THE CENTRE FOR internet & society

Rethinking National Privacy Principles

Evaluating Principles for India's Proposed Data Protection Law

By **AMBER SINHA**
Edited by **ELONNAI HICKOK** and **VIPUL KHARBANDA**

The Centre for Internet and Society, India

Designed by **Saumyaa Naidu**

Background

This report is intended to be the first part in a series of white papers that CIS will publish which seeks to contribute to the discussions around the enactment of a privacy legislation in India. In subsequent pieces we will focus on subjects such as regulatory framework to implement, supervise and enforce privacy principles, and principles to regulate surveillance in India under a privacy law. This analysis intends to build on the substantial work done in the formulation of the National Privacy Principles by the Committee of Experts led by Justice AP Shah.[1] This brief, hopes to evaluate the National Privacy Principles and the assertion by the Committee that right to privacy be considered a fundamental right under the Indian Constitution. The national privacy principles have been revisited in light of technological developments such as big data, Internet of Things, algorithmic decision making and artificial intelligence which are increasingly playing a greater role in the collection and processing of personal data of individuals, its analysis and decisions taken on the basis of such analysis. The solutions and principles articulated in this report are intended to provide starting points for a meaningful and nuanced discussion on how we need to rethink the privacy principles that should inform the data protection law in India.

Our approach in this report draws heavily from Lawrence Lessig's dictum that 'code is law' and the recognition that architecture and norms can play and equally important role in regulation as law. Therefore, regulatory intervention for technology need not only deal with regulation of technology, but also how technology may be leveraged for regulation.[2] As is the case with the regulation of most technological processes, a multi pronged approach which includes technical solutions, norms and principles is required in addition to legislation, in order to regulate and enforce collection and processing of personal data in India that respects and enables the right to privacy. In that light we have included under each principle a clear articulation of rights that arise to data subjects as a result of the principle. In this report, we discuss present day challenges to each principle, provide recommendations towards aspects that need to be incorporated and/or accounted for in the principle, and discuss norms, standards, and technological solutions that can be adopted to implement or enhance the principles.

1 The full text of the Report of Group of Experts on Privacy is available at **http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf**.

2 Lawrence Lessig, Code: Version 2.0 (2006); Joel R. Reidenberg, Lex Informatica: The Formulation of Information Policy Rules Through Technology, 76 TEX. L. REV. 553 (1998).

1. Privacy Principles

A. Notice[3]

Challenges

- **Broad language**: The Notice principle in the National Privacy Principles requires that privacy policies must be 'in clear and concise language.' The requirement of "clear" and "concise" is overly broad and leaves the door open for extremely long notices, often not available in most vernacular languages. In practice many privacy policies suffer from the following problems which are not addressed by the Notice principles: a) overkill – long and repetitive text in small print, b) irrelevance – describing situations of little concern to most consumers, c) opacity – broad terms reflect the truth that is impossible to track and control all the information collected and stored, d) non-comparability – simplification required to achieve comparability will lead to compromising accuracy, and e) inflexibility – failure to keep pace with new business models.[4]
- **Carte blanche consent**: Often privacy notices are used as one time consent forms which allow the data controllers all rights over the data by taking blanket consents from data subjects often not a collection but at the stage of installation or through implied notice in the forms of privacy policy on a webpage. Further, only the data collectors have responsibility for obtaining consent, and data controllers who obtain personal data from third party sources are not subject to any consent or transparency requirements.[5]

3 **Principle 1 - Notice in National Privacy Principles**: *A data controller shall give simple to understand notice of its information practices to all individuals, in clear and concise language, before any personal information is collected from them. Such notices should include:*

a) During Collection

- *What personal information is being collected;*
- *Purposes for which personal information is being collected;*
- *Uses of collected personal information;*
- *Whether or not personal information may be disclosed to third persons;*
- *Security safeguards established by the data controller in relation to the personal information;*
- *Processes available to data subjects to access and correct their own personal information;*
- *Contact details of the privacy officers and SRO ombudsmen for filing complaints.*

b) Other Notices

- *Data breaches must be notified to affected individuals and the commissioner when applicable.*
- *Individuals must be notified of any legal access to their personal information after the purposes of the access have been met.*
- *Individuals must be notified of changes in the data controller's privacy policy.*
- *Any other information deemed necessary by the appropriate authority in the interest of the privacy of data subjects.*

4 Scott Mason and Amber Sinha, A critique of consent in Informational privacy, Centre for Internet and Society, January 2016, available at **https://cis-india.org/internet-governance/blog/a-critique-of-consent-in-information-privacy**.

