Mozilla San Francisco
2 Harrison Street, Suite 175
San Francisco, CA 94105
United States of America
650.903.0800

January 31, 2018

TO:
Justice Srikrishna and the honourable members of the Ministry of Electronics and Information Technology Committee of Experts

CC:
Shri Rakesh Maheshwari
Scientist G & Group Co-ordinator, Cyber laws
Ministry of Electronics and Information Technology

RE: Mozilla's comments on
the white paper of the Committee of Experts on data protection framework for India

Thank you for the opportunity to provide comment on the important topic of India's first comprehensive data protection law. 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 your report. The Supreme Court of India's recent landmark ruling on the right to privacy and the ongoing debate around the Aadhaar project highlights the need for urgent policymaking in this arena.

We commend you for the strong approach you have outlined in your report, and believe that India has an opportunity to craft a data protection law that can, and will, be a model to the world. Rather than answer all of the many questions posed by your report, we have focused our comments on the areas where we feel protections are missing and where your recommendations can be strengthened based on our experience and expertise advocating for individual security and privacy all over the world.

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, as well as other products including Pocket, Rocket, Focus, Coral, and Thunderbird. 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.

Mozilla San Francisco
2 Harrison Street, Suite 175
San Francisco, CA 94105
United States of America
650.903.0800

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**
> 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 look forward to continuing to engage with you and other stakeholders in the Government of India as work progresses to craft India's historic first data protection law. If you have any questions about our submission or if we can provide any additional information that would be helpful to the Committee as you continue your important work, please do not hesitate to contact Mozilla Senior Global Policy Manager Jochai Ben-Avie at jochai@mozilla.com.

General contours of a data protection law

The approach that you have outlined in this report, drawing strongly on the recommendations[2] developed by the honorable Group of Experts headed by the learned Justice A.P. Shah, former Chief Justice of the Delhi High Court and the European Union's General Data Protection Regulation (GDPR) is a strong one. In our submission[3] to the Telecom Regulatory Authority of India's (TRAI) recent consultation paper on "Privacy, Security, and Ownership of Data in the Telecom Sector"[4] we advocated for just such an approach.

As we have argued in that submission and elsewhere, a strong data protection law requires:

---

[1] https://www.mozilla.org/en-US/privacy/principles/
[2] http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf
[3] https://blog.mozilla.org/netpolicy/files/2017/11/Mozilla-TRAI-Data-Protection-Filing.pdf
[4] http://trai.gov.in/sites/default/files/Consultation_Paper%20_on_Privacy_Security_ownership_of_data_09082017.pdf

Mozilla San Francisco
2 Harrison Street, Suite 175
San Francisco, CA 94105
United States of America
650.903.0800

1. The enshrinement of a robust framework of rights of individuals with meaningful user consent at its core;
2. Strong obligations on data controllers reflecting the significant responsibilities associated with collecting, storing, using, analyzing, and processing user data; and
3. Effective enforcement mechanisms including an empowered, independent, and well-resourced Data Protection Authority (DPA).[5]

Consent

While we were pleased to see the attention that your Committee paid to the concept of consent, we remain deeply concerned about your comment that "consent may not be as relevant" in the context of big data analytics.

We believe consent is and should remain a critical component of how users' private is protected on the web. Some exception to a consent model may be advisable in the cases where data is de-identified or represents little no or private risk; i.e. in cases where the data collected essentially is not personal. Nonetheless, many important analytics services can be used to collect sensitive data or to build sophisticated profiles about users. Those profiles may then be shared or sold to others. When those sensitive profiles are created, and then possibly shared, consent becomes all the more critical. We refer you to the below sections where we elaborate the other legal grounds for processing which can be used in addition to consent.

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.

We commend to your attention recent guidance developed by the Article 29 Working Party (of EU Data Protection Authorities) on the consent obligations of the GDPR.[6] In particular, this paper

[5] We recommend throughout this submission 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 be necessary to create a DPA in each state.

[6] https://iapp.org/media/pdf/resource_center/wp29_consent-12-12-17.pdf

Mozilla San Francisco
2 Harrison Street, Suite 175
San Francisco, CA 94105
United States of America
650.903.0800

elucidates in great detail how to interpret the requirements that consent be "freely given, specific, and informed."

