The Centre for Internet and Society's Comments and Recommendations to the: Indian Privacy Code, 2018

By: Shweta Mohandas, Elonnai Hickok, Amber Sinha and Shruti Trikanand

The debate surrounding privacy has in recent times gained momentum due to the Aadhaar judgement and the growing concerns around the use of personal data by corporations and governments. As India moves towards greater digitization, and technology becomes even more pervasive, there is a need to ensure the privacy of the individual as well as hold the private and public sector accountable for the use of personal data. Towards enabling public discourse and furthering the development a privacy framework for India, a group of lawyers and policy analysts backed by the Internet Freedom Foundation (IFF) have put together a draft a citizen's bill encompassing a citizen centric privacy code that is based on seven guiding principles.[1] This draft builds on the Citizens Privacy Bill, 2013 that had been drafted by CIS on the basis of a series of roundtables conducted in India.[2] Privacy is one of the key areas of research at CIS and we welcome this initiative and hope that our comments make the Act a stronger embodiment of the right to privacy.

Section by Section Recommendations

Preamble

Comment: The Preamble specifies that the need for privacy has increased in the digital age, with the emergence of big data analytics.

Recommendation: It could instead be worded as 'with the emergence of technologies such as big data analytics', so as to recognize the impact of multiple technologies and processes including big data analytics.

Comment: The Preamble states that it is necessary for good governance that all interceptions of communication and surveillance be conducted in a systematic and transparent manner subservient to the rule of law.

Recommendation: The word 'systematic' is out of place, and can be interpreted incorrectly. It could instead be replaced with words such as 'necessary', 'proportionate', 'specific', and 'narrow', which would be more appropriate in this context.

[1] These seven principles include: Right to Access, Right to Rectification, Right to Erasure And Destruction of Personal Data,Right to Restriction Of Processing, Right to Object, Right to Portability of Personal Data,Right to Seek Exemption from Automated Decision-Making.
[2]The Privacy (Protection) Bill 2013: A Citizen's Draft, Bhairav Acharya, Centre for Internet & Society, https://cis-india.org/internet-governance/blog/privacy-protection-bill-2013-citizens-draft

Chapter 1

Preliminary

Section 2: This Section defines the terms used in the Act.

Comment: Some of the terms are incomplete and a few of the terms used in the Act have not been included in the list of definitions.

Recommendations:

- The term “effective consent” needs to be defined. The term is first used in the Proviso to Section 7(2), which states “Provided that effective consent can only be said to have been obtained where...:”It is crucial that the Act defines effective consent especially when it is with respect to sensitive data.

- The term “open data” needs to be defined. The term is first used in Section 5 that states the exemptions to the right to privacy. Subsection 1 clause ii states as follows “the collection, storage, processing or dissemination by a natural person of personal data for a strictly non-commercial purposes which may be classified as open data by the Privacy Commission”. Hence the term open data needs to be defined in order to ensure that there is no ambiguity in terms of what open data means.

- The Act does not define “erasure”, although the term erasure does come under the definition of destroy (Section 2(1)(p)). There are some provisions that use the word erasure , hence if erasure and destruction mean different acts then the term erasure needs to be defined, otherwise in order to maintain uniformity the sections where erasure is used could be substituted with the term “destroy” as defined under this Act.

- The definition of “sensitive personal data” does not include location data and identification numbers. The definition of sensitive data must include location data as the Act also deals in depth with surveillance. With respect to identification numbers, the Act needs to consider identification numbers (eg. the Aadhaar number, PAN number etc.) as sensitive information as this number is linked to a person's identity and can reveal sensitive personal data such as name, age, location, biometrics etc. Example can be taken from Section 4(1) of the GDPR[3] which identifies location data as well as identification numbers as sensitive personal data along with other identifies such as biometric data, gender race etc.

- The Act defines consent as the “unambiguous indication of a data subject’s agreement” however, the definition does not indicate that there needs to be an informed consent. Hence the revised definition could read as follows “the informed and unambiguous indication of a data subject’s agreement”. It is also unclear how

[3]General Data Protection Regulation, available at https://gdpr-info.eu/art-4-gdpr/.

this definition of consent relates to ‘effective consent’. This relationship needs to be clarified.