5 Daniel Solove, "Privacy self-management and consent dilemma," Harvard Law Review 126, (2013): 1880.

Recommendations for Principle

Timing of the privacy notice

The privacy notice shall be provided at the time of collection from the data subject, and, where the personal data are obtained from another source, at the time of receipt of data from such source.[6] Further, data protection authorities must explore, incentivise and mandate evolving standards and norms for provision of privacy notices in a staggered manner which ensure repetition of notice when the activity in question is relevant to the privacy interests of the individual.[7]

Contents of the privacy notice

The privacy notices should include the following information:

1. *What personal information is being collected;*
2. *Name and contact details of the entity collecting the data;*
3. *Purposes for which personal information is being collected;*
4. *Uses of collected personal information;*
5. *Whether or not personal information may be disclosed to third persons, and the third party recipients or categories of recipients of the personal data;*
6. *The period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period*
7. *The manner in which it may be accessed, verified and modified;*
8. *The procedure for recourse in case of any grievance in relation to collection and processing of data*
9. *Security safeguards established by the data controller in relation to the personal information;*
10. *Contact details of the privacy officers and ombudsmen for filing complaints.*

Form of the privacy notice

The privacy notice should be easily accessible, easy to understand, in clear, plain, intelligible, easily legible and concise language that a reasonable person without any legal or technical training can comprehend, and must follow any standards or formats that the data protection authority or the relevant sectoral regulatory bodies specify. The privacy notice ought to be a meaningful overview of the intended processing of the data collected.

Recommended Rights

All persons shall have a right to seek an easily accessible, easy to understand privacy notice in clear, plain, intelligible, easily legible and concise language prior to collection of any personal data from them.

6 Traditionally, the notice and consent regime only involves notification from the data collector directly collecting personal data from the data subject. Given the indiscriminate sharing of data in the age of big data, we suggest introducing another layer of notice, wherein each data controller in receipt of personal data from other service providers must notify the data subject as well. This additional layer of notice is also reflected in Article 14 of the GDPR.

7 While we do not suggest adoption of prescriptive formats for providing notice, however, it is expected that the regulator plays an active role in the evolution and adoption of privacy enhancing privacy notices as standards.

B. Consent and Choice[8]

Challenges

- **Lack of a real choice**: The traditional choice against the collection of personal data that users have had access to, at least in theory, is the option to 'opt-out' of certain services. This draws from the free market theory that individuals exercise their free will when they use services and always have the option of opting out, thus, arguing against regulation but relying on the collective wisdom of the market to weed out harms. The notion that the provision of data should be a matter of personal choice on the part of the individual and that the individuals can, if they chose decide to 'opt-out' of data collection, for example by ceasing use of a particular service, is an important component of privacy and data protection frameworks.[9] The proliferation of internet-enabled devices, their integration into the built environment and the real-time nature of data collection and analysis however are beginning to undermine this concept. For many critics of Big Data, the ubiquity of data collection as well as the compulsory provision of data as a prerequisite for the access and use of many key online services, is making opting-out of data collection not only impractical but in some cases impossible. As online connectivity becomes increasingly important to participation in modern life, the choice to withdraw completely is becoming less of a genuine choice.[10] Further, Mere silence or inaction in the case of default settings should not be valid consent.[11]
- **Lack of capacity to take informed decisions**: Even those who understand privacy notices and are capable of making rational choices about it, cannot conceptualize how their data will be aggregated and possibly used or re-used. Seemingly innocuous bits of data revealed at different stages could be combined to reveal sensitive information about the individual. Daniel Solove, the John Marshall Harlan Research Professor of Law at the George Washington University Law School, in his book, "The Digital Person", calls it the aggregation effect. He argues that the ingenuity of the data mining techniques and the insights and predictions that could be made by it render any cost-benefit analysis that an individual could make ineffectual.[12]

---

8 **Principle 2 - Choice and Consent in National Privacy Principles**: *A data controller shall give individuals choices (opt-in/opt-out) with regard to providing their personal information, and take individual consent only after providing notice of its information practices. Only after consent has been taken will the data controller collect, process, use, or disclose such information to third parties, except in the case of authorized agencies. When provision of information is mandated by law, it should be in compliance with all other National Privacy Principles. Information collected on a mandatory basis should be anonymized within a reasonable timeframe if published in public databases. As long as the additional transactions are performed within the purpose limitation, fresh consent will not be required. The data subject shall, at any time while availing the services or otherwise, also have an option to withdraw his/her consent given earlier to the data controller. In such cases the data controller shall have the option not to provide goods or services for which the said information was sought if such information is necessary for providing the goods or services. In exceptional cases, where it is not possible to provide the service with choice and consent, then choice and consent should not be required.*

9 Fred Cate, Viktor Schoenberger, Notice and Consent in a world of Big Data, available at **http://idpl.oxfordjournals.org/content/3/2/67.abstract**.

