Mozilla Headquarters
331 E Evelyn Avenue
Mountain View, CA 94041
United States of America
650.903.0800

TO:
Shri Ravi Shankar Prasad
Minister of Electronics & Information Technology (MeitY)

CC:
Joint Secretary
Ministry of Electronics and Information Technology (MeitY)
Room No. 4016, Electronics Niketan,
6 CGO Complex, CGO Complex,
Lodhi Road,
New Delhi – 110 003.

RE: Mozilla's feedback on
the Draft Personal Data Protection Bill, 2018

Thank you for the opportunity to provide feedback on the Draft Personal Data Protection Bill, 2018. The enactment of a baseline data protection law should be a national policy priority for India. Earlier this year, we had put forth a detailed submission[1] to the Justice Srikrishna Committee, and made the same open to the public. The swift progress on this 2018 bill and consultation progress brings India one step closer to a data protection framework that promises to be a model to the world. We are supportive of all of the work that it has taken to get to this point. The intention of this note is to acknowledge that work, and to provide specific comments on the Bill along with some recommendations on areas of improvement. We welcome your commitment to broadening the scope of this important consultation to invite suggestions from experts, stakeholders, and the general public.

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, and Focus. 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

[1] Mozilla submission to Justice Shrikrishna Committee, available at https://blog.mozilla.org/netpolicy/files/2018/02/Mozilla-submission-to-Srikrishna-Committee.pdf

our users. Mozilla's commitment to user security and privacy is evident not just in our products but in our global policy work. [2]

Below we provide comments on several sections of the draft bill. These comments are organised chapter wise, beginning with Chapter I. We have explained our support for the intent and rationale behind several provisions. Where we feel there is scope for improvement or have identified missing protections, we provide specific recommendations. A brief summary of these recommendations is as follows:

- Location metadata should be included in the list of sensitive personal data.

- Data fiduciaries should offer privacy notices and other policies in every language that they offer services in.

- A separate ground for data processing necessary for performance of contract should be included, modeled on the existing provision in the GDPR.

- A right to object to processing should be included to address data processing done under the ground of "functions of the state" and modeled on the existing provision in the GDPR. It should also be clarified that direct marketing will require seeking the consent of the user.

- The term "services and benefits" in the ground on "functions of the state" is overbroad and should be pared down to include core public functions.

- In the "storage limitation" principle, it should be clarified that withdrawal of consent will trigger deletion of data. It should also be clarified that deletion of data should generally occur "as soon as is practicable" to take into account bonafide technical and operational reasons for any delay.

[2] Consider, for example, Mozilla's Data Privacy Principles, available at https://www.mozilla.org/en-US/privacy/principles/

331 E Evelyn Avenue, Mountain View, CA 94041, United States of America • 650.903.0800

- As part of the right to access and confirmation, access to 'a copy of' the personal data undergoing processing should be guaranteed, in addition to the 'brief summary'.

- In case of high risk breaches, data fiduciaries should be obligated to communicate directly to users without undue delay.

- A record of every data breach (with exceptions for zero risk breaches) should be maintained by the data fiduciary for periodic review by the DPAI.

- The requirement to store a copy of all personal data in India should be removed.

- Categories of critical personal data that are currently localised in India for strategic or security reasons should be clearly stated. The open ended mandate to the Central government to notify further categories should be removed.

- Chapter IX titled Exemptions should be renamed "Partial Exemptions"

- The Criminal Procedure Code should be amended to bring it in compliance with the "necessity and proportionality" standard in Section 43.

- Conditions relating to the qualification, manner, and terms of appointment of Adjudicating Officers should be included to ensure independence of such officers.

- The requirement to have the data protection officer "based in India" should be removed and instead only require registration of contact details.

- A defence or exemption for bona fide security research should be included in Section 92.

331 E Evelyn Avenue, Mountain View, CA 94041, United States of America • 650.903.0800

We look forward to continuing to engage with you and other stakeholders in the Government of India as work progresses to finalize 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 as you continue your important work, please do not hesitate to contact Mozilla's Policy Advisor Amba Kak at amba@mozilla.com.

