Mozilla Corporation
331 East Evelyn Avenue
Mountain View, CA 94041

25 February 2020

TO:
Smt. Meenakshi Lekhi,
Member of Parliament,
Chair, Joint Committee on The Personal Data Protection Bill, 2019

CC:
Director, Lok Sabha Secretariat,
Room No. 152, Parliamentary House Annex,
New Delhi - 110001

RE: Mozilla's comments on the Draft Personal Data Protection Bill, 2019

Respected Ma'am,

Thank you for the opportunity to provide feedback on the Draft Personal Data Protection Bill, 2019. As we have long argued, the enactment of a baseline data protection law should be a national policy priority for India. In 2018, Mozilla had put forth a detailed submission to the Justice Srikrishna Committee[1], made the same open to the public, and also engaged with the Ministry of Information Technology (MeitY) in their public consultation on the bill.[2] We are supportive of the work that it has taken to get to this point. The intention of these comments is to acknowledge that work, and to provide specific comments on the Bill along with recommendations on areas of improvement. We welcome the Committee's decision to invite suggestions from experts, stakeholders, and the general public as a part of its deliberations.

Mozilla is a global community of technologists, thinkers, and builders -- including thousands in India -- working together to keep the internet open,

[1] Mozilla submission to Justice Srikrishna Committee, available at https://blog.mozilla.org/netpolicy/files/2018/02/Mozilla-submission-to-Srikrishna-Committee.pdf
[2] Mozilla's comments on the Draft Personal Data Protection Bill, 2018 available at https://blog.mozilla.org/netpolicy/files/2018/10/Mozilla-Submission_MEITY_PDP-Bill-2018.pdf

Mozilla Corporation
331 East Evelyn Avenue
Mountain View, CA 94041

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, Firefox Lite, 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 our users. Mozilla's commitment to user security and privacy is evident not just in our products but in our global policy work.[3]

One of the biggest concerns in the new draft is the bill's expansion of the broad exceptions that were present in the 2018 draft. Crucially, the requirement that government processing of data be "necessary and proportionate" has been removed. This power is unrestricted and not subject to any checks and balances, either independently via the judiciary or internally within the government. This leaves the current legal vacuum around India's surveillance and intelligence services intact, which is fundamentally incompatible with effective privacy protection. We urge that this provision be urgently reformed and that the 'necessary and proportionate' standard be reintroduced into the final bill to give Indians the privacy that they deserve.

Below we provide comments on several sections of the draft bill. To briefly summarize, we recommend that:

- **Section 3 (36) -** Location metadata should be included in the list of sensitive personal data.

- **Section 7 -** Data fiduciaries should offer privacy notices and other policies in every language that they offer services in.

- **Section 9 -** 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

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

Mozilla Corporation
331 East Evelyn Avenue
Mountain View, CA 94041

practicable" to take into account bonafide technical and operational reasons for any delay.

- **Section 12 -** The term "services and benefits" in the ground on "functions of the state" is overbroad and should be pared down to include core public welfare or regulatory functions as discussed in the Justice Srikrishna Committee report.

- **Section 14 -** A separate ground for data processing necessary for performance of contract should be included, modeled on the existing provision in the GDPR.

- **Section 19** - As part of the right to access and confirmation, access to "a copy of" the personal data undergoing processing should be guaranteed (instead of being optional), in addition to the "brief summary".

- **Section 25 -** 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 minimal risk breaches) should be maintained by the data fiduciary for periodic review by the DPAI.

- **Section 26 -** The requirement to have the data protection officer "based in India" should be removed and instead only require registration of contact details.

- **Section 28 -** The provision on social media user verification should be removed as it is not related to data protection and creates additional privacy and security risks for users.

- **Section 33(2) -** 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.

Mozilla Corporation
331 East Evelyn Avenue
Mountain View, CA 94041

- **Chapter IX** titled Exemptions should be renamed “Partial Exemptions”

- **Section 35 -** Any government exceptions should be limited by the “necessary and proportionate” standard present in Section 42 of the 2018 draft bill.

- **Section 42** - Revert the composition of the “selection committee” of the DPA in Section 42 to include judicial and independent members present in Section 50 of the 2018 draft.

- **Section 82 -** A defense or exemption for bona fide security research should be included in Section 82.