At the same time, the Article 29 Working Party also indicates that data controllers should not overly rely on consent due to the burden it places on the user and the risk of "consent fatigue." Moreover, in instances where there is a substantial imbalance of power between the individual and the data controller, consent may not be meaningful and therefore would be an inappropriate basis for data processing. "for the majority of … data processing at work, the lawful basis cannot and should not be the consent of the employees" as it is unlikely that employees will feel able to freely respond to a request to process, or able to refuse without detriment. Similar to public authorities, however, employers may rely on consent under some "exceptional circumstances." The Article 29 Working Party's guidance on how public authorities can use consent as a basis for processing may be particularly instructive.

Sensitive personal data

List of sensitive personal data

A stricter regime for certain specified categories of data is useful in order to signal to data controllers that a higher level of protection and security will be required given the sensitivity of the information. A well defined list of sensitive personal data codified in law is desirable for the certainty it affords data controllers. However, the classification of what data is regarded as sensitive may evolve with changing societal norms and technologies. To this end, we would recommend that the DPA be empowered to periodically assess and add to this definition of sensitive personal data, subject to an open consultation process.

The Committee's provisional views mention categories of health information, financial information, genetic information, religious beliefs and affiliations, sexual orientation, racial and ethnic origin. These are not sufficient. Categories such as biometric data, political and philosophical beliefs, criminal convictions and offences and related security matters should be included as well, as the EU does in Article 10 of the GDPR.

In the context of Aadhaar, India's national biometric ID project, the exclusion of biometric data from this list would be particularly worrisome. Biometric systems use the body (e.g., iris scans, fingerprints, face) for identification and in this way directly implicate bodily integrity, a core privacy concern as emphasized by the judges in *Puttaswamy v. Union of India.* The threat of identity theft and unauthorised access is amplified because biometrics cannot simply be regenerated and once breached, it is no longer possible to change these immutable characteristics of an individual. Finally, the breach of biometric data can have severe consequences for individual liberty - such as be used to implicate individuals in criminal process due to the probative value of fingerprints, for example, in crime scenes. In a similar vein, the Aadhaar number itself should also be treated as sensitive personal data given that it links multiple databases and is linked to bank accounts and other sensitive databases.

In addition, location and communications metadata should also be considered sensitive given that it enables a comprehensive mapping of an individual's personal life, including insights about sensitive information, for example, like visits to an HIV clinic or political party offices.

Mozilla San Francisco
2 Harrison Street, Suite 175
San Francisco, CA 94105
United States of America
650.903.0800

Stricter requirements
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, data stored on the user's device, and biometrics) are especially sensitive, and warrant that the user's consent be obtained every time such information is processed.[7]

It should also be illegal to transmit or store any sensitive personal data in an unencrypted form. Likewise, there are many generally accepted security practices such as multi-factor authentication, security audits, and role-based access control which should be required for the processing of sensitive personal data. As the state of security best practice changes, some of these requirements may also periodically need to be updated. As such, we would recommend that the DPA be empowered, subject to a consultation process, to periodically update security guidance for data controllers in accordance with this law.

Finally, as recommended by the Committee, a higher quantum of penalties for breach of sensitive personal data requirements would be warranted.

Right to Access, Rectify, and Object
The Committee emphasizes the importance of a right to seek confirmation, access, and rectify personal data, despite foreseeable enforcement challenges when the data is derived from behavioural analytics. This is a welcome acknowledgment, and recognizes that the context of big data analytics on its own does not merit exemptions to foundational privacy rights. In fact, decisions that have a profound impact on people's lives are increasingly driven by big data analytics. In this context we need more, not less, emphasis on rights that afford users control over their data.

This is why we are concerned with the Committee's parallel observation that the right to object may not be suitable in the Indian context. Similarly, the Committee does not endorse a right to delete. These rights, enshrined in most data protection laws around the world, are integral to

[7] We note, however, that data processing actions necessary for the performance of a service should still be a valid basis for processing even when the data in question is sensitive personal data. Examples of this include:

- *Security:* This includes scanning, filtering, and ultimately processing 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:* This includes automated tools deployed by service providers to identify illegal content, such as child exploitation imagery.
- *Product features:* Consider certain communications product features 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.