Respectfully submitted by:

Denelle Dixon
Chief Operating Officer
Mozilla Corporation

Jochai Ben-Avie
Senior Global Policy Manager
Mozilla Corporation

Amba Kak
Public Policy Advisor
Mozilla Corporation

Mozilla's Comments on The Personal Data Protection Bill, 2018

Chapter I: Preliminary

Section 2, Jurisdiction

The jurisdictional scope of the law, which mirrors that of the GDPR, goes beyond the requirement of a territorial nexus to regulate entities which offer goods or services in India even though they may not have a presence in India. This approach to jurisdiction is consistent with India's constitutional underpinnings. The fundamental right to privacy is guaranteed by the Indian Constitution and the Supreme Court in *K.S. Puttaswamy v. Union of India* most recently reaffirmed that this right inheres in the individual and it is the obligation of the State to protect this right.

We note, however, that this approach to jurisdiction may not scale well. While it may be tenable for some large companies to abide by differing laws of every country in the world, many startups and smaller companies could be unduly harmed by this, creating a potential barrier to entry into the market. This includes the impact on Indian companies looking to have global presence. This might dampen innovation and limit the provision of services for all but the world's most well-resourced companies.

Section 3 (35), Sensitive Personal Data

Recommendation: **We recommend the specific inclusion of location metadata in the list of sensitive personal data.**

We support having a distinction for categories of sensitive personal data (SPD), with a stricter regime that flows from this distinction. A well defined list of sensitive personal data codified in law is desirable for the certainty it affords data fiduciaries. The bill includes a generally inclusive and progressive list of sensitive personal data including data related to religious or political belief, sexuality, transgender, and intersex status.

Although the definition of SPD crucially includes data "revealing" SPD, we think that there are certain types of information that inevitably reveal sensitive information and therefore warrant such additional protection. For example, location metadata, in particular, should be explicitly included in this list of SPD. There is growing global consensus on the ability of location

331 E Evelyn Avenue, Mountain View, CA 94041, United States of America • 650.903.0800

metadata to comprehensively map an individual's private sphere with trivial effort. This includes insights about other categories of SPD, for example visits to an HIV clinic or political party offices. Data fiduciaries that process such data must be aware of high risk associated with processing such data, and should be subject to the requirement of obtaining explicit consent.

Chapter II: Data Protection Obligations

The set of obligations on all data fiduciaries, outlined in Chapter II represents a sea change for the protection of user privacy in India. We endorse the comprehensive and strongly worded set of obligations to apply to both government and private data fiduciaries, and which apply irrespective of the grounds on which the data is being processed.

In particular, we welcome the affirmation of core privacy principles requiring that businesses should limit the amount of data they collect and justify for what purpose they collect data. At Mozilla, we put these principles into action and advocate for businesses to adopt lean data practices[3]. Businesses managing data will have to consider privacy throughout the entire lifecycle of products and services. These limits will play a crucial role in shaping the scope and direction of business models around big data.

We have specific comments and suggestions for some of these obligations:

Section 8, Notice

Recommendation: **Clarify this provision in the bill to require data fiduciaries to offer privacy notices and other policies in every language that they offer services in.**

Section 8(2) requires translation into regional languages where "necessary and practicable". On the one hand, this flexibility is justifiable. Translation requirements can impose significant costs associated with translating legal documents (including the Privacy Policy, Terms of Service and linked appendices) and also to maintain translated updates to these documents over time. Broad requirements to translate into multiple languages may prove onerous, especially, for small and medium sized companies.

However, the reality remains that the vast majority of the country does not

[3] https://www.mozilla.org/en-US/about/policy/lean-data/

331 E Evelyn Avenue, Mountain View, CA 94041, United States of America • 650.903.0800

speak English, and there is a sizeable non-literate population coming online. There must be an earnest effort to address the challenges associated with making notice meaningful to these users. The DPAI should offer periodic guidance on innovative means to communicate privacy notices to users including non-written means.

Specifically for data fiduciaries that offer services in regional (i.e. non-English) languages, and thereby deliberately target speakers of non-English languages, we think notice should be offered in those language(s). The current "necessary and practicable" standard in Section 8(2) leaves too much ambiguity to data fiduciaries to evade any obligation to make the information required (for users to fully exercise their rights) easily available and understandable.

Section 10, Data Storage Limitation

Recommendation: **We recommend a clarification that withdrawal of consent will qualify as satisfaction of the purpose for which data was processed for the purposes of this section.**

We also recommend that an additional clause be added to the provision to specify that deletion of user data should occur "as soon as is practicable".

We are generally supportive of this provision. Mozilla's position on data retention is summarised in our Data Privacy Principles: "collect what we need, de-identify where we can and delete when no longer necessary."[4] The application of this provision depends on the interpretation of when it is "reasonably necessary to satisfy the purpose" of the data processing act.

