ASSESSING INDIA'S PROPOSED DATA PROTECTION FRAMEWORK:

WHAT THE SRIKRISHNA COMMITTEE COULD LEARN FROM EUROPE'S EXPERIENCE

accessnow.org

India is on the cusp of providing a data protection and privacy regime for the next billion users of the internet.

accessnow

Assessing India's proposed data protection framework: What the Srikrishna Committee could learn from Europe's experience

India is on the cusp of providing a data protection and privacy regime for the next billion users of the internet.

TABLE OF CONTENTS

I. INTRODUCTION

India is home to the second-largest internet user population in the world, but still awaits an effective national privacy and data protection law. The Government of India began the process of seeking to draft and enact a privacy law nearly a decade ago, starting more actively in 2010. The most recent work of the committee of experts chaired by Justice Srikrishna, constituted by the Ministry of Electronics and Information Technology, follows from multiple consultations, committee and drafting efforts by various ministries in the Indian government over the past decade. It is high time India gets a comprehensive data protection and privacy legislation.

On July 27, 2018, a 10-member committee of experts on the data protection framework in India submitted a 176 page report and a draft bill entitled The Personal Data Protection Bill, 2018 ("**Draft Bill**") to the Minister of Electronics and Information Technology, Ravi Shankar Prasad. The head of the committee is retired Indian Supreme Court Justice B.N. Srikrishna.

It is essential that the privacy and data protection framework for the next billion users of the internet in India is informed by global best practices, and provides a strong, user rights-respecting regime. Most recent global discussions around data protection have focused on the European Union's enactment and recent implementation of the General Data Protection Regulation (GDPR). The GDPR is a positive framework for users' protection and will help users take back the control of their personal information. The EU GDPR is inspiring a number of governments around the world to introduce data protection legislation or to upgrade the existing laws, and it is proving to be a benchmark in discussions around data protection standard-setting and enforcement. The Draft Bill prepared by the Srikrishna Committee draws inspiration in many instances from the GDPR as well. However, whether the Draft Bill provides an adequate framework for protecting the rights of the citizens of India is a matter of debate.

Access Now has published a data protection guide for lawmakers across the globe built on lessons from the EU's GDPR that highlights do's and don'ts for comprehensive data protection legislation. Here we match the Srikrishna Draft Bill against the recommendations in the guide to provide a metric for the success (and failures) of the draft law.

Following the submission of the report and the Draft Bill by the expert committee to the Government of India, we embarked on an exercise of evaluating the Draft Bill, using the principles from the lawmakers' guide as the benchmark. We have sought to provide a clear, concise, and principles-based evaluation of the complexities within the data protection framework proposed by the Indian expert committee.

II. ANALYSIS

1. ENSURE TRANSPARENT, INCLUSIVE NEGOTIATIONS

NEEDS IMPROVEMENT

The first principle Access Now advocates is ensuring transparent and inclusive negotiations, to guarantee that users' rights are adequately represented. The European Union held transparent public consultations to draft the GDPR: each consultation was published and made public. This made it so the negotiation process was relatively transparent and ensured adequate opportunity for the inclusion of multiple perspectives despite the unprecedented level of corporate lobbying against the law. In contrast, the B.N. Srikrishna committee organised only four public consultations during its study of data protection in India. Given the size of India's population and the importance of this issue, the consultations were not adequate to include diverse perspectives.

While the Indian government has previously made consultations public, the Srikrishna committee did not bring these consultations into the public domain. In addition, civil society did not find effective representation on the committee, and there are legitimate concerns that several members are biased in favour of the Aadhaar Unique ID programme.

Throughout the term of the committee, the government denied several Right to Information requests on its workings, including requests for the minutes of the committee meetings. These denials negatively impacted the transparency of the committee's work. Several documents showing the policy positions of the committee were nevertheless leaked, including provisions of the Draft Bill. These leaks served to inform the public about the proceedings in the committee as well as revealing draft legislation.

The committee has fallen short of carrying out a transparent and inclusive pre-legislative consultation. The onus now lies on the Union Government executive (specifically, the Ministry of Electronics and IT, and the Prime Minister's Office and Council of Ministers) to address this issue. It is important that the government conduct a thorough and transparent public consultation before the Draft Bill is passed by Parliament. The government is mandated to do so under its own Pre-Legislative Consultation Policy of 2014. It may also be beneficial for the executive to work with members of Parliament on public hearings and consultations. Additionally, after legislation is introduced in Parliament, the referred standing committee must conduct a comprehensive review, with public consultations as well as testimony from independent experts and civil society.

The Draft Bill provides for a mandatory consultation on codes of practice. Section 61 of the Draft Bill provides for mandatory consultations in the framing of codes of practice. This is a good first step. However, the Draft Bill does not require mandatory — leave aside meaningful — public consultation for all of the regulation-setting powers that the contemplated Data Protection Authority (the "Authority") is provided. The regulation-setting power of the central government occasionally requires consultation with the Authority, but the Draft Bill creates no mandate for the executive branch to conduct public consultations, only requiring the tabling of such regulations in

Parliament and the option of MPs seeking to annul or amend those regulations. The law must place a clear, cross-cutting public consultation mandate on all regulations issued under the proposed Act, building on the best practices established elsewhere in existing Indian regulatory law, including the principles that bind the Telecom Regulatory Authority of India. We would also encourage the government to consider requiring annual reports on the state of data protection from the proposed Data Protection Authority.

