Response to Data Protection Committee

Subhashish Bhadra, Omidyar Network

Background

I work for the Omidyar Network, which is a philanthropic investment firm that invests in organisations and visionary ideas that create opportunities for people to improve their lives, their communities and the world around them. In Oct '16, we started work in digital identity, wherein we look at how to improve both identification systems, public or private, but also 'de-facto identity', which is the data that can be used to identify individuals.

As part of this work, we have supported ISB's Digital Identity Research Initiative in India, the World Bank's ID4D Multi-Donor Trust Fund, Caribou Digital's Identities Project, IDinsight's State of Aadhaar report, and a report on blockchain and self-sovereign identity, among other things. Key to our approach is our focus on privacy and user control over data in an increasingly digital age. Therefore, we have also funded multiple research projects on privacy. In India, we are funding field research on privacy, starting with a research on how to make consent meaningful.

Part of our funding is directed towards start-ups that are enhancing user privacy. We are having conversations with multiple start-ups across the globe that are working on issues such as consent, data minimisation, zero-knowledge proofs and data security. Through this, we explore the frontiers of technology, both geographies ranging from Bangalore to Silicon Valley. We seek to closely understand user preferences and promote innovations that respond to such preferences in a privacy-enhancing manner.

This is a personal submission, but draws on my experience and expertise of working on digital identity issues globally with Omidyar Network.

CHAPTER 1: TERRITORIAL AND PERSONAL SCOPE

What are your views on what the territorial scope and the extra-territorial application of a data protection law in India should be?

The data protection law should cover any entity processing the personal data of Indian residents. The territorial scope of a law should be determined by the *need* and *capability* to regulate. For example, in the case of driving regulation, there is no need for the Indian state to regulate driving by Indians in the US, because of the heterogeneity of driving rules. In the case of data, the need to protect Indian residents' data is truly global because data rules draw from a fairly homogenous set of principles and data flows are already international in nature and will become increasingly so, as companies move their data centres to different countries in search of cost advantages. Moreover, as a country more populous than all of EU, one could argue that India also has the capability to regulate extra-territorial entities by using tools such as market access that the paper has highlighted.

To what extent should the law be applicable outside the territory of India in cases where data of Indian residents is processed by entities who do not have any presence in India?

Even with entities that have no presence in India, the *need* to regulate remains unaltered. However, the *capability* might be lower, because non-presence blunts threats such as market access. However, the state should be encouraged to explore other means of holding such entities to account. The US-EU "privacy shield" provides one such framework.

While providing such protection, what kind of link or parameters or business activities should be considered?
Since the objective of the data protection law should be to offer protections and recourse to Indian residents in a digital age, it should cover any entity that processes the data of Indian residents, which is the approach that GDPR has taken.

What measures should be incorporated in the law to ensure effective compliance by foreign entities *inter alia* where adverse orders (civil or criminal) are issued against them?
The paper has outlined a few measures to ensure accountability, such as restricting access to markets, penalties based on global turnover, mandatory establishing of a representative office and holding the Indian subsidiary/related entity liable for civil penalties or damages. These should be sufficient for entities that have a commercial presence in India. However, these should be measures of last resort. The focus should be on a general harmonisation of privacy laws across the world based on a shared understanding of principles. By exploring practices across countries, we are moving in the right direction. Moreover, the government should explore the idea of bilateral agreements with foreign states that will hold such entities to account. The US-EU "Privacy Shield" agreement is one such template.

CHAPTER 3: WHAT IS PERSONAL DATA?

What are your views on the contours of the definition of personal data or information?
Personal data under the law should be broadly defined as data that pertains to an individual ('identified') or that can be used to identify her with reasonable accuracy ('reasonably identifiable'). Within this broad definition, certain exemptions may then be found, for example anonymised or aggregated data.

For the purpose of a draft data protection law, should the term 'personal data' or 'personal information' be used?
The term 'personal data' should be used and defined in the law. This will remove any ambiguity regarding the scope of the law.