Firstly, this provision should play a critical role in situations where individuals withdraw their consent from a service, and should therefore be guaranteed that their personal data will be deleted (assuming no legal requirements to store data for longer). Withdrawal of consent should qualify as satisfaction of the purpose for which data was processed under this section.

Secondly, we are concerned that the provision, at present, might be interpreted to enforce impractical expectations of how soon the deletion would be affected. While data fiduciaries should act expeditiously to honor

[4] Firefox Data Collection

331 E Evelyn Avenue, Mountain View, CA 94041, United States of America • 650.903.0800

their obligations under this Act, for technical and operational reasons it may take some time to delete user data (e.g., when data must be retained for fraud prevention purposes) and the same should not be penalised.

Section 11, Accountability

We strongly support this overarching obligation on data fiduciaries to demonstrate compliance, which is usually fulfilled by proper documentation or data processing actions and decisions. Documentation lies at the heart of open source and it works to create a shared experience that others can reflect back on. It pushes data fiduciaries to make more conscious decisions about how they handle the private information that they've been entrusted with, and aids the regulator in oversight activities designed to ensure that the protections enshrined in law and regulation are followed. This ensures that a data protection law inculcates a culture of preventing harm, not just rectifying it after it has happened.

Chapters III & IV: Grounds for Processing

While the bill provides multiple grounds of processing, for businesses, consent is given a substantial degree of primacy. We welcome this approach as consent is and should remain a critical component of how users' privacy is protected on the web, and this bill puts forth a high standard of meaningful consent.

The bill also permits processing on the basis of other non-consensual grounds, especially for State data processing. We generally agree that in instances where there is a substantial imbalance of power between the individual and the data fiduciary, consent may not be meaningful and therefore may be an inappropriate basis for data processing. However, even where consent is inappropriate, the obligation to provide Notice (in Section 8) must be strictly enforced. We provide specific comments on the grounds below:

Section 17, Ground for Reasonable Purposes

Recommendation: **We recommend clarifying that Section 17(2)(g) does not constitute a safe harbour where the data fiduciary knew or could be expected to have known that such public disclosure was in contravention of the Act.**

331 E Evelyn Avenue, Mountain View, CA 94041, United States of America • 650.903.0800

Overall, we think this is a strongly worded ground for processing, and successfully rectifies some of the ambiguities associated with the parallel provision in the GDPR on "legitimate interest." In particular, the provision specifies certain activities that may be associated with reasonable purposes, including prevention of fraud, whistleblowing, network security, recovery of debt, credit scoring, and others. We generally agree that these are situations where either there is an imbalance of power making consent inappropriate, or the reasonable purpose itself would be frustrated by the need to seek consent.

Moreover, other activities may only come under the scope of this provision if notified by the Authority based on carefully detailed criteria, which minimises the scope for an expansive reading of this provision. These conditions are welcome, and prevent this provision from becoming a loophole to evade the requirement for consent.

However, clause (g) delineated under Section 17(2), ***"Processing of publicly available personal data",*** is concerning. We caution that personal data is often accessible online in some form, or may be buried in some corner of the web, in many cases without the data principal's knowledge or control. For example, consider the many recent unauthorized disclosures of Aadhaar numbers on websites. While we understand that several cases of downstream processing of publicly available personal data might be legitimate (e.g., web crawling for search engines or similar activities), this provision should not allow for activities that take advantage and perpetuate disclosures of personal data that are in violation of provisions of the bill. We recommend that the provision should include a clarification that Section 17(2)(g) does not constitute a safe harbour where the data fiduciary knew or could be expected to have known that such disclosure was in contravention of the Act.

Missing: Performance of Contract

Recommendation: **We recommend including a ground to allow for data processing necessary for the performance of contract modelled on the existing provision in the GDPR.**

In the White Paper prepared by the Justice Srikrishna Committee, they noted correctly that "Grounds such as performance of contract appear to be intuitively necessary, and have been adopted, as is, by jurisdictions." In the Bill, however, there is no separate ground for performance of the contract, and no corresponding explanation in the Report for this omission. The corresponding ground in the GDPR reads that performance of contract will be

331 E Evelyn Avenue, Mountain View, CA 94041, United States of America • 650.903.0800

a valid ground where "the processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract"

