is it consistent with the principles developed by Group of Experts chaired by the learned Justice A.P. Shah, former Chief Justice of the Delhi High Court. For example, it is difficult to reconcile the notion of a data sandbox with the concepts of notice, choice, consent, purpose limitation, collection limitation, or right to object. As such, a data sandbox would represent a violation of data protection standards and the right to privacy. Furthermore, we are deeply skeptical that such a data set could be sufficiently anonymized. There is increasing research demonstrating the strong potential for reidentification, especially when databases are combined.

[14] https://www.theguardian.com/business/2017/jan/14/moodys-864m-penalty-for-ratings-in-run-up-to-2008-financial-crisis
[15] ibid.

Q. 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?

We are skeptical that there is a single technology solution for monitoring compliance with data protection. As we have articulated above, data protection relies on a chain of integrated actions and responsibilities. However, robust documentation around data processing, storage, access, and use is a critical component of any strong data protection framework. In that regard, we can envision a system to consolidate this documentation enabling more effective and efficient oversight by the data protection authority and other relevant regulatory bodies. Given the sensitivity of the information that would be contained in such a system, we would strongly recommend strict data security requirements, including encryption, role-based access control, multifactor authentication, etc.

We would further add that no technology solution can be a substitute for regular and robust interaction between the data protection authority and data controllers. This should also be supplemented with regular multistakeholder dialogues on data protection, which are critical to ensuring that public interest organizations and technical experts can assist in the implementation and enforcement of the data protection framework.

Q. 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?

Strong security standards, including obligations to use encryption, role-based access control, and multifactor authentication are critical to ensuring the safety and security of telecommunications infrastructure and the digital ecosystem as a whole. We would recommend that TRAI work in concert with the data protection authority and other relevant regulatory bodies to regularly publish guidance on how best to secure infrastructure and users.

We would also commend for your attention the issue of government vulnerability disclosure. Vulnerabilities are at the heart of many hacks, attacks, and breaches, and the government is often in a unique position of knowledge about vulnerabilities in the digital ecosystem. Governments learn about vulnerabilities through their own research and development, by purchasing them, through intelligence work, or by reports from third parties. Disclosing these vulnerabilities to affected companies allows companies to:

- patch them quickly;
- increase the security, privacy, and safety of their systems and users;
- reduce conflict and improve trust between companies and government; and,
- especially for organizations with limited cybersecurity resources, benefit from external discovery of vulnerabilities in their products and systems that they may not otherwise have the resources to find.

In the interest of making users and infrastructure in the digital ecosystem as secure as possible, it is critical that the Government of India develop a robust, accountable, and transparent process for reviewing and coordinating the disclosure of vulnerabilities to affected companies.

Due to the serious security and policy implications of vulnerability disclosure processes, we recommend that these policies be institutionalized and the participants, standards, timeframes, and accountability mechanisms be explicitly defined and made public so that companies and consumers can have trust in

government disclosure decisions. More specifically, we recommend that the Government of India develop policies around vulnerability disclosure that include the following norms and practices:

- Ensure all vulnerabilities go through the process, and create and publicly communicate timelines to direct how quickly a vulnerability must be submitted to the review process and how long a vulnerability may be held before it is subject to disclosure or an additional review.
- Require and facilitate the participation of all relevant governmental agencies, and publicly clarify which agencies regularly participate in determinations and what criteria guide their decision-making.
- Require independent and transparent post-hoc oversight of the process to ensure that on the whole, disclosure decisions are balancing equities properly. Accountability will be further enhanced by public reporting.
- The process should be housed in a civilian agency with sufficient expertise, infrastructure, and trust in the community to appropriately coordinate disclosure.
- The process should be codified in law where possible to ensure that the policy decisions of this magnitude are made in part by legislative bodies, understood by the public, and not subject to revision behind closed doors.

Q. 9 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?

As we articulate in our answer to Question 1 of this consultation, we believe there are significant risks to taking a sector-by-sector approach to data protection. To this end, we strongly recommend that the data protection obligations and responsibilities that we have articulated above should apply to all actors.

Q. 10 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?

As we articulated in our answer to the previous question, we believe that data protection requirements should apply to all actors. However, this should not be interpreted as a recommendation that TSPs and OTTs should be treated in the same way from a licensing perspective. As we wrote in our response to TRAI's Cloud Computing Consultation Paper,[16] licensing requirements must not be used as a way to impose access requirements for law enforcement and government retention for data stored by OTTs. Any mandatory licensing scheme would likely prove onerous and would increase the costs of creating online, thereby discouraging Indian entrepreneurs from building the next internet giant. The Department of Telecommunication rightfully concluded in 2015 that licensing requirements for OTTs were not warranted,[17] and we respectfully recommend that TRAI should likewise conclude the same here.