10 **https://www.ftc.gov/system/files/documents/public_comments/2014/08/00015-92370.pdf**

11 Anca D. Chirita, The Rise of Big Data and the Loss of Privacy (June 15, 2016). Personal Data in Competition, Consumer Protection and IP Law - Towards a Holistic Approach? (eds) Bakhoum, M., Gallego Conde, B., Mackenordt, M.O. & Surblyte, G. Berlin Heidelberg, Springer, 2018, Forthcoming; Durham Law School Research Paper (2016), available at SSRN: **https://ssrn.com/abstract=2795992**

12 Daniel Solove, The Digital Person: Technology and Privacy in the Information Age, NYU Press, 2006.

- **Lack of clear exceptions**: The principle allows for services to be provided in exceptional cases where it is not possible to take consent of the individual. If such a situation arises the principle should clarify that retroactive consent is necessary. Such exceptional cases should also be clearly defined. If a new exceptional case is needed, this determination should be taken by the Privacy Commissioner.

Recommendations for Principle

Timing of consent

A data controller shall obtain the informed consent of the data subject to the processing of her personal data prior to the collection and processing of the data.

Nature of consent

Informed consent should be voluntarily given through an express and affirmative act on the part of the data subject which establishes a freely given, specific, informed and unambiguous indication of the data subject's agreement. It shall be the data controller's' responsibility to demonstrate consent. When the processing has multiple purposes, consent should be given for all of them.[13]

No one time consent

When the purposes for which personal data was collected are modified or expanded subsequent to its collection, consent will be deemed to be specific only if it is obtained afresh in respect of that modification or expansion, prior to any use of that data for the modified or expanded purposes.

Consent not a tool of coercion

If data being collected is merely incidental and not essential to the service being provided, then agreeing to a privacy policy that mandates collection of such data should not be a condition precedent.[14]

Exceptions

In the following circumstances only to the extent absolutely necessary, personal data may be collected and processed in the absence of a informed consent: (a) vital interest of data subject (question of life and death such as medical emergencies) (b) legitimate interest of the data controller, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject.[15]

Recommended Rights

Right to withdraw

The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.

13 This principle seeks to address to the issue of implied consent where privacy policies available on web-pages are seen as valid contracts without any affirmative action on the part of the users.

14 This principle respond to the concerns arising out of the negligence of the data minimisation principle, and data is collected often without having a reasonable nexus to the purpose of data collection.

15 Vital interest and legitimate interest have been articulated as exception in the EU Directive and the GDPR.

The data subject shall have a right to seek all information reasonably necessary to decide whether to withdraw his or her consent, including not limited to purposes for which their data is being processed, the manner in which such processing is being conducted, the duration which the data collector intends to process and retain the data.

Right against unfair denial of service

All persons shall have the right against unfair denial of services on the grounds that such persons do not agree to share data, not essential but merely incidental to the provision of service, being made a precondition to the provision of services.[16]

C. Collection and Purpose Limitation[17]

Challenges

- **Unknown purposes**: With present day data practices, it becomes difficult to pin down a particular purpose for companies when it comes to data collection and usage. The thrust of big data is to collect as much information as possible and allow the use and purpose for the information to emerge. Big data proponents argue that the utility of data is no longer restricted to the primary purpose for which it is collected but can be used to provide all kinds of secondary services and resources, reduce waste, increase efficiency and improve decision-making.[18] These kinds of positive externalities are only made possible by the reprocessing of data.[19]
- **Vague purposes**: In practice, reasons often given in company ToS and privacy policies, typically include phrases such as, 'for marketing purposes' or 'to improve the user experience' that are vague and open to interpretation. These practices are intended to allow the data controllers to use the data for undefined purposes.[20]

Recommendations for Principle

Collection limitation

Personal data collected and processed by data controllers should be adequate and relevant to the purposes for which they are processed. The data collected shall be necessary for the achievement of a purpose that is connected to a stated function of the person seeking its collection.

---

16 This principle responds to the existing issues with the Opt-out principle where opting out is often not

17 **Principle 3 - Collection Principle in National Privacy Principles**: *A data controller shall only collect personal information from data subjects as is necessary for the purposes identified for such collection, regarding which notice has been provided and consent of the individual taken. Such collection shall be through lawful and fair means.*

Principle 4 - Purpose Limitation in National Privacy Principles: *Personal data collected and processed by data controllers should be adequate and relevant to the purposes for which they are processed. A data controller shall collect, process, disclose, make available, or otherwise use personal information only for the purposes as stated in the notice after taking consent of individuals. If there is a change of purpose, this must be notified to the individual. After personal information has been used in accordance with the identified purpose it should be destroyed as per the identified procedures. Data retention mandates by the government should be in compliance with the National Privacy Principles.*

18 Viktor Mayer Schoenberger and Kenneth Cukier, Big Data: A Revolution that will transform how we live, work and think" John Murray, London, 2013.