What kind of data or information qualifies as personal data? Should it include any kind of information including facts, opinions or assessments irrespective of their accuracy?
Personal data under the law should be broadly defined as data that pertains to an individual, that can be used to identify her *or* cause any kind of harm to her. Exemptions can then be carved out. Accuracy of the facts, however, should not be one of the criteria. False information pertaining to an individual should be considered personal information, given its capacity for harm.

Should the definition of personal data focus on identifiability of an individual? If yes, should it be limited to an 'identified', 'identifiable' or 'reasonably identifiable' individual?

Identifiability will be a difficult criterion to implement. Data analytics and cross-referencing may permit identifiability from data – even anonymised - which seems non-identifiable. Therefore, a more holistic definition consisting of 'reasonably identified' should be used, such that codes of practice will have to be developed so that if deanonymisation can allow for inference about personal data, those instances are included as well.

Should anonymised or pseudonymised data be outside the purview of personal data? Should the law recommend either anonymization or pseudonymisation, for instance as the EU GDPR does?
Whether anonymization is truly possible is still under discussion. Therefore, the law should cover both anonymised and pseudonymised data. For example, if a data point collected by a body corporate is anonymised, but will reveal the identity when combined with another anonymised data point, it should fall within the purview of the law as soon as it becomes reasonably identifiable.

Should there be a different level of protection for data where an individual is identified when compared to data where the individual may be identifiable or reasonably identifiable? What would be the standards of determining whether a person may or may not be identified on the basis of certain data?
No. Identified and identifiable data must be treated in the same way. The line separating the two will get increasingly blurred with the evolution of data analytics.

CHAPTER 4: SENSITIVE PERSONAL DATA

What are your views on sensitive personal data?
Classification of data is important and such classification may need to have more than just two categories. A criteria-based approach needs to be followed, so that new data fields can be added in future. Some personal information needs to be treated as 'sensitive personal data' because simple revelation of the data can cause significant physical, economic or reputational harm to an individual. This should include race, ethnicity, health status, sexual orientation and religion.

Should the law define a set of information as sensitive data? If yes, what category of data should be included in it?
Yes, the law should define a set of information as sensitive data. In addition, it should lay out the principles for such classification. In addition, sectoral regulators should be allowed to add categories of data to the list. Based on the earlier definition of sensitive data as those whose revelation can cause significant physical, economic or reputational harm, this would imply that race, ethnicity, religion, health status and sexual orientation should form part of that.

Are there any other views on sensitive personal data which have not been considered above?
There need to be multiple categories of data, based on risk-based regulation. One of the categories should be sensitive personal data. Another category needs to be 'potentially sensitive personal data'. This should include information that, combined with other data, can cause significant physical, economic or reputational harm. Therefore, financial information would fall in this category. A third category should be data access controls. This should include

information that controls access to other information, such as passwords and biometrics. Fourth, there should be a category of personal data that includes all other data. More such categories might be needed. This categorisation will keep evolving and therefore needs to be subject to periodic review via open consultation.

CHAPTER 9: DATA LOCALISATION

What are your views on data localisation?
There is no reason to mandate data localisation. There is a need to protect the right to access of the government, after following due process of law. This could, for example, be for law and order purposes. Data localisation will not ensure such access. For example, foreign entities could store the data in encrypted format even on Indian servers and this would prevent law enforcement agencies from accessing it. If data is stored unencrypted, it will be prone to hacking by international actors anyway. To ensure access, the law must provide that the data controllers should share information with the government, after following due process of law. Existing processes for such access should be reviewed and streamlined to ensure that adequate safeguards are built into them. To ensure the data subjects' right to data security, the rights enshrined in the law must be strictly enforced. If that is done, companies will be sufficiently disincentivised from storing data in geographies that do not provide adequate security.

Should there be a data localisation requirement for the storage of personal data within the jurisdiction of India?
No.