Q. 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,

[16] https://blog.mozilla.org/netpolicy/files/2016/07/Mozilla-Submissions-TRAI-Consultation-on-Cloud-Computing.pdf

[17] Net Neutrality DoT Committee Report, Department of Telecommunications (May 2015), http://www.dot.gov.in/sites/default/files/u10/Net_Neutrality_Committee_report%20%281%29.pdf.

what are the checks and balances that need to be considered in the context of lawful surveillance and law enforcement requirements?

According to international human rights law, all surveillance constitutes an interference with the right to privacy. The question, which protections and procedures outlined in law help to answer, is whether the interference is justified. This is often expressed as tests of necessity, proportionality, legitimacy, etc. which in turn give rise to requirements for *inter alia* procedural safeguards and that the authority and purpose for violating an individual's privacy be established in law. The learned Justice Sanjay Kishan Kaul, J of the Supreme Court of India in his concurring opinion in *Puttaswamy and Another vs. Union of India and Others* includes a test for the "Principle of Proportionality and Legitimacy"

> *"Test: Principle of Proportionality and Legitimacy*
> *71. The concerns expressed on behalf of the petitioners arising from the possibility of the State infringing the right to privacy can be met by the test suggested for limiting the discretion of the State:*
> *(i) The action must be sanctioned by law;*
> *(ii) The proposed action must be necessary in a democratic society for a legitimate aim;*
> *(iii) The extent of such interference must be proportionate to the need for such interference;*
> *(iv) There must be procedural guarantees against abuse of such interference."*

Elsewhere, in Justice R.F. Nariman, J's concurring opinion of the same case, he cites the International Principles on the Application of Human Rights to Communications Surveillance[18] (also known as the Necessary and Proportionate Principles), which we would particularly commend for your attention. In summary, the Necessary & Proportionate Principles are:

> **LEGALITY**
> Any limitation on the right to privacy must be prescribed by law.
>
> **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.
>
> **NECESSITY**
> Laws permitting Communications Surveillance by the State must limit surveillance to that which is strictly and demonstrably necessary to achieve a Legitimate Aim.
>
> **ADEQUACY**
> Any instance of Communications Surveillance authorised by law must be appropriate to fulfill the specific Legitimate Aim identified and effective in doing so.
>
> **PROPORTIONALITY**
> 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.
>
> **COMPETENT JUDICIAL AUTHORITY**
> Determinations related to Communications Surveillance must be made by a competent judicial authority that is impartial and independent.

[18] https://necessaryandproportionate.org/principles

DUE PROCESS
States must 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.

USER NOTIFICATION
Individuals 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.

TRANSPARENCY
States should be transparent about the use and scope of Communications Surveillance laws, regulations, activities, powers, or authorities.

PUBLIC OVERSIGHT
States should establish independent oversight mechanisms to ensure transparency and accountability of Communications Surveillance.

INTEGRITY OF COMMUNICATIONS AND SYSTEMS
States 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 State Communications Surveillance purposes.

SAFEGUARDS FOR INTERNATIONAL COOPERATION
Mutual Legal Assistance Treaties (MLATs) 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 should apply.

SAFEGUARDS AGAINST ILLEGITIMATE ACCESS
States should enact legislation criminalising illegal Communications Surveillance by public and private actors.

What these tests and principles further make clear is that a blanket exception to data protection requirements for such broad and ambiguous notions of "national security" and "public order" should not be permitted and is inconsistent with the right to privacy as a fundamental constitutional guarantee under both the Indian Constitution and the International Covenant on Civil and Political Rights.

Finally, even surveillance activities that are legitimate can still harm user trust, safety and security. We further propose that the Government of India adopt the following basic principles to guide the scope of their surveillance activities, balancing their legitimate needs with the broader good:

User Security: Governments need to strengthen user security, including encryption, not weaken it.
Encryption is critical to protecting user security. Requirements to weaken encryption make it easier for bad actors to attack the technology we all depend on, exposing users to financial, physical, and other harms.

Minimal Impact: Government surveillance should minimize impact on user trust and security.

Governments should collect only the information that is needed and, whenever possible, only data about specific, identifiable users. Governments should avoid compromising systems and such actions should be viewed as unacceptable if other options for obtaining information are available.