Mozilla San Francisco
2 Harrison Street, Suite 175
San Francisco, CA 94105
United States of America
650.903.0800

realising your commitment to informed and meaningful consent. Informed consent should not be viewed as a one time static event. The continuing rights of a user to object to certain kinds of processing and to compel deletion of personal data on the user's request affirms that control of personal data vests with the individual. It prevents processing of data that may be antithetical to his or her autonomy and dignity. As the Article 29 Working Party makes clear in their recent report on the GDPR consent obligations,[8] consent must be freely given, which means that the user must also be freely able to withdraw that consent at any time. Where consent cannot be given or withdrawn freely, consent cannot be used as a lawful basis for data processing. In a similar vein, a prohibition on evaluative decisions taken solely on the basis of automated decisions is desirable to prevent a loss of control and a lack of redress for the user.

Omitting critical rights from the data protection framework like the right to object may also risk India obtaining an adequacy determination from the EU.

Data portability

We commend the Committee's stance on data portability. A right to demand all personal data about the individual in a universally machine readable format or ported to another service provider with the consent of an individual is key to both strengthening user control and the competitiveness of the market for consumer facing services. As one of the world's biggest and oldest open source companies, we have long been a proponent of open standards and interoperability. The Government of India too has long been a champion of open source and open standards, and we're pleased to see that commitment reflected in the provisional views of this report. Interoperability not only gives users more choice over which services they entrust their data to by reducing the barriers of switching, but in doing so, increases healthy competition and reduces the costs to innovation.

Obligations of 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 treated as paramount. 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. Access, correction, deletion, and a right to object
4. Security requirements and protections against unlawful disclosure
5. Training of employees and contractors

These recommendations are consistent with the Principles developed by the honorable Group of

[8] https://iapp.org/media/pdf/resource_center/wp29_consent-12-12-17.pdf

Mozilla San Francisco
2 Harrison Street, Suite 175
San Francisco, CA 94105
United States of America
650.903.0800

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.

Other grounds of processing

While consent is certainly an important basis for data processing, there are many examples where seeking consent in every instance would be overly burdensome. For example, data processing should be permitted when necessary for the performance of a contract. Other jurisdictions have recognized the need for data processing on alternative grounds in their data protection regimes. The provisions of the GDPR, which allows for data processing on six grounds, are instructive:

1. The data subject has consented.
2. Processing is necessary for performance of contract. 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. Moreover, recent guidance from the Article 29 Working Party[9] has clarified that there must be "a direct and objective link" between processing and performance for performance to qualify as a lawful ground for processing.
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, it can also easily be abused by companies. 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 of 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 utilise several experimentation platforms that require users to opt into tests. For example, users can join the Test Pilot program,[10] which

[9] https://iapp.org/media/pdf/resource_center/wp29_consent-12-12-17.pdf
[10] https://testpilot.firefox.com/experiments/

Mozilla San Francisco
2 Harrison Street, Suite 175
San Francisco, CA 94105
United States of America
650.903.0800

will install new addons with additional browser features. Those addons 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.

Given that legitimate interest is a vague concept that can be easily be abused at the expense of user data protection rights and interests, we respectfully recommend that legitimate interest be narrowly and specifically defined if it is included. In particular, it would be beneficial for guidance to be developed -- most likely by the DPA after enactment of the data protection law -- articulating how legitimate interest can be used without overriding the rights of the individual.

Exemptions to data protection requirements

Your Committee's report, as most international data protection regimes, contemplates several exemptions to certain data protection requirements. While we believe that there are several such grounds that should be enshrined in India's forthcoming data protection law as discussed above, we note that consent of the user should certainly be the preferred route in most cases. In *Puttaswamy v. Union of India*, the Supreme Court of India found that privacy as a fundamental right is embedded within the constitutional right to individual liberty. It is difficult to conceptualize of this notion of liberty without endowing in the individual the agency to consent to how their data are collected, stored, and processed. To this end, any exemptions must be limited, strictly construed, in the public interest, and enshrined in law. Moreover, *all* exemptions should be understood as an exemption to seek the user's consent to store, access, analyse, or process user data, *not* as an exemption from all data protection obligations, in particular data minimization, collect limitation, purpose limitation, and data security. All data processing must also be necessary and proportionate. We recommend a careful analysis to ensure that any exemptions are narrowly tailored and describe specific permitted activities.