If yes, what should be the scope of the localisation mandate? Should it include all personal information or only sensitive personal information?
N/A

If the data protection law calls for localisation, what would be the impact on industry and other sectors?
Given the large size of the Indian market, market leaders such as Amazon have opened data centres in India. Most start-ups are using such servers that are based out of India, such as Amazon's Mumbai data centre. Since so much data is already stored locally, the economic impact of data localisation might not be very significant. However, there is no justification for data localisation.

PART III

CHAPTER 1: CONSENT

What are your views on relying on consent as a primary ground for processing personal data?
Informed and meaningful consent should be the primary ground for processing data. User control should be the bedrock of a data protection regime and consent is an irreplaceable part of user control. In general, consent should be viewed as a *necessary but not sufficient* condition. Consent does not exhaust all duties of the data collectors.

What should be the conditions for valid consent? Should specific conditions such as 'unambiguous', 'freely given' etc. as in the EU GDPR be imposed? Would mandating such requirements be excessively onerous?
Consent should be unambiguous, well-informed, clearly articulated, specific, time-bound, revocable and auditable. Since a law will be in force for several generations, such principles should be articulated, even if some of them are aspirational under today's conditions. With these high-level principles in place, the specific consent requirements can evolve and be updated through delegated legislation. For example, some of the conditions (eg. well-informed) might be better specified by sectoral regulators. What is important is that the DPA should be empowered to call out deliberate violation of these principles.

How can consent fatigue and multiplicity of notices be avoided? Are there any legal or technology-driven solutions to this?
The primary reasons of consent fatigue are length of notices, immediacy of service requirement, lack of meaningful choice and jargon. The general principle to address consent fatigue is to not make it a one-time decision under time pressure. Therefore, a few solutions to consent fatigue could be: (a) auditability and revocability of consent through storage of consent certificates in user-controlled digital lockers (b) sector-specific 'simplified information packets' that can use tools such as pictorial representation (c) printing and pasting of relevant consent notices on the walls of public utilities such as PDS shops etc.

Should different standards for consent be set out in law? Or should data controllers be allowed to make context-specific determinations?
The same standards for consent should be applicable to all entities, public and private. The law itself should carve out very limited and specific exemptions, such as for national security, which must be clearly defined and constrained by due process. Any other exemptions should be considered on a case-by-case basis by the DPA and be open to judicial review.

Would having very stringent conditions for obtaining valid consent be detrimental to day-to-day business activities? How can this be avoided?
Obtaining consent will not be incrementally costly for businesses, because it is already part of most workflows. Ensuring auditability and revocability of consent may create upfront costs (eg. legal) for businesses, but these should be viewed as necessary, since the long-term cost of breaches and lack of trust for both individuals and businesses, is extremely high. Current state of technology allows for low-cost meaningful consent, for example through SMS-based one-time passwords (OTPs) and multiple-language IVRs. Therefore, the premise that a

requirement to obtain valid consent would be a major cost centre for businesses is unlikely to be true.

Are there any other views regarding consent which have not been explored above?
In many cases such as child's consent, zero-knowledge proofs might be desirable. These enable the individual to provide proof of one attribute (eg. age) without revealing any other information (eg. name, address). These are important to protect the privacy of individuals on digital platforms.

CHAPTER 3: NOTICE

Should the law rely on the notice and choice mechanism for operationalising consent?
Yes. In addition, notice must be the absolute minimum requirement for any kind of data processing. It must also be available in non-consent grounds for data processing.

How can notices be made more comprehensible to individuals? Should government data controllers be obliged to post notices as to the manner in which they process personal data?
The DPA should encourage sectoral regulators to specify simplified notices and update them from time to time, based on the principles that should be specified in the law itself. These guidelines should explore options such as pictorial depiction, IVR or SMS-based consent, local languages, simplified 'information packets' etc. Organisations, both public and private, should then be encouraged to follow the specified formats. Industry guidelines through self-regulatory processes might also be considered. In either case, the involvement of sectoral regulators is important because 'informed consent' may different from sector to sector.