This ground in the GDPR has been routinely invoked in a variety of business activities that do not pose significant risk to the data principal. For example, when a user buys something on an e-commerce platform, their credit card details may be processed by a third party payment gateway and their address details will be transmitted to the shipping service that will deliver the package to the user's home. Note, however, that demonstrating "necessity" is key for reliance on this ground. If the data fiduciary could reasonably perform the contract (say, providing a service) without processing their personal data, this basis will not apply. For example, if the same e-commerce platform seeks to shares the user's credit card information with a third party for direct marketing purposes, this processing activity would not be necessary for the performance of the contract (i.e. the delivery of goods bought on the platform), so if the firm wishes to use this data for marketing purposes, they must seek the user's consent. The European Article 29 Working Party Guidelines provide helpful guidance for the interpretation of necessity in the context of performance of contract.[5]

Overall, if the processing is indeed necessary to perform the contract, as the provision should require, having to repeatedly seek consent adds to the concern of consent fatigue with no corresponding benefits. While this bill's ground for employment purposes does cover employment contracts, there are a wider variety of situations that may slip through the cracks in the absence of a separate legal ground for performance of the contract.

Section 13 & 19, Ground for Functions of the State

Recommendation: **The term "services and benefits" should be pared down to include a narrower subset of services and contexts in which where the state is the primary or sole benefit provider. Even in such cases, the notice requirement in Section 8 along with other protections in Chapter II must be strictly enforced. Notices should specify the existence of a right to object to processing and a simple process to exercise this right.**

[5] Article 29 Working Party Guidelines on Consent under Regulation 2016/679; http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051 at page 8,9.

331 E Evelyn Avenue, Mountain View, CA 94041, United States of America • 650.903.0800

The Bill creates broadly worded grounds for processing of personal data by the State. We generally agree that certain data processing by the State demonstrates an imbalance of power with the citizen, and one that is most stark when it comes to essential government services, like food rations or access to healthcare. Especially, for those that have few effective options, the ability to withdraw consent may remain theoretical.

However, the phrasing in the bill casts a wide net that includes all government "services or benefits". This might include many government services that increasingly compete directly with private services (for example, payment and insurance providers, schools, Public Sector Undertakings). It is not reasonable that the data principal is afforded the opportunity to consent only when they use a private provider, and not a state provider operating in the same market. This also harms the level playing field in these markets. While the Justice Srikrishna Committee Report acknowledges this concern and claims that this ground should be limited to the government's core public welfare or regulatory functions, this carve out is not reflected in Section 13. This provision should be narrowly tailored to such essential public functions.

Note that the absence of a consent requirement, even if tailored only to essential government services, still creates the risk that government processing will become opaque and unaccountable. Even if consent is not the basis for processing, data fiduciaries still have an obligation to let users know how their personal data is processed and what rights they have. For example this notice should specify the existence of a right to object to processing and a simple procedure to exercise this right (we expand on this below). In the absence of this right to object, the individual is left with no real recourse to resist data processing by the State. In this context, the notice requirement in Section 8 is paramount, data processing without scrutiny should not be possible.

Chapter VI: Rights

Missing: Right to Object to Processing

Recommendation: **The bill should include a right to object to processing, modelled on the GDPR, and to specifically address data processing by the government. It should separately be clarified that direct marketing will require seeking consent of the user.**

331 E Evelyn Avenue, Mountain View, CA 94041, United States of America • 650.903.0800

In this bill, the lack of a right to object to processing leaves individuals with little control over data processing where consent is not obtained, most notably, when data processing is by the government under the ground of "functions of the state". Justice Srikrishna committee takes the example of an individual refusing to consent to be part of an employment survey as an example of why a right to object might be inappropriate, potentially "skewing the accuracy of the dataset." However, if an individual has a strong reservation to be counted in an employment survey—hypothetically, because they are the only sex worker in a particular sub-district—that is precisely the decisional autonomy that a data protection law should uphold.

The right to object to processing is a key part of the bundle of rights guaranteed by many data protection laws around the world, including the GDPR. It is specifically for situations where consent was not the ground for processing, and therefore the option to withdraw consent does not exist. While an individual must generally provide an explanation for why they're exercising their right to object, under the GDPR, these requests may only be rejected if they are shown to be "manifestly unfounded or excessive".