- **Section 91 (2) -** The provision related to forced sharing of non-personal data should be removed as it is not related to data protection and contains significant risks of violating group privacy and trade secrets.

- The implementation timelines present in the 2018 draft of the bill should be included for predictability and clarity.

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 Udbhav Tiwari at udbhav@mozilla.com

Respectfully submitted by:

Udbhav Tiwari,
Public Policy Advisor, Mozilla Corporation

Jochai Ben-Avie,
Head of International Policy, Mozilla Corporation

Mozilla Corporation
331 East Evelyn Avenue
Mountain View, CA 94041

Mozilla's Comments on The Personal Data Protection Bill, 2019 to India's Joint Parliamentary Select Committee on the Personal Data Protection Bill, 2019

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.

Section 3 (36), 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

Mozilla Corporation
331 East Evelyn Avenue
Mountain View, CA 94041

list of SPD. There is growing global consensus on the ability of location 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.

Recommendation: We recommend the specific inclusion of location metadata in the list of sensitive personal data in Section 3(36).

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.[4] 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 7, Notice

Section 7(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

[4] Lean Data Practices available at https://www.mozilla.org/en-US/about/policy/lean-data/

Mozilla Corporation
331 East Evelyn Avenue
Mountain View, CA 94041

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 speak English, and there is a sizable 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.

In general, data fiduciaries should provide binding privacy and other legal notices in any language which they offer their services in. 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.

Recommendation: Clarify Section 7(2) to require data fiduciaries to offer privacy notices and other policies in every language that they offer services in.

Section 9, Data Storage Limitation

An additional clause should be added to Section 9to 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."[5] The application of this provision depends on the interpretation of when it is "reasonably necessary to satisfy the purpose" of the data processing act.

[5] Firefox Data Collection available at https://wiki.mozilla.org/Firefox/Data_Collection

Mozilla Corporation
331 East Evelyn Avenue
Mountain View, CA 94041

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 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.

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 and that data deletion section should include a "as soon as reasonable"standard to account for practical considerations such as fraud detection.

Chapters III: 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 7) must be strictly enforced.

We provide specific comments on the grounds below:

Mozilla Corporation
331 East Evelyn Avenue
Mountain View, CA 94041

Section 14, Ground for Reasonable Purposes

Overall, we think Section 14(2) 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 14(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.[6] 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. The recent disclosures of Clearview AI scraping publicly available social media images for its facial recognition offering[7] is a prime instance of why such practices should be discouraged. We recommend that the provision should include a clarification

[6] https://cis-india.org/internet-governance/information-security-practices-of-aadhaar-or-lack-thereof-a-documentation-of-public-availability-of-aadhaar-numbers-with-sensitive-personal-financial-information-1
[7] https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html

Mozilla Corporation
331 East Evelyn Avenue
Mountain View, CA 94041

that Section 14(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.

Recommendation: We recommend clarifying that Section 14(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.

Missing: Performance of Contract

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 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

Mozilla Corporation
331 East Evelyn Avenue
Mountain View, CA 94041

Guidelines provide helpful guidance for the interpretation of necessity in the context of performance of contract.[8]

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.

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.

Section 12, Ground for Functions of the State

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

[8] 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.

Mozilla Corporation
331 East Evelyn Avenue
Mountain View, CA 94041

not reflected in Section 12. 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 should 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 7 is paramount, data processing without scrutiny should not be possible.

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 7 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.

Chapter V: Rights

Section 17, Right to confirmation and access

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 gives a choice within the right to access either a copy of the data or 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 rather than as an option. Such a protection would limit data fiduciaries' ability to cherry pick details, and will better allow third party experts to verify processing details ensuring better

Mozilla Corporation
331 East Evelyn Avenue
Mountain View, CA 94041

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.

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

Section 19, Right to Data Portability

In general, this is a strongly worded data portability right with the key definitional elements. Section 19 (1) (a) (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 19(2)(b) 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. However, this technical feasibility should not be used as a gating mechanism to avoid data export obligations and the law must account for best efforts being made to allow for the right to be exercised by subjects.

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 overly expansive interpretation of this exception.

Recommendation: We recommend an additional provision that states that Section 19 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."