2. DEFINE AND INCLUDE A LIST OF BINDING DATA PROTECTION PRINCIPLES IN THE LAW

NEEDS IMPROVEMENT

For a data protection framework to be effective, it must include a clear definition of personal and sensitive data, which the Draft Bill provides. In addition to a clear definition, Access Now's data protection handbook proposes eight principles for meeting the "minimum standards" for data protection, which should form the core of any data protection framework. These principles are:

1. Fairness and Lawfulness: This principle provides that personal data must be processed fairly, lawfully, and in a transparent manner. The Draft Bill provides for collection and processing of data only when there is a clear legal basis for doing so, and it also provides for transparency. (We shall discuss the legal basis as well as the transparency provisions below.)

2. Purpose Limitation: This principle provides that personal data shall be collected and processed only for a specific purpose. The Draft Bill sets purpose limitations for processing as well as collection, as overarching principles which must be abided. However, the section on purpose limitation provides overbroad allowances for data processing. In addition to the specified purpose, it allows processing of data for "*for any other incidental purpose that the data principal would reasonably expect the personal data to be used for, having regard to the specified purposes, and the context and circumstances in which the personal data was collected.*" These allowances dilute the principle of purpose limitation and are ambiguous in nature.

3. Data Minimisation: This principle provides that personal data collected and used shall be limited to what is adequate, relevant, and not excessive in relation to a specific and defined purpose. Section six of the Draft Bill limits the collection of personal data to the data that is necessary for the purposes of processing, and thus, provides a collection limitation requirement. The United Kingdom Data Protection Act, 2018 [section 57(3) and 57(4)] provides a narrower data minimisation requirement, where collection of data must be limited to the data that is necessary for the specific purposes of processing.

4. Accuracy: This principle provides that personal data should be accurate and kept up-to-date. The Draft Bill puts the responsibility on the data fiduciary to ensure that the personal data processed is accurate, complete, and updated. However, this requirement has been limited to taking reasonable steps, and does not serve as an absolute obligation. A data fiduciary is defined under the Draft Bill as a person who determines the purpose and means of processing personal data. Additionally, under section 25 of the Draft Bill, the data principal (the user) has the right to rectify any incorrect or incomplete personal data stored with the data fiduciary. However, under

the provision, the user does not have the direct right to approach the Authority if the efforts of the data fiduciary are not satisfactory.

5. Retention Limitation: This principle provides that personal data processed for any purpose shall not be kept for longer than necessary. Provisions of the Draft Bill (section 10) work on similar lines. In the Draft Bill, the data fiduciary is allowed to retain personal data only for the time period necessary to satisfy the purpose of processing. However, under the provision, the user does not get a direct right to approach the Authority if the efforts of the data fiduciary are not satisfactory.

6. Users' Rights: This principle provides that personal data should be processed in accordance with necessary binding user rights. The Draft Bill grants users four major rights, including the rights to confirmation and access (section 24), the right to correction (section 25), and the right to data portability (section 26). The right to information is diluted under the Draft Bill; it is limited to a "brief summary" of the personal data being processed and the processing activities. However, it does not entitle users with certain rights, such as the right to an explanation and the right to erasure, which are provided to the users under the EU's GDPR and also the UK Data Protection Act, 2018. The rights to explanation and erasure are crucial for accountability and transparency in the use of algorithms to make decisions in our lives.

7. Integrity and Confidentiality: This principle provides that processing of personal data should be done in a manner that ensures the state-of-the-art security of the data, using appropriate technical or organisational measures. Section 29 of the Draft Bill advocates for "privacy by design", an important and positive step. According to Section 31 of the Draft Bill, the data fiduciary and data processor will have to implement security safeguards including use of de-identification and encryption methods, steps to protect the integrity of personal data, and steps necessary to prevent misuse, unauthorised access to, modification, disclosure, or destruction of personal data. Further, every data fiduciary and the data processor will also have to undertake a periodic review of its security safeguards. The Draft Bill takes a great step forward towards a secure internet by providing for requirements of encryption.

8. Adequacy: This principle provides that data transfers to other countries should always be prohibited until the country ensures an adequate level of protection for the rights of users in relation to personal data processing. The Draft Bill, under section 41, empowers the proposed Data Protection Authority to determine the adequacy status of other countries. Other mechanisms, such as model contract clauses, similar to provisions under the GDPR, have also been provided.

---

3. DEFINE LEGAL BASIS AUTHORISING DATA TO BE PROCESSED

NEEDS IMPROVEMENT

Any data protection law must clearly define the legal basis under which users' personal data can be processed. These usually include the execution of a contract, in compliance with a legal obligation, and a user's consent. Consent shall be defined as an active, informed, and explicit request from the user. It must be freely given and the user must have the capacity to withdraw consent at any time. Section 12 of the Draft Bill makes it mandatory to obtain the prior consent of

the data principal for personal data processing. Valid consent under the Draft Bill is supposed to be when it is free, informed, specific, clear, and can be withdrawn. The Draft Bill also provides that the ease of withdrawing consent must be comparable to that of giving consent. These provisions are positive and would ensure good protection of consent in all situations where it is needed. In addition, the data fiduciary is prohibited from making provision of service or quality thereof conditional on consent for the processing of any personal data, if the processing is not necessary for that purpose. This provision is an encouraging step towards data minimisation and ensuring privacy for the individual. However, no specific right to contest such "necessity" has been provided under the Draft Bill, and the data fiduciary remains the arbiter for determining the standard of such "necessity".