National security purposes

Notwithstanding the state's compelling interest and obligation to ensure the security of the populace of India, the terms national security and public order must be defined in law and narrowly construed. These terms must not be allowed to be used as a loophole to allow prolific and pervasive violations of the fundamental right to privacy. To that end, any exemptions for the purposes of investigating a crime, apprehending an offender, prosecuting an offender, or for any other purposes related to maintaining national security and public order must be understood as exemptions from seeking user consent, not from all data protection requirements, as noted above. All law enforcement, intelligence, and other national security elements of the State must, for example, still be bound by requirements around data security, purpose limitation, collection limitation, the right to rectify, etc. Given the disproportionate power of the State vis-a-vis the individual, the unparalleled access to private data available to the State, and the substantial interference and invasion into the private lives of individuals that the State is capable of, the authority of the State must be strictly prescribed in law and additional protections for individual security and privacy are required. Exempting entire State agencies from all data protection requirements is wholly untenable and in conflict with the jurisprudence of the Supreme Court of India as well as India's obligations under international law.

Mozilla San Francisco
2 Harrison Street, Suite 175
San Francisco, CA 94105
United States of America
650.903.0800

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 v. Union of India* 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[11] (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

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

Mozilla San Francisco
2 Harrison Street, Suite 175
San Francisco, CA 94105
United States of America
650.903.0800

competing interests.

COMPETENT JUDICIAL AUTHORITY
Determinations related to Communications Surveillance must be made by a competent judicial authority that is impartial and independent.

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 (which India is a party to).

Mozilla San Francisco
2 Harrison Street, Suite 175
San Francisco, CA 94105
United States of America
650.903.0800

Finally, even surveillance activities that are legitimate can still harm user trust, safety, and security. We 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.

Data retention and deletion

Mozilla's position on data retention is summarised in our Data Privacy Principles[12]: *"collect what we need, de-identify where we can and delete when no longer necessary."* As the Committee recognises, storage limitations are intrinsic to goals of purpose and collection limitation. The standard of storing data only for a time period that is reasonably necessary for the purpose for which it was collected, is a sound principle but its adoption must be subject to close monitoring and review. As with other obligations, data controllers must be able to justify their interpretation of and demonstrate compliance with this standard. As the increasing frequency of data breaches make clear, amassing the personal information of everyone in India exposes those data to breach, theft, misuse, and abuse. Data retained are data at risk. In addition to making troves of private user information vulnerable to malicious actors, requiring companies to hold user data longer than necessary for business purposes would create additional liability and risk, and harms trust online.

Any calls for data retention by the state (e.g., for law enforcement or national security purposes) requires strict scrutiny and accountability. Jurisprudence across the world, and particularly in Europe, shows that governments have not been able to credibly demonstrate the necessity or proportionality of data retention mandates. In the *Digital Rights Ireland* decision of the Court of

[12] https://www.mozilla.org/en-US/privacy/principles/

Mozilla San Francisco
2 Harrison Street, Suite 175
San Francisco, CA 94105
United States of America
650.903.0800

Justice of the EU, the court noted that the mere collection of metadata that could identify individuals or reveal insights about them was problematic. It "is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance," the courts said. Finally, a "collect it all" mentality has the practical impact of overwhelming security agencies with more data than they can possibly analyze, which actually limits the intelligence value with high costs on the government and a loss of user privacy and trust online.[13]

Extraterritoriality

In human rights law, including international treaties like the International Covenant on Civil and Political Rights as well as the Indian Constitution, it is understood that rights adhere to individuals and that the State has a compelling interest and obligation in protecting these rights. To that end, it is natural that the Committee would contemplate the extraterritorial applicability of India's forthcoming data protection regime. We would generally recommend that India adopt a GDPR-like model of regulating entities which offer goods or services in India even though they may not have a presence in India.

While we believe that such a regime of extraterritorial application is appropriate for a country of India's considerable size and population, we note that this approach does not scale well. It is not tenable for a company to have to abide by the laws of every country in the world, especially for companies that offer services that do not require direct payment by users. That would effectively kill innovation and limit the provision of services to all but the world's most well-resourced companies.

We further note that the EU regulatory regime also has several mechanisms for countries to obtain a determination that their data protection laws are adequate as well as for companies to certify that they are compliant with relevant data protection requirements, and we strongly encourage India to adopt this approach if a law with extraterritorial application is adopted. If India itself were to obtain an adequacy determination from the EU and enter to reciprocal arrangements with other countries that have deemed to have adequate data protection laws, that would create the largest market in the world, which would offer tangible and immense benefits to India and Indian companies.