- The Act defines ‘data controller’ in Section 2(1)(l) as “ any person including appropriate government..”. In order to remove any ambiguity over the definition of the term person, the definition could specify that the term person means any natural or legal person.

- The Act defines ‘data processor’ in Section (2(1)(m) as “means any person including appropriate government”. In order to remove any ambiguity over the definition of the term ‘any person’, the definition could specify that the term person means any natural or legal person.

CHAPTER II

Right to Privacy

Section 5: This section provides exemption to the rights to privacy**.**

Comment: Section 5(1)(ii) states that the collection, storage, processing or dissemination by a natural person of personal data for a strictly non-commercial purposes are exempted from the provisions of the right to privacy. This clause also states that this data may be classified as open data by the Privacy Commission. This section hence provides individuals the immunity from collection, storage, processing and dissemination of data of another person. However this provision fails to state what specific activities qualify as non commercial use.

Recommendation: This provision could potentially be strengthened by specifying that the use must be in the public interest. The other issue with this subsection is that it fails to define open data. If open data was to be examined using its common definition i.e “data that can be freely used, modified, and shared by anyone for any purpose”[4] then this section becomes highly problematic. As a simple interpretation would mean that any personal data that is collected, stored, processed or disseminated by a natural person can possibly become available to anyone. Beyond this, India has an existing framework governing open data. Ideally the privacy commissioner could work closely with government departments to ensure that open data practices in India are in compliance with the privacy law.

[4] Antonio Vetro, Open Data Quality Measurement Framework: Definition and Application to Open Government Data, available at https://www.sciencedirect.com/science/article/pii/S0740624X16300132

CHAPTER III

Protection of Personal Data

PART A

Notice by data controller

Section 6: This section specifies the obligations to be followed by data controllers in their communication, to maintain transparency and lays down provisions that all communications by Data Controllers need to be complied with.

Comment: There seems to be a error in the *Proviso* to this section. The proviso states "Provided that all communications by the Data Controllers including but not limited to the rights of Data Subjects under this part **shall may be** refused when the Data Controller is, unable to identify or has a well founded basis for reasonable doubts as to the identity of the Data Subject or are manifestly unfounded, excessive and repetitive, with respect to the information sought by the Data Subject ".

Recommendation: The proviso could read as follows "The proviso states "Provided that all communications by the Data Controllers including but not limited to the rights of Data Subjects under this part ***may*** be refused when the Data Controller is…". We suggest the use of the 'may' as this makes the provision less limiting to the rights of the data controller. Additionally, it is not completely clear what 'included but not limited to...' would entail. This could be clarified further.

PART B

CONSENT OF DATA SUBJECTS

Section 10: This section talks about the collection of personal data.

Comment: Section 10(3) lays down the information that a person must provide before collecting the personal data of an individual.

Comment: Section 10(3)(xi) states as follows "the time and manner in which it will be destroyed, or the criteria used to Personal data collected in pursuance of a grant of consent by the data subject to whom it pertains shall, if that consent is subsequently withdrawn for any reason, be destroyed forthwith: determine that time period;". There seems to be a problem with the sentence construction and the rather complex sentence is difficult to understand.

Recommendation: This section could be reworked in such as way that two conditions are clear, one - the time and manner in which the data will be destroyed and two the status of the data once consent is withdrawn.

Comment: Section 10(3)(xiii) states that the identity and contact details of the data controller and data processor must be provided. However it fails to state that the data controller should provide more details with regard to the process for grievance redressal. It does not provide guidance on what type of information needs to go into this notice and the process of redressal. This could lead to very broad disclosures about the existence of redress mechanisms without providing individuals an effective avenue to pursue.

Recommendation: As part of the requirement for providing the procedure for redress, data controllers could specifically be required to provide the details of the Privacy Officers, privacy commissioner, as well as provide more information on the redressal mechanisms and the process necessary to follow.

Section 11: This section lays out the provisions where collection of personal data without prior consent is possible.

Comment: Section 11 states “Personal data may be collected or received from a third party by a Data Controller the prior consent of the data subject only if it is:..”. However as the title of the section suggests the sentence could indicate the situations where it is permissible to collect personal data without prior consent from the data subject”. Hence the word “without” is missing from the sentence. Additionally the sentence could state that the personal data may be collected or received directly from an individual or from a third party as it is possible to directly collect personal data from an individual without consent.