Accountability: Surveillance activities need empowered, independent, and transparent oversight.
Oversight bodies should be independent of surveilling agencies, with broad mandates, enforcement authority, and transparent processes. They should have technical expertise and assess both the demonstrable national security benefits and the potential harms of the surveillance.

Q.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?

Data localization
At the outset, we would respectfully recommend that the honourable members of TRAI and other stakeholders considering legislation and regulation around data protection to more specifically define the challenges posed by cross border flow of information and the jurisdictional challenges in the digital ecosystem. While having data stored in other jurisdictions can certainly pose a challenge to law enforcement investigations in some cases, the free flow of information increases the efficiency of internet traffic delivery, lowers costs, reduces barriers to innovation, and ensures that users can access the full diversity of the open internet.

Data localization policies that mandate national borders for data or introduce new restrictions on data portability present a major threat toward the growth of the internet and internet-based services by introducing high costs and actual limitations on technology innovation, development, and use. Instead of imposing unnecessary legal barriers, TRAI should support further study of the harmful impact of such policies and the benefits of advancing open information flow across jurisdictions.

As we argued in our submission to TRAI's Cloud Computing Consultation[19]:

> *"A mandate to route traffic through data centers within the borders of India would massively disrupt the efficient and effective flow of Internet traffic, contravening the mandate of TRAI to ensure the orderly growth of the Internet and the telecommunications sector. Efficient Internet routing depends on the network's end-to-end design and dynamic transfer of packets of data. Routing protocols are designed to ensure that these packets travel along the most efficient route between two points. Limiting the routes data can travel ultimately undermines the efficiency and potentially the integrity of Internet traffic. Requirements to store data in India or segregate certain types of data may present a prohibitively difficult and expensive barrier to startups, hurting innovation, limiting entrepreneurship, and undermining the promise of Digital India."*

Finally, any move to require data to be located in India would not only set a dangerous example for other countries, but also other countries would likely reciprocate in kind, requiring Indian companies to store data in their jurisdictional borders, which would represent a heavy burden on Indian industry and limit the efficacy of the Digital India and Made in India initiatives.

MLATs

[19] https://blog.mozilla.org/netpolicy/files/2016/07/Mozilla-Submissions-TRAI-Consultation-on-Cloud-Computing.pdf

We would respectfully suggest that it would be more productive to focus on reforming the Mutual Legal Assistance Treaties (MLATs) that India is a party to. MLATs are well established tools allowing for the cross-border transfer of data and other forms of collaboration between governments and investigative authorities with built in protections for users. At the same time, the MLATs today often do not function expeditiously and struggle to cope with the speed of data transfer in the digital age. There are several reforms that could be undertaken that could improve the efficiency and effectiveness of the MLAT system. For example:

- Authenticating law enforcement requests and court documents, possibly through a centralized system;
- Providing a simple, consistent method for submitting requests online (either centralized or company or country-specific);
- Standardizing the format internationally that the companies will use to turn over evidence; and
- Creating single points of contact within government and companies.

For further analysis on how to reform the MLAT system, we would commend for your attention the analysis on https://MLAT.info developed by the organization AccessNow.

Adequacy and harmonizing with Europe
Cross-border data exchange through MLAT and other cooperation channels will also be facilitated by the introduction of strong data protection standards in India. Governments and companies will be more willing to turn over data in response to legitimate requests if they are confident that there are procedural requirements in place to protect the rights of their citizens and users.

Adopting a high level of data protection, in line with the EU's GDPR or at least sufficiently high as to be granted adequacy status by the EU, could offer several benefits. Indeed, a harmonized or at least substantially similar data protection regime across the EU and India would represent the largest addressable market in the world. This would likely attract talent, companies, and infrastructure investment in India, and would also more easily enable Indian companies looking to go global to easily enter the large European market as well as the several other markets that model their data protection laws after Europe.

Furthermore, adopting different data protection approaches in the EU and India will introduce substantial capital and human resources costs on Indian businesses wishing to go global who will need to build and maintain two systems to comply with these different legal frameworks. This tax on Indian industry will limit development, innovation, and the appeal of starting or operating a company in India.

Conclusion
Following the Supreme Court of India's landmark ruling establishing that privacy is a fundamental right guaranteed by the Indian Constitution, India now has a unique opportunity and obligation to articulate how this right will be protected in law. We urge TRAI, the Government of India, and other stakeholders to work together to enact strong meaningful privacy protections that can be a model to the world.

Respectfully submitted by:

Denelle Dixon
Chief Business and Legal Officer, Mozilla Corporation

Jochai Ben-Avie
Senior Global Policy Manager, Mozilla Corporation