The GDPR also includes a right to object to direct marketing when a user's data is not processed on the basis of their consent. The Justice Srikrishna Committee Report argued that no direct marketing opt-out is required because the bill gives primacy to consent, making it effectively mandatory for data fiduciaries to seek opt-in consent to direct marketing. While this is a reasonable assumption, the same should be explicitly clarified in the law so that data fiduciaries cannot argue that it is a secondary use expected by users whose contact information has been obtained.

Section 24, Right to confirmation and access

Recommendation: **In addition to a 'brief summary', the bill should also guarantee access to 'a copy of' the personal data undergoing processing.**

We support the inclusion of the right to confirmation and access as a key piece of ensuring accountability to users. In recent times, the corresponding right in the GDPR has been actively exercised by users to investigate data processing by widely used online services. However, this bill limits the right to access of a 'brief summary' of personal data and of processing activities. While a concise summary has its advantages from the user's perspective, access to a copy of their data should always be available to the user. Such a protection would limit data fiduciaries' ability to cherry pick details, and will

331 E Evelyn Avenue, Mountain View, CA 94041, United States of America • 650.903.0800

better allow third party experts to verify processing details ensuring better accountability. We note that the exact contours of what such a "copy of personal data" would entail, including the form and substance of the response, are evolving and further guidance from the DPAI will likely be required.

Section 26, Right to Data Portability

Recommendation: **We recommend an additional provision that states that Section 26 should not be applied to the prejudice of rights of other individuals and obligations in the Act. Further, the DPAI should be specifically mandated to publish guidance to govern the interpretation of the term "trade secrets".**

In general, we think this is a strongly worded data portability right with the key definitional elements. Section 26 (1) (iii) is critical as it includes personal data that may have been purchased or otherwise obtained by the data fiduciary.

One of the controversial applications of this provision is where personal data generated by one individual implicates personal data of another, for example, "likes" on social media, or information about membership of private groups. Here, while Section 26(2)(c) would generally safeguard against such disclosure (it is likely to be "technically infeasible" to separate an individual's personal data from that of others) it may be preferable to have a more explicit safeguard.

Another area of contention could be the interpretation of "trade secrets". While this is a necessary carve out to the application of a data portability right, we encourage the DPAI to publish codes of practice that prevent an over-expansive interpretation of this exception.

Chapter VII: Transparency and Accountability Measures

Recommendation: **In addition to Section 32(1), we recommend that this provision mandate that a record of every data breach (with exceptions for zero risk breaches) is maintained by the data fiduciary for periodic review by the DPAI. We further recommend that the DPAI specifically issue guidance on the criteria to assess "harm caused to the data principal".**

331 E Evelyn Avenue, Mountain View, CA 94041, United States of America • 650.903.0800

Finally, the provision should vest discretion with the data fiduciaries to communicate with the data principals directly in case of a breach, as well as provide a copy of such notice to the DPAI for review and further directions. In cases of high risk breaches, data fiduciaries should be obligated to communicate directly to users without undue delay.

While we welcome a provision that obligates notification of data breach, Section 32 provides too much discretion to the data fiduciary to determine when this duty comes into play. The current provision requires that the data fiduciary only notify the Authority *"where such breach is likely to cause harm to any data principal"*, who will further decide whether such information should be relayed to the data principal.

We note that there may be breaches that impact very few users, cause minimal harm or are mitigated by encryption or other remedies. Based on these factors, it might be the case that every breach need not and should not be notified to the data principals. However, we think that it is important for the DPAI to have some periodic visibility into such instances in order to ensure accountability. Data fiduciaries should still be required by the DPAI to log all such breaches, along with their self assessment of the risk category, so that periodically the DPAI has the opportunity to review. The DPAI should also publish clear guidance on the criteria with which to assess harm and risk to the user in order to prevent varying standards of self-assessment. For example, it may be reasonable to categorise those cases where data is encrypted or de-identified and the key or corresponding records (in the case of de-identification) wasn't breached as zero/low risk of harm to data principals and therefore not requiring follow up action by the DPAI.

Finally, this provision does not accommodate for data fiduciaries voluntarily informing their users in case of breach. We believe some discretion should vest with the data fiduciaries, and further that when it is a case of a high risk breach, data principals should also be obligated to notify affected users without undue delay. The GDPR mandates that where the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, users must also be notified without undue delay (Article 34).

Where data fiduciaries directly notify their users of a breach or other compromise of their personal data, a copy of the same should be sent to the DPAI for review. If the DPAI finds such notice to be insufficient, they should still have the opportunity to order the data fiduciary to take additional action. Particularly where time is of the essence, we believe this would incentivise

331 E Evelyn Avenue, Mountain View, CA 94041, United States of America • 650.903.0800

those companies with healthy data security practices to communicate with their users in a timely manner.