19 *Ibid* at 153.

20 *Supra* Note 2.

Purpose limitation

The collection of personal data pursuant of the consent of the data subject will be valid only if it is obtained in respect of the purposes and duration strictly necessary to provide the product or service in relation to which personal data is sought to be collected, processed or disclosed. A data controller shall collect, process, disclose, make available, or otherwise use personal information only for the purposes as stated in the notice after taking consent of individuals. If there is a change of purpose, this must be notified to the individual, and only after the individual has consented to the new purpose, should the data be processed for such purposes. After personal information has been used in accordance with the identified purpose it should be destroyed as per the identified procedures.

Processing under legitimate interest[21]

The data controller may process data for purposes other than those expressly consented to by the data subject in cases where it can demonstrate the existence of a legitimate interest. This legitimate interest of the data controller shall be limited by the interests of the data subject which require protection of data. Factors relevant for determining the existence of a legitimate interest shall include the reasonable expectations of data subject, whether processing leads to an adverse impact on the data subject, overriding public interest, nature of the data that are processed (sensitive or not), the relationship between the data subject and the controller and their respective positions of power, and the measures that the controller has taken to reduce the impact on the privacy of the individuals.[22]

Recommended Rights

Right to access information regarding processing under legitimate interests

All data subjects shall have the right to access the grounds on the basis of which legitimate interest principle is being used to process data beyond the purposes to which the data subject has consented. In cases where the data subject contests the legitimate interests for the processing of data by the controller for purposes for which consent of the data subject has not been taken pending the demonstration of the legitimate interest by the data controller, the data subject has the right to restrict the processing of the data in question.

D. Access, Correction,[23] Portability and Restriction

Challenges

- **Expanding the right to access**: While the original National Privacy Principles included a right to access and correction, technological advances and data economy which involves sharing of data between parties necessitates an update of the principles, along with the

21 The legitimate principle has been a part of European jurisprudence and is also reflected in the GDPR as one of the criteria for lawful processing.

22 Lokke Morael and Corien Prins, Privacy for the Homo Digitalis: Proposal for a New Regulatory Framework for Data Protection in the Light of Big Data and the Internet of Things (May 25, 2016), available at **http://dx.doi.org/10.2139/ssrn.2784123**

23 **Principle 5 - Access and Correction in National Privacy Principles**: *Individuals shall have access to personal information about them held by a data controller; shall be able to seek correction, amendments, or deletion such information where it is inaccurate; be able to confirm that a data controller holds or is processing information about them; be able to obtain from the data controller a copy of the personal data; Access and correction to personal information may not be given by the data controller if it is not, despite best efforts, possible to do so without affecting the privacy rights of another person, unless that person has explicitly consented to disclosure.*

addition of the right to restrict processing in certain circumstances. The right to access needs to be expanded and clearly articulated to include the form in which data must be provided to the individuals.

- **Scope of right to access**: With the advent of devices which collect real time and behavioral data, and big data and algorithmic technologies that analyse data to create user profiles, it important to update the principle of access to specify what kinds of data it covers. Aside from data directly provided by the individuals, data observed about the individuals which includes metadata collected by the applications must also included in the scope of the right. However, data generated or inferred by the data controllers which involves analysis of the data collected through user categorisation, profiling and or a personalisation process must not be covered by this right.
- **Greater user choice through portability rights**: Finally, there is a need for a right to data portability which includes right to transmit those data to another controller without hindrance from the controller to which the data have been provided. This would be key to enhancing user choice, incentivising good data practices and lowering the barriers to entry a market that new entrants face.

Recommendations for Principle

Implementation of access and portability

The data controllers should offer different implementation of the right to access and portability including but not limited to a direct download option and direct transmission of the data to another controller upon the request of the data subject. Access and correction to personal information may not be given by the data controller if it is not, despite best efforts, possible to do so without affecting the privacy rights of another person, unless that person has explicitly consented to disclosure.

Recommended Rights

Right to access

The data subject shall have the right to obtain from the controller access to the personal data collected and/or being processed. Additionally, the data subject can seek the purposes of the processing, the recipients or categories of third party recipient to whom the personal data have been or will be disclosed, the intended time period of which the data would be stored, details of sources where data was not obtained directly from the data subject. The data will be made available by the controller in a structured, machine-readable as well as human-readable format. This shall include both data directly collected from the data subject as well as data observed about the data subject.