Section 13 of the Draft Bill has a problematic dilution of the provision on prior and mandatory consent by the data principal. This provision authorises the state to process personal data for "the exercise of any function of the state" without the consent of the individual. The provision is vague and overbroad, and it gives the government an absolute right over citizens' data. In India, multiple levels of government — Union, State, Municipal / Panchayat (local government) — carry out state functions, with differing levels of sophistication. A catch-all exemption for all state functions becomes even more dangerous in this context. It is imperative that data protection principles apply to the state as well as to private actors.

Similarly, the Draft Bill, under section 14, entitles the Authority to process personal data to comply with any law, order, or judgment of courts or tribunals. Clause (a) of this provision is potentially harmful, given that its broad language allows legislatures and executive offices across the breadth of India's federal polity to weaken the comprehensive aim of a national data protection law by allowing any general law to override data protection provisions.

Sections 17 and 19 contain another set of provisions that could dilute the data processing provisions of the Draft Bill. These sections could allow an exception where personal and sensitive personal data may be processed without consent. According to the provisions, personal data may be processed for "reasonable purposes". This phrase is vague and gives latitude for violating the data rights of citizens. This power to establish "reasonable purposes" has been provided to the Data Protection Authority, and thus there is at least a process for determining such purposes. The presence of an illustrative list of "reasonable purposes" is concerning as it seeks to include "credit scoring", "recovery of debt", etc., already indicating that "reasonable" commercial interests could trump rights-protecting data protection measures.

Similarly, the Draft Bill entitles the Authority to process personal and sensitive personal data to comply with any order or judgment of courts or tribunals. This provision must be subject to standards of necessity and proportionality.

The Draft Bill also entitles employers with overbroad rights in relation to their employees. Section 16 of the Draft Bill allows employers to process the personal data of their employees for purposes related to employment, including recruitment, termination, and assessment of the employee, without the need for consent. These rights are overbroad and unnecessary, and subjugate an employee's rights to those of the employer. An employment relationship does not lead to the

cessation of fundamental rights of an employee. Such a provision is not present in the GDPR, UK Data Protection Act 2018, and other comparative legislation.

Finally, in order to process the personal and sensitive data of children, prior parental consent is required. According to section 23 of the Draft Bill, data fiduciaries must incorporate appropriate mechanisms for age verification and parental consent to process personal data of children. Besides, the Draft Bill prohibits processes like tracking, monitoring, and targeted advertising in relation to children, a regulatory approach that should be welcomed.

4. INCLUDE A LIST OF BINDING USERS' RIGHTS IN THE LAW

NEEDS IMPROVEMENT

Protecting users' data requires setting out a series of binding rights. The Draft Bill entitles users with some rights, including the right to confirmation and access, the right to correction, the right to data portability, and the right to legal representation. Below we discuss these rights:

***Right to confirmation and access*:** Section 24 of the Draft Bill entitles the data principal — that is to say, the user — with the right to obtain information about the personal data and the processing activities of the data fiduciary. However, this right is limited to a "brief summary" of the data processed and the associated processing activities. This dilution brings in ambiguity — a data principal must have a right to know what data is being processed, as well as the processing activities in sufficient detail, without compromising the intellectual property rights of the data fiduciary. This right is an essential right, wherein full and proper disclosure may form the foundation of the user's capacity to protect other rights, as learnt in one of the cases brought in the EU by Max Schrems, the founder of *noyb*.

***Right to correction*:** Section 25 of the Draft Bill entitles the data principal with the right to correct inaccurate personal data and update personal data that is old. If the data fiduciary does not agree to correct, complete, or update personal data at the request of the data principal, the data fiduciary must provide legal justification for rejecting the request. A dilution of the right lies in its nature as a non-mandatory entitlement. The data fiduciaries' obligation is limited to situations "where necessary", and not in every case.

***Right to data portability*:** The right to data portability enables data principals to move personal data from one platform to another that offers similar services. Section 26 of the Draft Bill entitles the data principal with the right to obtain the personal data from one data fiduciary and transfer it to another. The section grants the principal the right to receive the personal data which has either been submitted to the data fiduciary, generated in the course of the provision of service, or which forms a part of a profile of the data principal obtained by the fiduciary. This right, however, has been diluted, especially in relation to the data processed by the government. In cases where processing is necessary for state function (under section 13) or for compliance with law (under section 14), no right to data portability exists. While in certain situations the right to data portability may be constrained, it is important that such limitation is applied in a proportionate manner.

Right to object: Under the Draft Bill, users are provided the right to grievance redressal under section 39, and a right to file a complaint under section 28 and 68, in case the data fiduciary violates any of the provisions of the Draft Bill, including provisions relating to consent, purpose limitation, etc. However, no specific right to object is provided under the Draft Bill.

Right to explanation: Users have not been provided a specific right to an explanation regarding an automated decision under the Draft Bill. Such a right empowers users to obtain information about the logic involved in any automated processing of personal data and the consequences of such processing. This right is crucial for accountability and transparency in the use of algorithms to make decisions that impact users' lives.