Section 38 and Section 36(4), Significant Data Fiduciaries

Recommendation: **Remove "in such manner as may be specified" and replace with a more specific requirement to register contact details and other information relevant to the classification of an SDF.**

Remove the requirement to have the Data Protection Officer be "based in India" and instead only require registration of the DPO and their contact details.

Overall, we agree with imposing additional obligations on significant data fiduciaries (SDFs). In particular, the requirements of data protection impact assessments, record keeping, data audits, and appointment of a data protection officer are all critical parts of preventing harm before they occur and echo the rationale behind risk-based regulation.

However, the requirement to register with the DPAI should be more narrowly scoped. While it is reasonable that the DPAI shall keep track of the notified SDFs and their contact details, the requirement to register "in such manner as may be specified" leaves open the door for onerous registration requirements which should be avoided.

We also think the requirement in Section 36(4) to have the Data Protection Officer "based in India" may not be reasonable if the fiduciary does not otherwise have operations here, and this geographical mismatch would in fact hinder the DPO from effectively supervising operations. Moreover, fragmenting the DPO role based on country significantly curtails the benefit of having a single person responsible for compliance with data protection obligations. Here too, it is reasonable for the DPAI to have updated records of the DPO and their contact details, but the requirement to be based physically in India is excessive.

331 E Evelyn Avenue, Mountain View, CA 94041, United States of America • 650.903.0800

Chapter VIII: Transfer Of Personal Data Outside India

Localisation of Personal Data and Sensitive Personal Data

Recommendation: **Remove the requirement to store a copy of all personal data in India.**

This bill introduces a general requirement to store a copy of all personal data in India. The Justice Srikrishna Committee bases this decision on the premise that it will ensure better compliance with this law and orders of the DPAI. In its absence, they argue, India will be resigned to rely only on the inefficient MLAT process.

We disagree with this rationale for several reasons:

- Enforcement directives from a strong Data Protection Authority of the kind envisioned under this bill are unlikely to be ignored by foreign companies providing services to Indians. Companies with global ambition can no longer afford to keep all their assets out of India if they are serious about having a presence in this market. The stakes are already large enough, and it will be more so as they increase their exposure to India in terms of human resources, customers, and other assets.

- A requirement to store data in the country will likely create a conflict of laws situation for multinational companies. U.S. law, for example, would still effectively limit companies from disclosing many kinds of user data to foreign law enforcement authorities without a US warrant or subpoena. A similar situation is likely to hold for European companies, as per GDPR art. 48. Localisation does not, and should not, by itself do away with these procedural safeguards and cannot override foreign laws and treaties governing data flows.

- While large companies could more easily afford the additional costs associated with this data localization mandate, the expense of compliance may prove disproportionately harmful to small businesses and start ups.

331 E Evelyn Avenue, Mountain View, CA 94041, United States of America • 650.903.0800

On the other hand, a broad data localisation mandate introduces new risks for users and liabilities for businesses:

- *Surveillance and security*

  Localizing data in servers in India makes personal data more susceptible to overbroad access by law enforcement and surveillance agencies. As the Committee notes, surveillance reform in India is much overdue and currently there are little to no procedural safeguards around government surveillance. While surveillance may be a legitimate function of the state, these are powerful tools in the hands of government agents and should be subject to accountability, transparency, due process, and meaningful limits. This follows from the Supreme Court's diktat in *Puttaswamy v. Union of India* where the judges held that any state interference with privacy must be subject to tests of legality and strict proportionality. Given that the current legal framework falls short of these standards, a broad localisation mandate is likely to mean even fewer checks on the power of law enforcement to access personal data.

  Moreover, storing a copy of all personal data pertaining to Indians' in a handful of locations could create a "honey pot" for malicious actors, therefore increasing vulnerability to breach. In comparison, distributing storage of data across a network of servers globally means that there is no concentrated point of attack or single point of failure. Many businesses might find that this mandate would jeopardize the security of the personal data they retain, with implications for users globally, not just in India.

- *Routing and business inefficiencies*

  A requirement to store data locally, or store at least a copy of data locally, introduces potentially higher costs and actual limitations on technology innovation, development, and use.