Right to portability

The data subject shall the have the right to transmit those data obtained from the controller under the right to access to another controller without hindrance from the controller to which the data was originally provided.[24]

Right to correction

The data subject shall have the right to ensure from the data controller, the rectification of inaccurate or incomplete personal data, without any undue delay, especially in cases where the incompleteness or inaccuracy of the data has adverse impacts on the data subjects.

24 The right to data portability has been incorporated in the new GDPR and will be explored in greater detail in subsequent briefs.

Right to restrict processing

In cases where the accuracy or completeness of the data is contested by the data subject, the data subject has the right to restrict the processing of the data in question.[25]

E. Disclosure[26]

Challenges

- **Need for exceptions and their governance**: The principle of disclosure has been updated to include exceptions to the obligations to notify data subjects in case of law enforcement access to personal data where it may be impeded investigations. It is important that the disclosure principle address how such access to data may be governed.
- **Obligation on data recipients to notify**: Further, given that we are rapidly evolving into a data economy where data is sharing across parties, it is imperative that third parties who are recipients of the data must notify the data subjects of the receipt of data as per the Notice principle.

Recommendations for Principle

Disclosure

A data controller shall not disclose personal information to third parties, except after providing notice and seeking informed consent from the individual for such disclosure. Third parties are bound to adhere to relevant and applicable privacy principles. Disclosure for law enforcement purposes must be in accordance with the laws in force. Data controllers shall not publish or in any other way make public personal information, including personal sensitive information.

Law enforcement access to data

In case of disclosures made for law enforcement purposes, within a reasonable period of time, the data controller shall notify the data subject of such disclosures except in cases where such notifications would present a reasonable threat to the security of the state or public order, or adversely affect the prevention, investigation or prosecution of a cognisable offence. Further, in cases of such exceptions, the reasons shall be recorded in writing with the period till when the reasonable threat is anticipated to extend, on whose cessation the duty to inform must operate.[27]

25 This right adds to the principle of Opt-Out and seeks to strengthen it by formulating it as a separate right available at all times to data subjects.

26 **Principle 6 - Disclosure of Information in National Privacy Principles**: *A data controller shall only disclose personal information to third parties after providing notice and seeking informed consent from the individual for such disclosure. Third parties are bound to adhere to relevant and applicable privacy principles. Disclosure for law enforcement purposes must be in accordance with the laws in force. Data controllers shall not publish or in any other way make public personal information, including personal sensitive information.*

27 This principle draws from previous exercises in drafting laws around governance of law enforcement access to data such as the CIS Citizens Bill available at **https://cis-india.org/internet-governance/blog/privacy-protection-bill-2013-citizens-draft.**

Recommended Rights

Right to access when data indirectly obtained

All persons shall have a right to seek details as laid down in the Notice principle from any data controller about personally identifiable information about them obtained not directly from the data subject from a third party source.

F. Security[28]

Challenges

- **Growing security incidents:** Over the last few years, some of the largest companies globally such as Yahoo, LinkedIn, Dropbox, Weebly, Wendy's, Snapchat have suffered significant data breach incidents. In India, too, there have been data breaches suffered by Zomato[29] and the National Payments Corporation of India.[30]

Recommendations for Principle

Security obligations

A data controller shall take measures, including, but not restricted to, technological, physical and administrative measures, to secure the confidentiality, secrecy, integrity and safety of all information collected including but not limited to personal data, including from theft, negligence, loss or unauthorised disclosure. The security measures, as appropriate may include, without limitation: a) de-identification of personal data, b) ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident, and c) ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems.

Notification obligations

If the confidentiality, secrecy, integrity or safety of the data is violated by theft, loss, negligence, damage or destruction, or as a result of any collection, processing or disclosure contrary to these principles, or for any other reason whatsoever, as soon as the data controller becomes aware of such violation, they must notify the data subject to whom it pertains, and the regulatory bodies responsible for data protection.