Right to erasure: This right allows users to request the deletion of all personal data related to them when they leave a service or application. While under section 10, retention limitations have been imposed on the data fiduciary, and under section 27, a right to prevent disclosure of information has been provided after one leaves a service or application, no direct right to erasure has been provided. This right is essential to ensure that data trails are effectively deleted, which is important given the large number and popularity of services / applications in the world right now.

General conditions for exercise of rights of users: The Draft Bill provides certain conditions for the exercise of rights by data principals under section 28 of the Draft Bill. In order to exercise certain rights, the data principal may need to provide "a reasonable processing fee" to the data fiduciary. These rights are fundamental to a user, and the user should not be charged for their exercise. The rights are further limited under a broad exception, wherein a data fiduciary may refuse the data principal, in cases where the exercise of the right would harm the right of any other data principal. The language for the limitation is overbroad, and therefore is liable to be misused by data fiduciaries. It is important that limitations to the rights of users are narrow and specific, with clear avenues for redress.

---

5. DEFINE A CLEAR SCOPE OF APPLICATION

PASS

The entitled rights and principles established under any data protection law should apply all the time and should have clarity on the scope of application. Section two of the Draft Bill defines and specifies the application of the bill. The Draft Bill applies to the processing of personal data which has been collected, disclosed, shared, or processed within the Indian territory. The Draft Bill also applies to the processing of personal data by the Indian government, any Indian company, any Indian citizen, or any person incorporated or created under Indian law. However, the Draft Bill does not apply to the processing of anonymised data.

The internet and digital technologies more widely do not recognise territorial boundaries. Hence, it is always difficult for legislators and policymakers to ensure users' rights without applying the principle of extraterritoriality. The Draft Bill also applies to entities based outside India, if data processing is in connection with any business carried on in India, or if the processing is in connection with activities involving profiling of data principals within the territory of India. This provision is similar to the scope of application in the EU's GDPR. The GDPR is applicable to those

who are either processing personal information in connection with the offering of goods or services to, or monitoring of the behaviour of, users who are in the European Union. While such jurisdiction does raise concerns of extraterritoriality, it is important that such provisions be provided as they ensure that rights of users remain protected in all situations, regardless of location.

---

6. CREATE BINDING AND TRANSPARENT MECHANISMS FOR SECURE DATA TRANSFER TO THIRD COUNTRIES

FAIL

The Draft Bill troublingly seeks to establish a data localisation regime. Section 40 of the Draft Bill makes it mandatory for every data fiduciary to store one copy of users' personal data on a server or data centre located in India. This section dilutes India's connection to the global internet and betrays a governmental interest in desiring more control over the data of Indian citizens. The report submitted by the expert committee enlists enforcement and access as the primary motives behind this requirement. However, data localisation is not — and should not — be a prerequisite for enforcement of data protection rules. What is more, such a requirement may facilitate third-party abuse of personal data and infringe on users' right to privacy, as actors would know where data is located. Such proposals go against the spirit and objective of a data protection and privacy legislation. Curiously, there is an exception created to this rule wherein the central government may make certain categories of personal data exempt from the requirement of local storage on the grounds of necessity or strategic interests of the state. There is, however, no guidance provided regarding such strategic interests or necessity.

More positively, the section authorises the central government to mark categories of personal data as "critical personal data" — such data can only be processed or stored in a data centre located within India. The cross-border transfer of critical personal data is however allowed to a person or entity engaged in the provision of health services and emergency services. Transfer of critical personal data is also permissible to countries and international organisations if the central government in consultation with the Authority (the Data Protection Authority established under Section 49 of this Draft Bill) prescribes to do so. These provisions are therefore different from a data localisation requirement as it simply creates safeguards and conditions for this data to flow in a rights-respecting manner.

Section 41 of the Draft Bill specifies provisions for cross-border transfer of non-critical personal data. These provisions are similar to the GDPR. According to the section, the cross-border transfer of personal data is permissible when the central government in consultation with the Authority prescribes to so. The central government may ask for cross-border data transfers only where it finds that the personal data shall be subject to an adequate level of protection, having regard to applicable laws and international agreements. Additionally, data transfers may also be made subject to *standard contractual clauses or intra-group schemes* that have been approved by the Authority. In addition, the Authority may also approve a particular transfer or set of transfers as permissible due to a situation of necessity. There is no guidance provided regarding such situations of necessity.

7. PROTECT DATA SECURITY AND DATA INTEGRITY

PASS

The Draft Bill takes steps to protect personal data by introducing the principle of "privacy by design". Section 29 of the Draft Bill entitles the data fiduciary with the responsibility to implement policies and measures for privacy by design. Privacy by design not only protects data; it also leads to data integrity. This is in line with the EU GDPR principle of data protection by design and default.

Besides, section 31 of the Draft Bill holds the data fiduciary and the data processor responsible for implementation of appropriate security safeguards. It also makes it mandatory for every data fiduciary and data processor to undertake a review of its security safeguards periodically, which should help in ensuring actual compliance and increased data protection responsibility across businesses.