Recommendation: The sentence could read as “Personal data may be collected or received from an **individual or a third party** by a Data Controller ***without*** the prior consent of the data subject only if it is:..”.

Comment: Section 11(1)(i) states that the collection of personal data without prior consent when it is “necessary for the provision of an emergency medical service or essential services”. However it does not specify the kind or severity of the medical emergency.

Recommendation: In addition to medical emergency another exception could be made for imminent threats to life.

Section 12: This section details the Special provisions in respect of data collected prior to the commencement of this Act.

Comment: This section states that all data collected, processed and stored by data controllers and data processors prior to the date on which this Act comes into force shall be destroyed within a period of two years from the date on which this Act comes into force. Unless consent is obtained afresh within two years or that the personal data has been anonymised in such a manner to make re-identification of the data subject absolutely impossible. However this process can be highly difficult and impractical in terms of it being

time consuming, expensive particularly, in cases of analog collections of data. This is especially problematic in cases where the controller cannot seek consent of the data subject due to change in address or inavailability or death. This will also be problematic in cases of digitized government records.

Recommendation: We suggest three ways in which the issue of data collected prior to the Act can be handled. One way is to make a distinction on the data based on whether the data controller has specified the purpose of the collection before collecting the data. If the purpose was not defined then the data can be deleted or anonymised. Hence there is no need to collect the data afresh for all the cases. The purpose of the data can also be intimated to the data subject at a later stage and the data subject can choose if they would like the controller to store or process the data.The second way is by seeking consent afresh only for the sensitive data. Lastly, the data controller could be permitted to retain records of data, but must necessarily obtain fresh consent before using them. By not having a blanket provision of retrospective data deletion the Act can address situations where deletion is complicated or might have a potential negative impact by allowing storage, deletion, or anonymisation of data based on its purpose and kind.

Comment: Section (2)(1)(i) of the Act states that the data will not be destroyed provided that **effective consent** is obtained afresh within two years. However as stated earlier the Act does not define effective consent.

Recommendation: The term **effective consent** needs to be defined in order to bring clarity to this provision.

PART C

FURTHER LIMITATIONS ON DATA CONTROLLERS

Section 16: This section deals with the security of personal data and duty of confidentiality.

Comment: Section 16(2) states " Any person who collects, receives, stores, processes or otherwise handles any personal data shall be subject to a duty of confidentiality and secrecy in respect of it." Similarly Section 16(3) states "data controllers and data processors shall be subject to a duty of confidentiality and secrecy in respect of personal data in their possession or control. However apart from the duty of confidentiality and secrecy the data collectors and processors could also have a duty to maintain the security of the data." Though it is important for confidentiality and secrecy to be maintained, ensuring security requires adequate and effective technical controls to be in place.

Recommendation: This section could also emphasise on the duty of the data controllers to ensure the security of the data. The breach notification could include details about data that is impacted by a breach or attach as well as the technical details of the infrastructure compromised.

Section 17: This section details the conditions for the transfer of personal data outside the territory of India.

Comment: Section 17 allows a transfer of personal data outside the territory of India in 3 situations- If the Central Government issues a notification deciding that the country/international organization in question can ensure an adequate level of protection, compatible with privacy principles contained in this Act; if the transfer is pursuant to an agreement which binds the recipient of the data to similar or stronger conditions in relation to handling the data; or if there are appropriate legal instruments and safeguards in place, to the satisfaction of the data controller. However, there is no clarification for what would constitute 'adequate' or 'appropriate' protection, and it does not account for situations in which the Government has not yet notified a country/organisation as ensuring adequate protection. In comparison, the GDPR, in Chapter V[5], contains factors that must be considered when determining adequacy of protection, including relevant legislation and data protection rules, the existence of independent supervisory authorities, and international commitments or obligations of the country/organization. Additionally, the GDPR allows data transfer even in the absence of the determination of such protection in certain instances, including the use of standard data protection clauses, that have been adopted or approved by the Commission; legally binding instruments between public authorities; approved code of conduct, etc. Additionally, it allows derogations from these measures in certain situations: when the data subject expressly agrees, despite being informed of the risks; or if the transfer is necessary for conclusion of contract between data subject and controller, or controller and third party in the interest of data subject; or if the transfer is necessary for reasons of public interest, etc. No such circumstances are accounted for in Section 17.