Recommended Rights

Rights to access data about previous breaches

All data subjects shall have the right to seek information about the any previous instances of security breaches resulting in the theft, loss, negligence, damage or destruction of data held

---

28 **Principle 7: Security in National Privacy Principles**: *A data controller shall secure personal information that they have either collected or have in their custody, by reasonable security safeguards against loss, unauthorised access, destruction, use, processing, storage, modification, deanonymization, unauthorized disclosure [either accidental or incidental] or other reasonably foreseeable risks.*

29 **http://economictimes.indiatimes.com/small-biz/security-tech/security/zomato-hacked-security-breach-results-in-17-million-user-data-stolen/articleshow/58729251.cms**

30 **https://www.bloombergquint.com/business/2016/10/20/indias-biggest-security-breach-32-lakh-debit-cards-across-19-banks-may-have-been-compromised**

by the data controller or its agents, and the 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.[31]

G. Openness[32]

Challenges

- **Lack of Transparency**: In case of services employing automated or algorithmic decision making having a direct bearing on the users, the regulation must mandate that only appropriate statistical techniques must be used and that transparency must be ensured; that measures should be in place to correct inaccuracies and risks of errors; and that security must be ensured and discriminatory effects prevented. To minimize concerns of unauth data usage, organizations should disclose the logic underlying their decision-making processes to the extent possible without compromising their trade secrets or intellectual property rights.

Recommendations for Principle

A data controller shall take all necessary steps to implement practices, procedures, policies and systems in a manner proportional to the scale, scope, and sensitivity to the data they collect, in order to ensure compliance with the privacy principles, information regarding which shall be made in an intelligible form, using clear and plain language, available to all individuals.

Recommended Rights

Right to information

All data subjects shall have the right to seek information from data controllers about the nature of algorithmic technology in use for data processing, available information about the procedural fairness of the technology in question or comparable technologies, and any steps taken by them to minimise biases and discriminatory effects of using such practices.

H. Accountability

Challenges

- **Fiduciary responsibility of controllers**: Currently, the accountability principle only refers to the data controller's responsibility to comply with the principle. However, given the emergence of data driven business models, ubiquitous collection of data for all imaginable services, and the balance of power tilting heavily in the favor of data controllers. There is a need to establish a fiduciary relationship between data subjects and data controllers. This obligations would require data controllers to be cognizant of the impact of their data driven business models on the data subject.

---

31 Along with transparency and openness obligations, this right may also foster market competition for services providers to address security issues.

32 **Principle 8: Openness in National Privacy Principles***: A data controller shall take all necessary steps to implement practices, procedures, policies and systems in a manner proportional to the scale, scope, and sensitivity to the data they collect, in order to ensure compliance with the privacy principles, information regarding which shall be made in an intelligible form, using clear and plain language, available to all individuals.*

- **Lack of post facto governance measures**: Some experts have suggested the widening of the accountability principles to include obligations on the data controllers to ensure that data processing does not lead to any harms to the data subjects.[33] However, defining harms and its quantum can be tricky. Please refer to the Section 3 C, which deals with the harms based approaches to data protection.

Recommendations for Principle

Accountability mechanisms

The data controller shall be accountable for complying with measures which give effect to the privacy principles. Such measures should include mechanisms to implement privacy policies; including tools, training, and education; external and internal audits, and requiring organizations or overseeing bodies extend all necessary support to the regulatory body and comply with the specific and general orders of the regulatory body.

Privacy impacts assessments

Further, data controllers must conduct regular impact assessments to minimise adverse impacts, particularly those pertaining to privacy and discrimination, on the data subjects. In case of demonstrable adverse impacts on the data subjects, such impact shall be balanced against the legitimate interests of the data controllers and overriding public interest.

Recommended Rights

Right to fair treatment

All data subjects shall have the right to expect principles of fairness and accountability in processing of their data by data controllers. This right includes protection against adverse impacts on the data subjects due to biases and discriminatory effects of the data collection and processing practices.

2. Technological Solutions

As mentioned above, due to the huge role played by technology in data collection and processing practices, technical solutions which designed from the point of preserving and enhancing privacy can go a long in assisting privacy laws. While including these solutions within the scope of mandatory legal obligations may be too prescriptive, the regulator can engage with other stakeholders such as industry, academia and civil society to endorse, promote and incentivise the use of these privacy enhancing solutions. These solutions are contextual, and their efficacy may vary based on the circumstances, some of them are also in nascent stages of development; however, an active role by the regulator in recognising these practices.

A. Sticky Privacy Policies[34]

Sticky privacy policies involve cryptographic solutions in which policies can stick to data to define allowed usage and obligations as it travels across multiple parties, enabling users to improve control over their personal information. They allow the data subject to decide on

33 Rahul Matthan, "Beyond Consent: A New Paradigm for Data Protection" Takshashila Institution (July, 2017), available at **http://takshashila.org.in/wp-content/uploads/2017/07/TDD-Beyond-Consent-Data-Protection-RM-2017-03.pdf**.

34 This solution can aid the Notice and Consent principles.

a set of conditions and constraints which unambiguously lay down how her/his PII is to be used by the party receiving the data. As the data moves across multiple parties, these policies define an allowed usage and obligations, thus enhancing the control of the data owners over their personal information. They impose prohibitions and obligations such as access of third parties and the purpose for which the data is being used. These policies also allow the data owners to blacklist certain parties from gaining access to their personal information along with laying down rules such as a notice of disclosure and the deletion or minimization of data after a specified period of time.