Mozilla Corporation
331 East Evelyn Avenue
Mountain View, CA 94041

Chapter VI: Transparency and Accountability Measures

Section 25 should vest discretion with the data fiduciaries to communicate with the data principals directly in case of a data 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 25 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 allow for data fiduciaries voluntarily informing their users in the case of a 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

Mozilla Corporation
331 East Evelyn Avenue
Mountain View, CA 94041

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

Recommendation: In addition to Section 25(1), we recommend that this provision mandate that a record of every data breach (with exceptions for minimal risk breaches) be 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."

Section 26, Significant Data Fiduciaries

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 harms 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.

Mozilla Corporation
331 East Evelyn Avenue
Mountain View, CA 94041

We also think the requirement in Section 30(3) 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.

Recommendation: Remove "in such manner as may be specified" in Section 27(4) and replace with a more specific requirement to register contact details and other information relevant to the classification of an SDF. Additionally, the requirement from Section 30(3) to have the Data Protection Officer be "based in India" should be removed and instead should only require registration of the DPO and their contact details.

Section 28, Social Media User Verification

Compelling social media platforms to offer voluntarily verification of identity to users will be disastrous for the privacy and anonymity of Indian subjects, for (at least) four reasons: sensitive information used for verification will leak and be used in harmful ways; implementation will reinforce existing power asymmetries within companies; ambiguity in categorization will scale these active harms up; and all of this risk will come with no demonstrable benefits at addressing misinformation and similar challenges.

It stands to reason that the expected form of verifying a user's identity would involve the collection of government-issued identification. Aadhaar cards, driving licences, passports, and other government IDs contain a wealth of sensitive and irrevocable information about their users. These include names, dates of birth, addresses, contact numbers, photographs, and unique numbers that serve as an identifier to access critical government services (e.g., PAN numbers). The proposed provision will effectively hand over the data to social media companies on a vast scale. The companies that obtain consent

Mozilla Corporation
331 East Evelyn Avenue
Mountain View, CA 94041

under their often incomprehensible privacy policies will then be able to use this data against their users to profile and target them.

This is not a hypothetical scenario. There is considerable evidence of social media companies already doing so with other uniquely identifiable information, such as phone numbers. In order to prevent account takeovers and provide better security, many firms allow users to store their phone numbers for two-factor authentication. When enabled, users receive one time password (OTP) via SMS, which they need to provide in addition to their password to login into a website or an application.

Despite the clear security-focused nature of this service, Facebook[9] in 2018 and Twitter[10] in 2019 were both found to be using this information to profile users and send targeted ads. When such companies will be incentivised to collect government IDs, little would prevent them from using this treasure trove to further invade user privacy for profits.

Moreover, the resources that will be required to build and maintain these verification systems in a secure manner will further entrench the already lopsided power dynamics in social media. One of the surest ways to ensure only large companies can provide social media services is to design laws that create significant compliance burdens and privacy risks for startups.

There is also the inherent difficulty in rigidly categorizing "social media companies." Are websites that let users leave comments below news articles also social media companies? What about reviews for restaurants on food aggregator apps? The same issue extends to travel review websites and countless other service providers. This ambiguity will lead to companies erring on the side of caution and collecting user data anyway, harming privacy.

There is remarkably scant evidence to prove that the verification of users online will help combat fake news and misinformation, which is ostensibly

[9] https://www.engadget.com/2018/09/28/facebook-two-factor-phone-numbers-ads/
[10] https://techcrunch.com/2019/10/08/twitter-admits-it-used-two-factor-phone-numbers-and-emails-for-targeted-advertising/

Mozilla Corporation
331 East Evelyn Avenue
Mountain View, CA 94041

the motivation behind this provision. Given that the vast majority of misinformation spreads on WhatsApp groups, online forums, and chat applications, the verification of users for certain social media accounts will not improve digital literacy or critical reasoning, which are primarily responsible for its societal harms. It's also not clear that people spreading misinformation will be deterred by having to use their verified, real names. This provision also ignores the benefits that anonymity can bring to the internet, such as whistleblowing and protection from stalkers.

Given the above concerns and the impending amendments to India's intermediary liability regime, this provision should be removed from the bill in its entirety as it would actively harm the privacy of Indians.

Recommendation: Remove Section 28 as social media user verification is not related to data protection and in fact creates additional privacy and security risks.