  When faced with the mandate to store at least a copy of the data in India, many companies might choose to store only in India to save on costs. 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

331 E Evelyn Avenue, Mountain View, CA 94041, United States of America • 650.903.0800

ultimately undermines the efficiency and potentially the integrity of internet traffic.

Other small and medium sized global companies, in particular, might find that this requirement increases storage costs significantly, or compromise the security of their services, and might choose to close off their services to Indian users. This would be a loss to the vibrancy of the Indian digital ecosystem, and eventually, this loss of choice will hurt the end user.

Moreover, 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, in turn introducing a heavy burden on Indian companies looking to have global presence. Rather than ease the challenge of gaining lawful access for investigative purposes to personal data stored abroad, this state of affairs would exacerbate challenges for Indian law enforcement agencies.

Section 40(2), Localisation of Critical Personal Data

Recommendation: **Categories of critical personal data that are currently localised in India for strategic or security reasons should be clearly stated. The open ended mandate to the Central government to notify further categories should be removed.**

We acknowledge that certain categories of personal data may need to be mandatorily stored within the country, with restricted data flows, due to the strategic and security interests at play. It is reasonable therefore for defence or Aadhaar data, for example, to be stored exclusively in India as is current practice. However, Section 40(2) of the bill leaves the definition of critical personal data entirely open to Government discretion and does not elucidate what such categories might be, nor any parameters to circumscribe this discretion. Since mandating data storage in India generally amplifies the concerns of routing inefficiencies, increased costs and security risks, this wide discretion is concerning.

Section 41, Cross-border data transfer

Recommendation:
We recommend the removal of Section 41(6). Any stipulations relating to certification and further review of standard contractual clauses should

331 E Evelyn Avenue, Mountain View, CA 94041, United States of America • 650.903.0800

removed and be left to further guidance by the DPAI.
We recommend that Section 41(3) should be redrafted to clearly state that the provision is directed at critical personal data, and not all sensitive personal data.

The bill provides the right balance between protecting user rights and allowing businesses sufficient flexibility for cross-border transfer. It provides for a variety of options, including standard contractual clauses, binding corporate rules, and determination of adequacy for countries or sectors.

While it is reasonable for the Committee to have left the details of formulation and approval of standard contractual clauses out of the bill, Section 41(6) requires data fiduciaries to "certify" and "report" to the Authority when relying on such clauses. In the absence of any other context, this requirement is not justified. Eventually, if the DPAI decides to automatically certify standard clauses already approved in countries with adequate levels of data protection (the European Commission, for example, has approved a variety of model clauses), then this requirement would in fact become redundant and onerous.
We also note that Section 41(3) of the bill is ambiguously worded. Although the specific restrictions are clearly limited to critical personal data, the same is not explicit, and instead refers to "sensitive personal data... that is notified." This should be re-drafted to maintain uniformity of terms and improve clarity.

Chapter IX: Exemptions

Recommendation: **Rename the chapter "Partial Exemptions"**

This chapter is not one of complete exemptions, but rather limited applicability of the Act for certain types of data processing. As such, the Chapter should be re-titled "Partial Exemptions"

Section 42, Security of the State

The partial exemption for processing of data for the security of the state is a significant improvement over the status quo in several ways. First, this provision requires that a law is passed by Parliament to sanction intelligence gathering activities. Moreover, this law and activities sanctioned thereunder would have to fulfil the standards of "necessity and proportionality". If not, the law would also run foul of the Constitutional diktat in *Puttaswamy v*

331 E Evelyn Avenue, Mountain View, CA 94041, United States of America • 650.903.0800

Union of India.

It remains unclear, however, how the jurisdiction of the DPAI will apply in the event that this provision is not complied with, given that these processing activities seem to be exempt from the Chapter on enforcement by the DPAI. In this context, it becomes imperative for a law to regulate intelligence gathering to be passed in order to be harmonious with this provision.

Section 43, Prevention, detection, and investigation of contravention of law

Recommendation: **Amend criminal procedure code to bring it in compliance with the "necessity and proportionality" standard in Section 43.**

This partial exemption does require that law enforcement agencies comply with the standard of "necessity and proportionality". As Mozilla has long argued the standard for due process when it comes to law enforcement access must be high. We recently argued[6], for instance, that companies must always have the possibility to seek judicial review of law enforcement requests that risk violating our users' rights.