B. Nudges to Facilitate Privacy Enhanced Choices[35]

Technical solutions being explored that ensure adequate timing of notices include sticky privacy policies and privacy nudges. Sticky policies are policies that allow the data subject to decide on a set of conditions and constraints which unambiguously lay down how her/his PII is to be used by the party receiving the data.[36] As the data moves across multiple parties, these policies define an allowed usage and obligations, thus enhancing the control of the data owners over their personal information. They impose prohibitions and obligations such as access of third parties and the purpose for which the data is being used. These policies also allow the data owners to blacklist certain parties from gaining access to their personal information along with laying down rules such as a notice of disclosure and the deletion or minimization of data after a specified period of time.[37] Privacy notices often lean towards the default of maximum data sharing. The use of default privacy notice can also be used to nudge users towards privacy enhanced choices. This could include a) a usability approach that entails designing the system in way that is most intuitive and easy for users to decide whether to provide the information, or b) a soft paternalistic approach which seeks to aid the decision-making by providing other information such as how many people would have access to the information.[38] In case of privacy nudges, the insights from cognitive science, particularly using the theory of nudge would be an acceptable compromise between the inefficacy of privacy self-management and the dangers of paternalism.[39] The rationale is that while nudges influence choice, they are not overly paternalistic in that they still give the individual the option of making choices contrary to those sought by the choice architecture.[40]

C. Personal Data Stores[41]

A Personal Data Store or PDS helps you gather, store, manage, use and share the information. It gives the user a central point of control for their personal information (e.g. interests, contact information, affiliations, preferences, friends). For instance, openPDS can be installed on any server under the control of the individual (personal server, virtual machine, etc) or can be provided as a service (SaaS by independent software vendors or application

35 *Id*.

36 Siani Pearson and Marco Cassasa Mont, "HP Labs Bristol" IEEE Computer Society, available at **https://documents.epfl.ch/users/a/ay/ayday/www/mini_project/Sticky%20Policies.pdf**.

37 *Id.*

38 Alessandro Acquisti, Nudging Privacy, available at **http://www.heinz.cmu.edu/~acquisti/papers/acquisti-privacy-nudging.pdf**

39 Daniel Solove, Privacy self-management and consent dilemma, 2013 available at **http://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2093&context=faculty_publications**.

40 Amber Sinha, A case for greater privacy paternalism, Centre for Internet and Society, February 14, 2016, available at **https://cis-india.org/internet-governance/blog/a-case-for-greater-privacy-paternalism**.

41 This solution can aid the Consent principle.

service providers). Additionally, tools like SafeAnswers[42] can turn an algorithmically hard anonymization and application-specific problem into a more tractable security one by answering questions instead of releasing copies of raw data.

D. DND for the Internet Age/One Click Consent Withdrawal[43]

In the case of implementing the principle of Opt Out, data subjects should be provided with options such as a.) no further collection of data, b.) erasure of all previously collected data and the results of processing of such data. In certain cases, it may not be in the public interest to allow erasures of decisions already made on the basis of data collected. This could be facilitated by a system such as a Centralised website/service/phone number/email number - where an individual can withdraw consent easily, for instance through a single SMS for which the syntax is easy to use. Services providers could be automatically informed of such choices, or they could access the details of the users who have opted out periodically (daily or bi-weekly basis) and effect changes. In order to prevent mistaken removal of users, an additional layer of confirmation through email/SMS can also be built in.

E. Algorithmic Transparency for Automated Decision Making[44]

In case of services employing automated or algorithmic decision making having a direct bearing on the users, the regulation must mandate that only appropriate statistical techniques must be used and that transparency must be ensured; that measures should be in place to correct inaccuracies and risks of errors; and that security must be ensured and discriminatory effects prevented. To minimize concerns of unauth data usage, organizations should disclose the logic underlying their decision-making processes to the extent possible without compromising their trade secrets or intellectual property rights.[45]

3. Norms/Standards

Norms and standards, while lacking the force of regulatory compulsion, can still play a significant role in creating informal modes of behavior with an interplay with consumer demand and market competition. These norms are even more useful in cases where we lack one size fits all solutions, and writing these solutions into law may prove counter-productive. In such case, a regulator can still play a role by encouraging the creation of norms and standards which may be further the regulatory objective.