Chapter VII: Transfer Of Personal Data Outside India

Section 33(2), Localisation of Critical Personal Data

In a positive move compared to the 2018 draft, the law relaxes data localisation restrictions and applies them to only sensitive and critical personal data. For sensitive data, the data can be processed outside the country and there are also reciprocity based exceptions that allow even critical and sensitive data to be processed outside the country. However, sensitive data must be processed only in India, and it continues to be hard to see this as anything other than an effort to make surveillance easier.

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 33(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. Since mandating data storage in India

Mozilla Corporation
331 East Evelyn Avenue
Mountain View, CA 94041

generally amplifies the concerns of routing inefficiencies, increased costs and security risks, this wide discretion is concerning.[11]

Recommendation: The requirement to process sensitive personal data only in India should be removed from the law and data localisation should be limited exclusively to critical personal data. 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 VIII: 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"

Recommendation: Rename the chapter "Partial Exemptions"

Section 35, Government Exemptions

The 2018 draft of the data protection bill's exemption on processing for the "security of the state" was a significant improvement over the status quo in several ways. The provision required that a law be passed by Parliament to sanction intelligence gathering activities. Moreover, this law and activities sanctioned thereunder would have had to fulfil the standards of "necessity and proportionality" (which are an essential component of the *Puttaswamy v Union of India* case which enshrined the Fundamental Right to Privacy).

However, one of the biggest concerns in the new draft is the bill's expansion of the broad exceptions that were present in the 2018 draft. Crucially, the requirement that government processing of data be "necessary and proportionate" has been removed. Furthermore, a provision (Section 35) has been added granting the government complete discretion to exempt any entity or department from any part of the law.

[11] https://blog.mozilla.org/netpolicy/2018/06/22/data-localization-india/

Mozilla Corporation
331 East Evelyn Avenue
Mountain View, CA 94041

This power is unrestricted and not subject to any checks and balances, either independently via the judiciary or internally within the government. This leaves the current legal vacuum around India's surveillance and intelligence services intact, which is fundamentally incompatible with effective privacy protection.

The presence of such a provision also is likely to make obtaining adequacy under the GDPR or a similar bilateral agreement with any other country almost impossible, given that the biggest processor of data of Indian subjects (the government) can exclude itself from any part of the law.

One of the greatest incentives for a country to adopt a data protection law right now is to receive adequacy – a determination by the European Commission that a country has a sufficiently high level of privacy protections. Receiving adequacy would allow data to flow freely between Europe and India, creating the largest addressable market in the world. Likewise, companies that are already GDPR-compliant would easily be able to invest in India and process data without the need to design and maintain separate systems. Again, the key to unlocking this incredible economic opportunity is enacting strong data protection rules.

With the dramatic carve outs for government processing, it's hard to see how to see how the EU will find that data will be safe in India. European courts have not been shy about their concerns about state surveillance. Consider the struggles the US has had with various agreements governing the transfer of data between the US and Europe. 4 years ago, in the Schrems case, the Court of Justice of the EU (CJEU) struck down the Safe Harbour Agreement in its entirety, citing concerns that Europeans' data was not adequately protected from US government surveillance. In 2020, the CJEU may rule to strike down the Privacy Shield -- the new agreement for data trans-atlantic data transfer negotiated after Schrems -- in a separate case brought by Austrian privacy activist Max Schrems. While far from perfect, the US at least has laws establishing limits and procedures for government surveillance. Given the questions and challenges around government access to personal data that have been raised in EU-US transfers, it's hard to see how the CJEU, the

Mozilla Corporation
331 East Evelyn Avenue
Mountain View, CA 94041

European Commission, and other European regulators will sign off on adequacy for India given the total lack of limits on government access in the Personal Data Protection Bill.

Such a provision also runs afoul of the Constitutional diktat in *Puttaswamy v Union of India*, which stated any exceptions to the fundamental right to privacy must be necessary and proportionate. In order to provide Indian subjects effective data protection, it is vital that this provision be reformed and be amended with the "necessary and proportionate" language present in Section 42 of the 2018 draft of the bill.

Recommendation: Replace the language in Section 35 with the "necessary and proportionate" standard present in Section 42 of the 2018 draft bill.