Recommendation: Additionally, data controllers and processors could be provided with a period to allow them to align their policies towards the new legislation. Making these provisions operational as soon as the Act is commenced might put the controllers or processors guilty of involuntary breaching the provisions of the Act.

Section 19: This section states the special provisions for sensitive personal data.

Comment: Section 19(2) states that in addition to the requirements set out under sub-clause (1), the Privacy Commission shall set out additional protections in respect of:i.sensitive personal data relating to data subjects who are minors; ii.biometric and deoxyribonucleic acid data; and iii.financial and credit data.This however creates additional categories of sensitive data apart from the ones that have already been created.[6] These additional categories can result in confusion and errors.

[5] General Data Protection Regulation, available at https://gdpr-info.eu/chapter-5/.

[6] Sensitive personal data under Section 2(bb) includes, biometric data; deoxyribonucleic acid data; sexual preferences and practices;medical history and health information;political affiliation; membership of a political, cultural, social organisations including but not limited to a trade union as defined under Section 2(h) of the Trade Union Act, 1926;ethnicity, religion, race or caste; and financial and credit information, including financial history and transactions.

Recommendation: Sensitive data must not be further categorised as this can lead to confusion and errors. Hence all sensitive data could be subject to the same level of protection.

Section 20: This section states the special provisions for data impact assessment.

Comment: This section states that all data impact assessment reports will be submitted periodically to the State Privacy commission. This section does not make provisions for instances of circumstances in which such records may be made public. Additionally the data impact assessment could also include a human rights impact assessment.

Recommendation: The section could also have provisions for making the records of the impact assessment or relevant parts of the assessment public. This will ensure that the data controllers / processors are subjected to a standard of accountability and transparency. Additionally as privacy is linked to human rights the data impact assessment could also include a human rights impact assessment. The Act could further clarify the process for submission to State Privacy Commissions and potential access by the Central Privacy Commission to provide clarity in process.

Section 20 requires controllers who use new technology to assess the risks to the data protection rights that occur from processing. 'New technology' is defined to include pre-existing technology that is used anew. Additionally, the reports are required to be sent to the State Privacy Commission periodically. However, there is no clarification on the situations in which such an assessment becomes necessary, or whether all technology must undergo such an assessment before their use. Additionally, the differentiation between different data processing activities based on whether the data processing is incidental or a part of the functioning needs to be clarified. This differentiation is necessary as there are some data processors and controllers who need the data to function; for instance an ecommerce site would require your name and address to deliver the goods, although these sites do not process the data to make decisions. This can be compared to a credit rating agency that is using the data to make decisions as to who will be given a loan based on their creditworthiness. Example can taken from the GDPR, which in Article 35, specifies instances in which a data impact assessment is necessary: where a new technology, that is likely to result in a high risk to the rights of persons, is used; where personal aspects related to natural persons are processed automatically, including profiling; where processing of special categories of data (including data revealing ethnic/racial origin, sexual orientation etc), biometric/genetic data; where data relating to criminal convictions is processed; and with data concerning the monitoring of publicly accessible areas. Additionally, there is no requirement to publish the report, or send it to the supervising authority, but the controller is required to review the processor's operations to ensure its compliance with the assessment report.

Recommendation: The reports could be sent to a central authority, which according to this Act is the Privacy Commission, along with the State Privacy Commission. Additionally there needs to be a differentiation between the incidental and express use of data. The data processors must be given at least a period of one year after the commencement of the Act to present their impact assessment report. This period is required for the processors to align themselves with the provisions of the Act as well as conduct capacity building initiatives.

PART C

RIGHTS OF A DATA SUBJECT

Section 21: This section explains the right of the data subject with regard to accessing her data. It states that the data subject has the right to obtain from the data controller information as to whether any personal data concerning her is collected or processed. The data controller also has to not only provide access to such information but also the personal data that has been collected or processed.

Comment: This section does not provide the data subject the right to seek information about security breaches.

Recommendation: This section could state that the data subject has the right to seek information about any security breaches that might have compromised her data (through theft, loss, leaks etc.). This could also include steps taken by the data controller to address the immediate breach as well as steps to minimise the occurrence of such breaches in the future.[7]

CHAPTER IV

INTERCEPTION AND SURVEILLANCE

Section 28: This section lists out the special provisions for competent organizations.