Should the effectiveness of notice be evaluated by incorporating mechanisms such as privacy impact assessments into the law?
Yes. Organisations, or a subset of them, should be mandated to conduct privacy impact assessments (PIA) of their data practices before they start collecting personal data of individuals. The frequency of such privacy impact assessments should be determined by the scale of data collection – large organisations (eg. govt bodies, telcos) should do PIAs more frequently. The body doing such assessments could also vary. For example, smaller organisations might be permitted to have in-house assessments, whereas very large data controllers might need to hire external audit agencies. However, any data controller holding sensitive data should be subject to a higher bar for privacy impact assessments.

Should the data protection law contain prescriptive provisions as to what information a privacy notice must contain and what it should look like?
No. The data protection law should lay out the principles of what informed consent and notice must look like. Both the DPA and sectoral regulators should be encouraged to specify simplified notices and update them from time to time. Self-regulation by industry bodies should also be encouraged – they could be given a time within which to come up with such frameworks and the sectoral regulator could step in if they are unable to. This is because the possibilities of how consent can be obtained will keep changing with evolving technology and practices and technology should not be hard-coded into the law.

How can data controllers be incentivised to develop effective notices?

Templates of effective notices should be put out by the DPA or the sectoral regulator. Organisations should have to adhere to such notices. Any violation must be appropriately penalised. In addition, industry bodies or individual corporations should be incentivised to test new methods of consent.

Would a consent dashboard be a feasible solution in order to allow individuals to easily gauge which data controllers have obtained their consent and where their personal data resides? Who would regulate the consent dashboard? Would it be maintained by a third party, or by government entities?

This needs to be considered at two levels. First, every data controller should be mandated to provide the data subject with all the consent certificates that she has provided. This should be left to the data controllers, with penalties for non-compliance. There are already companies that enable such consent dashboards. The second level is to provide information on consent across *all* data controllers. This may not be required if the first level of information is provided. However, if it is deemed mandatory, it could be provided by third parties and regulated by the government.

Are there any other alternatives for making notice more effective, other than the ones considered above?

Several organisations and tech start-ups globally are actively seeking to make consent more meaningful. They are experimenting with simplified consent notices that enhance trust, thus enabling a more robust data economy to emerge. In this way, privacy and trust is emerging as the foundation for a new wave of innovation. While these innovations are slowly catching on, India has the opportunity to use regulation to nudge enterprises in that direction.

CHAPTER 5: PURPOSE SPECIFICATION AND USE LIMITATION

What are your views on the relevance of purpose specification and use limitation principles?

Purpose specification and use limitation ought to be the bedrock of any consent- or accountability- based data regime. The lack of these principles will result in unfettered use of an individual's data that is completely opaque to her.

How can purpose specification and use limitation principles be modified to accommodate the advent of new technologies?

Since the proposed law will be in force over multiple generations, the law should lay down the principles and not look at it from the lens of technologies at a particular point in time. Technologies available today, such as distributed ledgers, have evolved enough to enable auditability and immutability of data flows. Such technologies will continue evolving in future.

What is the test to determine whether a subsequent use of data is reasonably related to/compatible with the initial purpose? Who is make such determination?

For reasons of efficiency, such determination should be left to the data controllers within organisations. However, to ensure that they can be held accountable, all such determinations must be auditable. Second, individuals should be allowed to confirm the source of data about them. This will ensure that users can approach the proposed DPA for any harm caused and can demonstrate inappropriate use of their data.

What should the role of sectoral regulators be in the process of explicating standards for compliance with the law in relation to purpose specification and use limitation?
The DPA should prescribe baseline standards and sectoral regulators should be allowed to have additional/higher standards over and above these.