The Draft Bill (section 33) also entitles data fiduciaries with the responsibility of making data-protection impact assessments from time to time, especially when new technologies are introduced, or they use sensitive data, or carry out large-scale profiling. This is a positive measure.

The Draft Bill also seeks to establish transparency in data processing, as section 30 of the Draft Bill holds the data fiduciary responsible to notify the data principal of important operations in personal data processing. In addition, section 34 and section 35 of the Draft Bill specifies the provisions and makes it mandatory for data fiduciaries to maintain records and be subject to annual data audits.

The Draft Bill makes it mandatory for data fiduciaries to appoint a Data Protection Officer in order to ensure transparency and accountability measures. This person is also responsible for providing assistance to, and cooperating with, the Authority, and to act as the point of contact for the data principal for the purpose of raising grievances to the data fiduciary.

8. DEVELOP DATA BREACH PREVENTION AND NOTIFICATION MECHANISMS

NEEDS IMPROVEMENT

Despite taking stringent measures for data protection and data integrity, data breaches can still take place. Therefore, an express mechanism to address, prevent, and notify users of those breaches should be put in place. Section 32 of the Draft Bill provides for a legal requirement for data fiduciaries to inform the Authority of breaches of personal data. In case of data breaches, the data fiduciary has to notify the Authority regarding the breach, where such breach is likely to cause harm to any data principal. The notification sent to the Authority is supposed to include details on the nature of personal data, number of data principals affected, possible consequences, and measures being taken by the data fiduciary. Further, informing the data principal about the breach depends on the discretion of the Authority. Upon receipt of the notification, the Authority

is authorised to determine whether such breach should be reported by the data fiduciary to the data principal or not. In addition, the Authority may direct the data fiduciary to take appropriate remedial action. The Authority is also expected to post the details of the personal data breach on its own website. However, the entitlement of discretionary powers provided to the Authority could weaken the data breach prevention and notification mechanism — the users must have the right to always be notified so that they know when their information has been breached. Additionally, in case such information is only disclosed to the Authority, the Authority must make public the criteria for its assessment of severity of the harm to the user of a data breach and such criteria must include a human rights impact assessment.

9. ESTABLISH INDEPENDENT AUTHORITY AND ROBUST MECHANISMS FOR ENFORCEMENT

FAIL

No comprehensive data protection mechanism can be effective without a dynamic and powerful enforcement mechanism. A powerful enforcement mechanism includes the creation of an independent data protection authority. Section 49 of the Draft Bill seeks to establish and incorporate a data protection authority for the purposes of the Draft Bill, which will be known as the Data Protection Authority of India. According to Section 60, the duty of the Authority shall be to protect the interests of data principals, prevent any misuse of personal data, ensure compliance with the provisions of this Act, and promote awareness of data protection.

The constitution of the Authority

The chairperson and the members of the Authority shall be decided by a committee of six members, consisting of a judicial representative (the Chief Justice of the High Court of India or a judge she has nominated), the Cabinet Secretary to the Government of India, and one expert of repute nominated by the judicial representative. The chairperson and the members of the Authority shall be persons of ability, integrity and standing, and must have specialised knowledge of, and not less than 10 years professional experience in, the field of data protection, information technology, data management, data science, data security, cyber and internet laws, and related subjects. The criteria for membership can be considered vague, and given that the appointments are made by the government, there is a possibility of a pro-regime bias creeping into the Authority. Additionally, the expert, while nominated by the judicial representative, is required to be chosen from a pool of experts maintained by the Union Government. In such a case, there is a possibility of the Union Government hijacking the selection committee. This is important given the fact that in India, the government may soon be the biggest processor of data. Such provisions raise concerns regarding the independence of the Authority. The selection process around the composition of the Authority requires improvements, including more civil society involvement. Additionally, there seems to be no bar on re-employment of members of the Authority by the private sector or the government. It has been noted many times in India that such requirements help in creating an unbiased regulator, as observed under the Telecom Regulatory Authority of India Act, 1997.

There is a separate wing envisaged under the Authority in the Draft Bill for adjudication of penalties. However, the separation of powers between the adjudication wing and the Authority is not clear. While the Authority seems to be in charge of inquiries and subsequent orders in relation to practices of the data fiduciary, it appears that the adjudication of complaints is at the sole discretion of the adjudication officer. This seems to create multiplicity of jurisdictions within the same Authority, which may lead to competing claims in differing wings of the Authority.

The supervision of the adjudication wing is unclear as well; while the adjudication wing is within the Authority, the intention seems to be to create a separate wing, which isn't under the influence of the Authority. The report for the Draft Bill recommends that the adjudication wing function at an "arm's length" from the rest of the Authority.

Additionally, the method of appointing the adjudication officer is unclear, and is kept at the sole discretion of the central government. Given that the adjudication officer is the direct source of redressal and defence of user rights under the Draft Bill, it is imperative that the appointment and functions are also ensured to be bipartisan and independent.

Several powers of the Authority are proposed to be carried out by "inquiry officers" appointed by the Authority. These officers would inquire into concerns and complaints, admitted by the Authority. The Authority would issue directions and orders based on the reports submitted by these officers. The relationship between the inquiry officers and the adjudication wing is unclear; it seems that there is a multiplicity of jurisdictions under the current Draft Bill.