A. Standardized Privacy Notices[46]

The form in which notices are presented is extremely important. Therefore, summaries, infographics, highlighting relevant and actionable information can go a long way in making notices much more intelligible to laypersons. Some existing models of standardized formats for simple and easy to use privacy notices include the following: i) National Telecommunications and Information Administration (NTIA) developed a code of conduct for

42 Yves Alexandre de Montjoye et al, openPDS: Protecting the Privacy of Metadata through SafeAnswers, Plos, July 9, 2014, available at **http://journals.plos.org/plosone/article?id=10.1371/journal.pone.0098790**.

43 This solution can aid the Opt Out principle.

44 This solution can aid the Notice and Transparency principles.

45 Pasquale, F. "The Black Box Society: The Secret Algorithms That Control Money and Information". Harvard University Press. (2015).

46 This norm can add to the Notice principle.

standardized short-form privacy notices for smartphone app.[47] ii) Private Parts is a web based service to simplify privacy notices, eg.[48]

B. Privacy Commons[49]

The development of Privacy Commons Notices on the lines of Creative Commons Licenses can be a useful soft standard for recognised, easily understood privacy notices which are human and well machine readable. Not only will it increase awareness of key terms in privacy notices, this will also creates an incentive for service providers to improve their privacy policies if they want to claim that they use Privacy Commons Notice. Also, in the chain of big data co-controllership and information sharing, privacy preferences of the data subjects may often be neglected or not adequately considered which creates the need for automated policy definition and enforcement so that one party cannot refuse to honour the policy of another party in the chain of big data analytics. For this, the research community and the big data analytics industry needs to explore the area of privacy policy definition and to embody relevant mechanisms for automated enforcement of privacy requirements and preferences.[50]

C. Privacy Impacts Assessments Using a Harms Based Approach[51]

Under this approach, a matrix of threats and harms of collection and use of data must be arrived at. Threats can be categorised as —a) inappropriate use of personal information and b) personal information in the wrong hands. Harms, on the other hand, can be divided into: a) tangible harms which are physical or economic in nature (bodily harm, loss of liberty, damage to earning power and economic interests); b) intangible harms which can be demonstrated (chilling effects, reputational harm, detriment from surveillance, discrimination and intrusion into private life); and c) societal harm by diminished privacy.[52]

D. Strong Standards for De-identification to be Promoted for Research

The process of de-identification removes identifying information from a dataset such that remaining individual data cannot be used to personally identify specific individuals, thus reducing the privacy risk of further sharing and processing of data. The different approaches to de-identification include removal of direct identifiers, pseudonymization, De-identification of Quasi-Identifiers, field based de-identification, privacy preserving data mining and publishing. Effective employment of these techniques would involve regulatory bodies to frequently examine the efficacy of these techniques in light to emerging re-identification approaches, incentivising and/or mandating the use of de-identification techniques based on the sensitivity of personal data in question through sectoral regulations.

---

47 “Short form Notice Code of Conduct to promote Transparency in Mobile App practices” available at **https://www.ntia.doc.gov/files/ntia/publications/july_25_code_draft.pdf**.

48 **https://www.lookout.com/legal/privacy-policy**

49 This norm can aid the Notice principle.

50 “State of the Art Analysis of Data Protection in Big Data Architectures” European Union Agency For Network And Information Security, available at **https://iapp.org/resources/article/state-of-the-art-analysis-of-data-protection-in-big-data-architectures/**.

51 This norm can aid the Accountability principle.

52 Fred Cate, “The Failure of Information Practice Principles,” in Consumer Protection in the Age of the Information Economy, ed. Jane K. Winn (Burlington: Aldershot, Hants, England, 2006) **http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1156972**.

E. Privacy by Design

Privacy by design refers to the practice of technological and organisational measures to embed data protection principles in systems and services by way of implementing privacy enhancing technologies (PETs) and principles such as data minimization directly into the design of information technologies and systems.[53] Effective implementation of these principles require incentives and legal obligations from the regulators so that data protection becomes an integral part of the technological design and organizational structure of services providers.

F. Privacy by Default

Privacy by default is a principle intended to counter the wide use of privacy policies and terms of conditions by services providers to nudge users towards least privacy preserving choices by having maximum data collection and blanket consents as defaults. Implementation of privacy by default would entail that the strictest privacy settings automatically apply when a user signs up for a service. This would be done by ensuring that the default privacy settings would always lean towards privacy enhances choices and technological implementation of the data minimisation principle by automating deletion of data once the purpose has been fulfilled.[54]

53 Ann Cavoukian, Privacy by Design: The seven foundation principles, available at **https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf**.

54 Sam Pfeifle, "Privacy by Default" May Be Big Post-Regulation Issue, IAPP, available at **https://iapp.org/news/a/privacy-by-default-may-be-big-post-regulation-issue/**.