Data localization

There is a meaningful distinction to be made between mandatory data localization regimes (which require data to be stored within the borders of a given country unconditionally) and some of the limitations on data transfer found in some data protection laws, including the GDPR.

As noted above, the EU has several mechanisms permitting the transfer of data out of the EU, including adequacy determinations, bilateral agreements like the US-EU Privacy Shield, and consent of the data subject. Recently, Andrus Ansip, EU Vice-President for the Digital Single

[13] http://time.com/3667663/charlie-hebdo-attack-terrorism-intelligence/

Mozilla San Francisco
2 Harrison Street, Suite 175
San Francisco, CA 94105
United States of America
650.903.0800

Market speculated that: "data should be able to flow freely between locations, across borders and within a single data space… "[14]

By way of contrast, 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.

A mandate to route traffic through data centers within the borders of India would massively disrupt the efficient and effective flow of Internet traffic. 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.

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.

Allied laws

As noted by the Committee, a variety of sectoral laws will need to be tested against the new data protection law when it comes into existence. We emphasize that the principles endorsed by this Committee -- informed consent, purpose limitation, data minimization, structured enforcement, etc -- must be enshrined across these laws.

For example, provisions in the Aadhaar Act and its regulations relating to data security policies, the right to access data, and procedures of grievance redress bodies are still wanting in many respects, and will need to be revisited in light of these principles. Other issues such as the choice of opt-out from the Aadhaar database, or procedure for enrolling into the 'biometric exception' will need to be built into the design of the Aadhaar system.

Other laws such as those governing surveillance of communications (such as the Indian Telegraph Act, 1885 and the IT Rules, 2011) will need to be tested against principles such as purpose limitation read with the Supreme Court of India's standard of proportionality laid down in *Puttaswamy v. Union of India*.

[14] https://iapp.org/news/a/talking-free-data-and-the-gdpr-with-commission-vp-andrus-ansip/

Mozilla San Francisco
2 Harrison Street, Suite 175
San Francisco, CA 94105
United States of America
650.903.0800

Empowered and independent DPA with the authority to enforce these protections against both government and private entities

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 well-resourced data protection authority (DPA) that has enforcement capabilities against both state and non-state entities. While the growing power of private companies over individuals' personal data cannot be overstated, the application of the framework to state actors must be equally strong. The government is arguably the largest data collector in India, more often than not, data collection is mandatory for access to their services. If the data protection framework is to be meaningful, it must apply to all processors and controllers of user data, and if enforcement is to be meaningful, all processors and controllers of user data, public and private, must be accountable to the DPA.

The DPA should be empowered 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.

Given the jurisdiction of the DPA over claims against the state, officials and staff of the DPA must have a high degree of independence from government. It is also critical that the DPA be well staffed and have sufficient resources to fulfill these responsibilities.

Since the nuances of the data protection framework are likely to be detailed in regulations, rules and guidelines of the DPA (apart from sectoral regulations) mandating a consultative process as a necessary component of the process is vital. The Telecom Regulatory Authority of India (TRAI)'s process of consultation for policy and regulatory processes may be instructive.

Finally, we would recommend that given the incredible sensitivity and intimate nature of biometric data, the DPA should be notified before market entry of any and all products, services, and features that collect, store, process, or use biometric data. These notifications should further be supplemented with regular dialogues and consultative processes with industry and public interest stakeholders. The DPA will be best positioned to fulfil its mandate when it is in regular contact with all stakeholders about contemporary data protection issues and practices.

Conclusion

We want to end by thanking the honourable members of the Srikrishna Committee for your diligent engagement with the many issues inherent in crafting a data protection law and for the generally strong approach that you propose. This is a historic moment where India has the opportunity to craft protections that will safeguard the rights of Indians for generations to come. With this law, India has the chance to be a true global leader in protecting individual privacy and

Mozilla San Francisco
2 Harrison Street, Suite 175
San Francisco, CA 94105
United States of America
650.903.0800

security. We look forward to continuing to work with you and other stakeholders throughout this pivotal process.

Respectfully submitted by:

Denelle Dixon
Chief Business and Legal Officer
Mozilla Corporation

Jochai Ben-Avie
Senior Global Policy Manager
Mozilla Corporation

Amba Kak
Tech Policy Fellow
Mozilla Foundation