Appeals from the order of the adjudication wing and the Authority would lie with an appellate tribunal. Second appeals from the tribunal would lie with the Supreme Court of India. Given the vast mandate of the tribunal, its independence and functioning gains importance. No criteria for qualifications and appointment of appellate tribunal members has been provided under the current Draft Bill. The central government has been provided full powers to determine this, without need of parliamentary approval. This could lead to considerable loss of autonomy and independence by letting the executive branch control the appeals process.

Powers of the Authority

The Draft Bill entitles the Authority with judicial powers. The Authority has been entitled with the same powers as are vested in a civil court under the Criminal Procedure Code (CrPC) such as the power to discover and inspect documents, to summon and examine witnesses, besides several other powers. The Authority has the power to conduct inquiries (under section 64), the power to issue directions (under section 63), issue codes of practice (under section 61), and order search and seizures (under section 66), along with the power to issue a variety of orders on the basis of an inquiry (under section 65).

Under section 65 of the Draft Bill, the Authority may (a) issue a warning to the data fiduciary or data processor, (b) issue a reprimand to the data fiduciary or data processor, (c) require the data fiduciary or data processor to cease and desist from certain actions, (d) require the data fiduciary or data processor to modify its business or activity for compliance, (e) temporarily suspend or

discontinue the business or activity of the data fiduciary or data processor, and (f) suspend or discontinue any cross-border flow of personal data, among other things.

In addition to the above, the adjudication officer under the Authority may also order penalties, up to four percent of the worldwide turnover of the preceding year of the contravening entity in case of breaches of the provisions of the Draft Bill by such entity.

---

10. CONTINUE PROTECTING DATA PROTECTION AND PRIVACY

PASS

Even if a comprehensive data protection law is codified and notified, the government should keep protecting personal data and privacy. Digital technology is evolving at a rapid rate. This implies that a frequent review process will be necessary to address potential issues for compliance and to update the law. Section 61 of the Draft Bill authorises the Authority to issue codes of practice to promote good practices of data protection and entitles it with the right to review, modify, or revoke a code of practice. The Authority is given the responsibility for checking for a data fiduciary or data processor's failure to comply in data protection. In addition, the lawmaking process by the Authority requires a mandatory consultation process with relevant sectoral regulators and stakeholders. This provision is commendable and will lead towards participative policy-making on data protection.

Further, Section 62 of the Draft Bill provides powers to the Authority to issue directions from time to time to data fiduciaries or data processors. In addition, Section 63 of the Draft Bill grants powers to the Authority to call for and ask the data fiduciary and data processor to provide information, whenever necessary.

11. DO NOT SEEK BROAD DATA PROTECTION AND PRIVACY LIMITATIONS FOR NATIONAL SECURITY

FAIL

Government also has a security interest in data protection, especially when the government agencies themselves are the data fiduciaries and store data. Governments often seek limitations to data protection and privacy rights for their own use of personal data by asking for broad exceptions. Section 42 of the Draft Bill provides exemption for processing of personal data in the interests of the security of the state. According to the provision, such data processing shall not be permitted unless it is authorised pursuant to a law. It must be noted that this law could be any law passed by Parliament or a state legislative assembly, without a specific reference or carve-out on data protection. No clear procedure or criteria has been defined to exempt data processing in the interests of the security of the state. Such broad exemptions render these provisions open to abuse and dilution of the protection provided for the rights of users at risk. Additionally, Indian law requires effective surveillance law reforms, a fact that the Srikrishna committee also noted in its expert report; in particular, Indian government agency practices and powers for surveillance may not be in compliance with the Indian Supreme Court's clarifications on the fundamental right

to privacy from its August 2017 *Puttaswamy* constitutional bench decision (which also explicitly cites the internationally recognised Necessary and Proportionate Principles that set out human rights standards to govern communications surveillance). Data protection and surveillance reform are complementary to each other in ensuring the privacy rights of users, yet this Draft Bill does not provide any surveillance reforms and is thus a missed opportunity to provide effective data protection in that regard.

12. DO NOT AUTHORISE PROCESSING OF PERSONAL DATA BASED ON THE LEGITIMATE INTEREST OF COMPANIES WITHOUT STRICT LIMITATIONS

NEEDS IMPROVEMENT

Data fiduciaries argue that they should have the right to collect and process personal data without user consent based on their legitimate interest. That demand should not be met, as it directly contradicts data protection principles and deprives users of control over their data. The EU GDPR allows organisations and companies to collect personal data based on their "legitimate interests". Under "legitimate interest" an organisation is authorised to collect and use personal data without notifying the concerned users.

Section 17 of the Draft Bill allows for data processing for "reasonable purposes" without obtaining the consent of the data principal. This exception, along with the broad definition of purpose under purpose limitation, seems to be another way of approaching the "legitimate interest" exemption. A data fiduciary can process personal data of a user without consent if processing is in the interest of the data fiduciary. The data without user consent can also be processed where it is expected that the user might give her consent for doing so. This section authorises the Authority to specify reasonable purposes for activities, including whistleblowing, mergers and acquisitions, recovery of debt, and prevention and deletion of fraudulent activities. The provision on data processing for "reasonable purposes" weakens the binding rights of users, as they cannot exercise these rights unless they know that an organisation has gathered and holds data about them.