Comment: Section 28(1) states ”all provisions of Chapter III shall apply to personal data collected, processed, stored, transferred or disclosed by competent organizations unless when done as per the provisions under this chapter ”. This does not make provisions for other categories of data such as sensitive data.

Recommendation: This section needs to include not just personal data but also sensitive data, in order to ensure that all types of data are protected under this Act.

Section 30: This section states the provisions for prior authorisation by the appropriate Surveillance and Interception Review Tribunal.

Comment: Section 30(5) states “any interception involving the infringement of the privacy of individuals who are not the subject of the intended interception, or where communications relate to **medical, journalistic, parliamentary or legally privileged material** may be involved, shall satisfy additional conditions including the provision of specific prior justification in writing to the Office for Surveillance Reform of the Privacy Commission as to

[7] Submission to the Committee of Experts on a Data Protection Framework for India, Amber Sinha, Centre for Internet & Society, available at https://cis-india.org/internet-governance/files/data-protection-submission

the necessity for the interception and the safeguards providing for minimizing the material intercepted to the greatest extent possible and the destruction of all such material that is not strictly necessary to the purpose of the interception." This section needs to state why these categories of communication are more sensitive than others. Additionally, interceptions typically target people and not topics of communication - thus medical may be part of a conversation between two construction workers and a doctor will communicate about finances.

Recommendation: The section could instead of singling out "medical, journalistic, parliamentary or legally privileged material" state that "any interception involving the infringement of the privacy of individuals who are not the subject of the intended interception may be involved, shall satisfy additional conditions including the provision of specific prior justification in writing to the Office for Surveillance Reform of the Privacy Commission.

Section 37: This section details the bar against surveillance.

Comment: Section 37(1) states that "no person shall order or carry out, or cause or assist the ordering or carrying out of, any surveillance of another person". The section also prohibits indiscriminate monitoring, or mass surveillance, unless it is necessary and proportionate to the stated purpose. However, it is unclear whether this prohibits surveillance by a resident of their own residential property, which is allowed in Section 5, as the same could also fall within 'indiscriminate monitoring/mass surveillance'. For instance, in the case of a camera installed in a residential property, which is outward facing, and therefore captures footage of the road/public space.

Recommendation: The Act needs to bring more clarity with regard to surveillance especially with respect to CCTV cameras that are installed in private places, but record public spaces such as public roads. The Act could have provisions that clearly define the use of CCTV cameras in order to ensure that cameras installed in private spaces are not used for carrying out mass surveillance. Further, the Act could address the use of emerging techniques and technology such as facial recognition technologies, that often rely on publicly available data.

CHAPTER V

THE PRIVACY COMMISSION

Section 53: This section details the powers and functions of the Privacy Commission.

Comment: Section 53(2)(xiv) states that the Privacy Commission shall publish periodic reports "providing description of performance, findings, conclusions or recommendations of any or all of the functions assigned to the Privacy Commission". However this Section does not make provisions for such reporting to happen annually and to make them publicly

available, as well as contain details including financial aspects of matters contained within the Act.

Recommendation: The functions could include a duty to disclose the information regarding the functioning and financial aspects of matters contained within the Act. Categories that could be included in such reports include: the number of data controllers, number of data processors, number of breaches detected and mitigated etc.

CHAPTER IX

OFFENCES AND PENALTIES

Sections 73 to 80: These sections lay out the different punishments for controlling and processing data in contravention to the provisions of this Act.

Comment: These sections, while laying out different punishments for controlling and processing data in contravention to the provisions of this Act, mets out a fine extending upto Rs. 10 crore. This is problematic as it does not base these penalties on the finer aspects of proportionality, such as offences that are not as serious as the others.

Recommendation: There could be a graded approach to the penalties based on the degree of severity of the offence.This could be in the form of name and shame, warnings and penalties that can be graded based on the degree of the offence.

Additional thoughts: As India moves to a digital future there is a need for laws to be in place to ensure that individual's rights are not violated. By riding on the push to digitization, and emerging technologies such as AI, a strong all encompassing privacy legislation can allow India to leapfrog and use these emerging technologies for the benefit of the citizens without violating their privacy. A robust legislation can also ensure a level playing field for data driven enterprises within a framework of openness, fairness, accountability and transparency.