Some legal provisions currently on the books, such as Section 91 of the Code of Criminal Procedure, could potentially run foul of the standard in Section 43. At present, Section 91 allows "any officer in charge of a police station" to summon "any document or other thing" if it is considered "necessary or desirable" for the investigation. This broadly worded provision without any layer of independent or judicial oversight over these orders or purpose limitation seems to stray away from the standard of necessity and proportionality endorsed in this bill. We recommend amendments to bring this provision in compliance with the necessity and proportionality principle, and that such amendments be tabled alongside this Act.

Chapter X: Data Protection Authority of India/Chapter XV: Miscellaneous

Recommendation: **Include conditions relating to the qualification, manner, and terms of appointment of Adjudicating Officers in the Bill, as has been included for the DPAI, to ensure independence of such**

[6] https://blog.mozilla.org/netpolicy/2018/08/22/europe_lawful_access/

331 E Evelyn Avenue, Mountain View, CA 94041, United States of America • 650.903.0800

officers.

The composition of the DPAI is well detailed in the bill, and includes several commendable safeguards to ensure competency and independence. These include a host of stipulations relating to selection process, tenure, termination, cool-off period, and so on. The complete lack of such safeguards for the adjudicating officer (and appellate tribunal) that are *solely* responsible for compensation and penalties is a major deficiency in the bill. Instead, the Central Government is delegated very broad powers to select the number, qualifications, jurisdiction, and terms of appointment of such officers. These vastly different standards for the executive and investigatory functions, on one hand, and the adjudicatory body with penalty powers on the other is without justification and puts the independence of the DPAI in question.

Section 98, Power of Central Government to issue directions

***Recommendation:* Section 98 must be narrowly tailored to prevent the DPAI from being unilaterally subject to government directions.**

Section 98 gives wide powers to the Central government to issue directions to the DPAI on "questions of policy" , as it thinks fit, to protect a wide range of state interests. Further, as per Section 98(4), the Central Government has final authority on whether the direction pertains to a "question of policy" and there is no clear avenue for judicial review of such directions. This provision appears to be a common feature for other statutory regulators such as the TRAI and SEBI, and there is existing court jurisprudence to limit its interpretation.

However, we believe there is a need to narrow the scope of this provision, especially in the context of a regulator that will have jurisdiction over several government agencies, including the power to enforce penalties or order compensation from the government if the law is violated. In the UK, for example, the Information Commissioner (ICO) has routinely fined government agencies for violations of the data protection legislation. For such a deterrent to function effectively in India, the DPIA must be sufficiently insulated from the Central Government's diktat and this provision threatens to weaken this independence.

The lack of independence of the DPAI could jeopardize India's chances of obtaining a determination of adequacy from the European Commission, and other countries evaluating the strength of India's data protection laws. The

331 E Evelyn Avenue, Mountain View, CA 94041, United States of America • 650.903.0800

European Commission's officials have time and again pointed out that "States have a responsibility to ensure the independence of all DPAs".[7]

Chapter XIII: Offences

Section 92, Re-identification and processing of de-identified personal data

Recommendation: **Introduce a defence or exemption for bona fide security research.**

Section 92 attaches criminal penalties to re-identifying personal data which has been de-identified by a data fiduciary or data processor without their consent. While re-identification without consent removes anonymity and might cause harm to data principals, we worry that this provision is over-inclusive. In particular, those that do bona fide security research, for example, to demonstrate that purportedly anonymised data is not in fact anonymised, might be caught under this provision. Given that this offence is punishable with imprisonment or a hefty fine, a defence for such bona fide processing is necessary to prevent this provision from discouraging such bona fide security research

[7] Giovanni Buttarelli, European Data Protection Supervisor, CPDP 2017, speech available at https://edps.europa.eu/sites/edp/files/publication/17-01-26_cpdp_2017_competition_en.pdf

331 E Evelyn Avenue, Mountain View, CA 94041, United States of America • 650.903.0800

Conclusion

We want to end by thanking Hon'ble Minister of Electronics & Information Technology, Shri. Ravi Shankar Prasad and MeitY for your commitment to enacting a comprehensive data protection law in India. This is a historic moment where India has the opportunity to craft protections that will safeguard the rights of Indians for generations to come and be a true global leader in protecting individual privacy and security. We look forward to continuing to work with you and other stakeholders throughout this pivotal process.

Respectfully submitted by:

Denelle Dixon
Chief Operating Officer
Mozilla Corporation

Jochai Ben-Avie
Senior Global Policy Manager
Mozilla Corporation

Amba Kak
Public Policy Advisor
Mozilla Corporation