13. DO NOT DEVELOP A "RIGHT TO BE FORGOTTEN"

NEEDS IMPROVEMENT

The "right to be forgotten" or the "right to de-list" gives users the right to request that search engines de-list web addresses from results when a search is done using their name. This right is always confused with the "right to erasure", which allows the users to delete all personal data in case they have left the service or application. In the EU GDPR, the right to be forgotten was added to the right to erasure, codifying the jurisprudence of the EU Court of Justice in the "Google Spain" case. The right to erasure is one of the most important binding rights to ensure data protection and privacy of the user.

The Draft Bill does not entitle users with the right to de-list or right to be forgotten. But Section 27 of the bill entitles users with the right to restrict the disclosure of personal data in case they leave

the service or application. However, this right has been designated as a right to be forgotten in the Draft Bill. The terms should not be confused.

In relation to disclosure of information, the Draft Bill has taken a balanced approach by entitling users with the right to restrict data processing after leaving services and in a manner which establishes a balance between users' control over their data and freedom of speech and expression. A "right to be forgotten" request under the Draft Bill shall only be effectuated pursuant to an order by an adjudication officer, who must consider the rights and interests of the data principal in preventing or restricting the continued disclosure of personal data and ensure that they don't override the right to freedom of speech and expression and the right to information of any citizen. However, under the Indian legal framework, the right to information is a separate right established under a distinct institution. Interactions between the "right to be forgotten" and the "right to information" must necessarily be decided upon by the authorities under the right to information framework.

---

14. DO NOT AUTHORISE COMPANIES TO GATHER SENSITIVE DATA WITHOUT CONSENT

NEEDS IMPROVEMENT

Sensitive personal data requires a higher level of protection than other personal data. Therefore collection and processing of sensitive personal data should be allowed only when the user gives explicit and informed consent. Also, she should be able to withdraw her consent conveniently. The EU GDPR requires data fiduciaries to obtain explicit consent of the user to gather and process sensitive data. However, it also allows data fiduciaries to collect and use sensitive personal data without users' consent for some specific purposes, including "scientific or historical research purposes or statistical purposes". Section 18 of the Draft Bill allows data fiduciaries to process data on the basis of explicit consent. According to the section, valid user consent should be clear, informed, and specific. Section 21 of the Draft Bill allows the processing of personal data without consent in situations where prompt action is necessary. Such situations include responding to a medical emergency, providing medical treatment during an epidemic, and ensuring safety during any disaster or breakdown of public order. The Draft Bill allows processing of sensitive data without users' consent for "certain functions of the state". This broad exception dilutes the strong provisions for sensitive data processing and deprives users of control over their data. The exception becomes more problematic with the rapid growth of the digital health industry and big data analytics.

Like the EU GDPR, the Draft Bill does allow the data fiduciaries to process sensitive data without users' consent for purposes like scientific or historical research. Section 45 of the Draft Bill allows the processing of sensitive personal data for research, archiving, and statistical purposes, as specified by the Authority. In specifying such purposes, the Authority must ensure that (a) the compliance with the provisions of this Act will disproportionately divert resources from the purpose, (b) the purposes of processing cannot be achieved if the personal data is anonymised, (c) the data fiduciary has carried out de-identification meeting the standard contained in any code of practice, (d) personal data will not be used to take any decision specific to or action directed specifically towards the data principal and (e) personal data will not be processed in a manner

that gives rise to a risk of significant harm to the data principal. These principles for deciding "research, archiving, and statistical purposes" are a good start for the Authority and would help in guiding decision making.

Section 91 of the Draft Bill specifies a penalty for obtaining, transferring, or selling sensitive personal data. According to the section, any person who obtains, discloses, transfers, or sells sensitive personal data shall be punishable with imprisonment up to five years or a fine up to rupees three lakhs, or both.

The Draft Bill proposes a prospective framework; therefore, the status of sensitive data collected and processed before the enactment of this law would be in question. Would the troves of data already collected and processed before enactment of the law then go unregulated? Indian lawmakers must surely come up with an equitable solution for this problem.

---

15. DO NOT FAVOUR SELF-REGULATION AND CO-REGULATION MECHANISMS

PASS

For a long time, data fiduciaries have called for a data protection mechanism — but through self-regulation. However, examples of successful non-binding regimes for data protection are scarce. The Draft Bill prohibits self-regulation by the industry or co-regulation, so the influence of private players under its provisions would be limited.

Section 180 of the Draft Bill entitles the Authority with the power to make regulations consistent with the provisions and rules prescribed under the legislation to carry out its purposes. It is important to note that under section 61 of the Draft Bill, the Authority is also allowed to approve and issue codes of practice submitted by an industry association, any association representing the interests of data principals, any regulator, or the ministries of the central or state Government of India. Such codes of practice would, however, remain subject to public consultation. The Draft Bill seems to try to find a middle path to allow other stakeholders to propose regulations, while keeping the final approval power with the Authority.

III. CONCLUSION

A step forward for data protection, but the work is not done

The submission of the report and the Draft Bill by the committee to the Ministry of Electronics and Information Technology is an important step in that direction, but it is one that requires substantial improvements and fixes. The imperative now lies with the the Ministry of Electronics and Information Technology to consider the bill, perhaps make amendments, and then choose to bring the bill to Parliament for enactment. Whether and when the bill will be introduced or passed remains a matter of speculation, given the upcoming general elections likely to occur in the first half of 2019. The current government has only two sessions of Parliament left for introduction, consideration, and passage of the bill. It is clear that while the government has initiated the

consultation process, the passage of a comprehensive data protection regime still faces many policy and political hurdles in India.