Section 36, Prevention, detection, and investigation of contravention of law

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, for instance, that companies must always have the possibility to seek judicial review of law enforcement requests that risk violating our users' rights.[12]

At present, Section 91 of the CrPC 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 Puttaswamy judgment. We recommend amendments to bring this provision in compliance with the necessity and proportionality principle, and that such amendments be tabled alongside this Act.

[12] Getting cross border lawful access in Europe right, available at https://blog.mozilla.org/netpolicy/2018/08/22/europe_lawful_access/

Mozilla Corporation
331 East Evelyn Avenue
Mountain View, CA 94041

Recommendation: Amend the criminal procedure code to bring it in compliance with the "necessity and proportionality" standard in Section 43 of the 2018 draft.

Chapter IX and X: Data Protection Authority of India and Penalties

The new law further reduces the powers and independence of the data protection authority of India (DPAI) by significantly weakening the commission that will appoint the Chairperson and members of the DPAI. Where the 2018 draft said that they were to be appointed by a diverse committee with executive, judicial, and external expertise, the new law limits this committee to members of the executive alone. This will make it much harder for the DPA to be independent, empowered, and effective as the entire governing structure will be appointed exclusively by the government. The independence of the data protection authority is essential to ensuring that government agencies and private entities are subject to fair, unbiased, and reliable governance in its administrative and adjudicatory functions.

Additionally, Article 45(2)(b) of the GDPR clearly states that an "independent supervising authority" is an essential criteria for obtaining adequacy, where the current framework would almost certainly negatively impact India's negotiations with the EU in this regard.

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 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.

Recommendation: Revert the composition of the 'selection committee' of the DPA in Section 42 to include judicial and independent members present in Section 50 of the 2018 draft.

Chapter XIII: Offences

Section 82, Re-identification and processing of de-identified personal data

Section 82 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. A recent report by Fireye states that organisations learnt about more cyber security incidents (which often involves performing re-identification) from third party reports than from internal teams.[13] This provision would actively outlaw such security research, harming India's cyber security posturing. 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.

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

Chapter XIV: Miscellaneous

Section 86, Power of Central Government to issue directions

[13] https://www.fireeye.com/current-threats/annual-threat-report.html

Mozilla Corporation
331 East Evelyn Avenue
Mountain View, CA 94041

Section 86 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 86(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' evaluation of the strength of India's data protection laws. The European Commission's officials have time and again pointed out that "States have a responsibility to ensure the independence of all DPAs".[14]

Recommendation: Section 86 must be narrowly tailored to prevent the DPAI from being unilaterally subject to government directions.

Section 91(2), Forced Transfer of Non Personal Data

[14] 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

Mozilla Corporation
331 East Evelyn Avenue
Mountain View, CA 94041

This provision currently mandates that certain companies can be forced to transfer non-personal data to the government for public good and policy planning purposes. Non-personal data can constitute protected trade secrets and the insights derived from such data may be protected by intellectual property law, both of which would raise significant concerns around the fundamental right to carry out business and international trade law. Turning over this information to the government or private entities without any checks and balances also raises significant privacy concerns. Information about sales location data from e-commerce platforms, for example, can be used to draw dangerous inferences and patterns regarding caste, religion, and sexuality. The law should continue to focus on the protection of personal data and leave the regulation of non-personal data to an independent law.

Recommendation: Remove this provision from the law as it is not related to personal data protection and contains significant risks of violating group privacy and trade secrets.

Missing: Implementation Timelines

The 2018 draft clearly laid out the timelines for the creation of the data protection authority, the accompanying subsidiary legislation, and the date in which the law would finally be enforceable. The new law removes all references to this timeline and merely mentions that the Central Government may notify the enforcement of the law at its complete discretion, creating ambiguity and uncertainty for data fiduciaries.

Recommendation: Include the implementation timelines present in the 2018 draft of the bill.

Conclusion

We want to end by thanking the Hon'ble Minister of Electronics & Information Technology, Shri. Ravi Shankar Prasad and MeitY for their commitment to enacting a comprehensive data protection law in India and the Joint Committee for undertaking this comprehensive review. This is a historic moment where India has the opportunity to craft protections that will

Mozilla Corporation
331 East Evelyn Avenue
Mountain View, CA 94041

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:

Udbhav Tiwari,
Public Policy Advisor,
Mozilla Corporation

Jochai Ben-Avie,
Head of International Public Policy,
Mozilla Corporation