While the Draft Bill draws from various sources, most notably the recently enacted General Data Protection Regulation (GDPR) in the EU, our analysis shows there are multiple areas of concern for its efficacy in protecting the rights of the users in India.

While the Draft Bill obliges a Data Protection Authority to conduct "'mandatory" public consultation while making "codes of practices", multiple areas of regulation have been put outside the purview of this obligation. While the step towards mandatory public consultations is positive, it is imperative that such consultations are made mandatory with respect to all regulations issued by the Authority. Such consultations would help to make policy development on data protection in India more user-centric, transparent, and accountable.

The central theme for a data protection regime lies in the rights provided to the users. While multiple important rights entitled to the users have been codified under the Draft Bill, many gaps persist under the proposed regime. Rights such as the right to access and rectify data have been diluted and must be strengthened, and certain key rights such as right to object and the right to explanation are not provided under the Draft Bill. It is imperative that the Draft Bill is improved to ensure a rights-respecting data protection framework in India. The steps taken toward data integrity and data protection impact assessment are encouraging.

Consent and the standards thereof for data collection are core principles underlying privacy and data protection, and the Draft Bill does provide encouraging provisions for ensuring proper consent. However, the provisions on obtaining prior explicit consent should not be diluted by the overbroad criteria of "exercise of functions of the state". As discussed above, such overbroad criteria expose the provisions to misinterpretation and misuse. Furthermore, given the importance of sensitive personal data, similar overbroad exceptions for treatment of this information must be narrowed.

The Draft Bill has taken a mixed approach in dealing with data flows. On one hand, the Draft Bill provides for data localisation norms, a major drawback. Keeping one copy of every instance of a user's data at data centres located in India is impractical and would impose a heavy burden on the internet-based companies and other data fiduciaries. More importantly, such measures serve a surveillance and law enforcement purpose, at the cost of privacy and protecting user data. In the absence of adequate regulation of governmental access to citizen data in India, these data localisation measures may make user data in India liable to indiscriminate access by the government. On the other hand, the Draft Bill has specified comprehensive cross-border data rules along the lines of those in the EU GDPR — including an "adequacy" assessment process.

Troublingly, the Draft Bill also seeks to amend a few most celebrated rights of Indian democracy: the right to information. The Draft Bill seeks to amend the Right to Information Act, which has been a dominant factor to ensure transparency in the functioning of the state. The additional language proposed by this bill to add to the existing Right to Information Act raises significant dangers, especially of government departments much more actively seeking to refuse right to

information requests. This would unnecessarily frustrate this landmark law's effectiveness in ensuring government transparency and public sector accountability.

Exemptions for the state in the name of "security of state" and "exercise of state functions", along with the lack of surveillance reform, has kept a huge void in the Draft Bill in relation to the privacy rights of users vis-a-vis the state. These overbroad exemptions and the lack of surveillance reform signal a surveillance creep in the data protection regime in India, and this is very concerning given the impact on almost a billion users. This is especially troubling since the Srikrishna Committee report acknowledged that existing Indian surveillance law and government practices may not be compliant with the strengthened tests for fundamental rights review laid down by the Indian Supreme Court in its fundamental right to privacy ruling in August 2017. Despite this acknowledgement, neither the Draft Bill nor the report contain legislative language to reform and tighten Indian surveillance and investigatory powers.

The Draft Bill proposes to establish a Data Protection Authority to oversee, supervise, and enforce data protection measures and policy in India. There are multiple concerns regarding the independence of the Authority, as well as ambiguities regarding the processes and jurisdiction of various departments within the Authority. Independence, accountability, and clarity are important for such an important entity, and more needs to be done to provide the Authority with such independence and clarity.

Amidst discussions of the pros and cons of the Draft Bill, users and activists in India are pushing for amendments before it is presented in the Parliament. The #SaveOurPrivacy initiative — an Indian advocacy movement founded in support of a model draft law called the Indian Privacy Code, 2018 — is also gaining steam in India. The model law — drafted by a committee of volunteer lawyers from the digital rights community in India — covers the specific and nuanced issues of privacy, data protection, interception, and surveillance, and builds on seven privacy principles the drafting committee identified as the pillars of the legislative effort. This movement aims to push the government in India to finally do something, to make sure that the outcome is one which protects the large base of users in India, and to institute proper mechanisms to protect the fundamental right to privacy in India.

The Srikrishna Committee report and its Draft Bill — which must be acted on by the Government of India and finally considered in Parliament — requires further work to ensure that it truly protects the rights of users. Access Now stands ready to assist in this regard.

CONTACT:

For any queries, please reach out to **Akash Kumar Singh (akash@accessnow.org)**, **Naman M. Aggarwal (naman@accessnow.org)**, and **Raman Jit Singh Chima (raman@accessnow.org)**.

accessnow

Access Now defends and extends the digital rights of users at risk around the world. By combining direct technical support, comprehensive policy engagement, global advocacy, grassroots grantmaking, and convenings such as RightsCon, we fight for human rights in the digital age.

https://www.accessnow.org