Are there any other considerations with respect to purpose specification and use limitation principles which have not been explored above?
Several innovations are taking place internationally to establish property rights in a digital age. Understandably, such innovation is starting with high-value data such as art and music. For example, a 'hash' of the data is stored on the blockchain, enabling verification of ownership without revealing the underlying data. The technologies and principles established in these sectors may find their way to personal data in the near future. That will make it easier to ensure purpose specification and use limitation. Therefore, the legislation should not take a conservative approach to these matters.

CHAPTER 6: PROCESSING OF SENSITIVE PERSONAL DATA

What are your views on how processing of sensitive personal data should be done?
Sensitive personal data (SPD) should have a higher standard of privacy and data protection than non-SPD.

Given that countries within the EU have chosen specific categories of "sensitive personal data", keeping in mind their unique socio-economic requirements, what categories of information should be included in India's data protection law in this category?
There need to be multiple categories of data. One of the categories should be sensitive personal data, i.e. data that can cause harm by its mere revelation. This should include race, ethnicity, health status, sexual orientation and religion. Another category needs to be 'potentially sensitive personal data'. This should include information that, combined with other data, can cause significant physical, economic or reputational harm. Therefore, financial information would fall in this category. A third category should be data access controls. This should include information that controls access to other information, such as passwords and biometrics. Fourth, there should be a category of personal data that includes all other data. More such categories might be needed.

What additional safeguards should exist to prevent unlawful processing of sensitive personal data?
Firstly, SPD should only be collected on the basis of unambiguous, well-informed, clearly articulated, specific, time-bound, revocable and auditable consent. Second, no transfer of sensitive personal data should be permitted without the kind of consent outlined above. Third, any data derived from the processing of sensitive personal data should also be treated as sensitive personal data. Fourth, the penalties for violation of provisions related to sensitive personal data should be higher. Fifth, higher technological protections should be considered for SPD – for example, any digital storage or transfer of SPD should be encrypted.

Should there be a provision within the law to have sector specific protections for sensitive data, such as a set of rules for handling health and medical information, another for handling financial information and so on to allow contextual determination of sensitivity?
The Data Protection Law should set the minimum threshold to which all sensitive personal data should adhere. Sectoral regulators should be permitted to include more kinds of data in this category and also prescribe higher protections.

Are there any alternative views on this which have not been discussed above?
Non-sensitive information can be processed to yield sensitive information. For example, regular Uber rides to a cancer hospital indicates a high probability that either the data subject or someone in her family has cancer. Therefore, one could argue that making a distinction is pointless. However, there is merit in making a distinction between data that is harmful in itself and others that are 'potentially harmful.'

CHAPTER 7: STORAGE LIMITATION AND DATA QUALITY

What are your views on the principles of storage limitation and data quality?
Storage limitation is an important step in preventing hoarding of data about an individual that can lead to profiling. Currently, there are no barriers and costs to data collection. Therefore, private and public sector enterprises keep collecting data, even if the marginal benefit is nearly zero. There are two components to preventing it – first, an outright limitation to data collection and storage. Second, the marginal cost of data collection (through penalties for mismanagement) need to be sufficiently high. Similarly, data quality has its own economic incentives – better and more recent data leads to better decision-making. However, this natural incentive needs to be bolstered with an explicit mandate to ensure good data quality.

On whom should the primary onus of ensuring accuracy of data lie, especially when consent is the basis of collection?
The mode of collection of data should be viewed distinctly from the mandate for its quality. In general, it should be the onus of the data controller, especially in situations where that data is processed for decision-making. This should be supplemented by the right of the individual to access and rectify any data held about her.

How long should an organisation be permitted to store personal data? What happens upon completion of such time period?
An organisation should be permitted to store personal data only for the time period that is specified in the consent certificate that is signed by the user. Sectoral regulators can also specify time limits for certain industries. On completion of such a time period, data should be completely erased, unless the data subject consents to its storage in an anonymised form. This is crucial because it is very challenging for data to be completely anonymised.

If there are alternatives to one-size-fits-all model of regulation (same rules applying to all types of entities and data being collected by them) what might those alternatives be?
Exemptions as outlined in the rest of the document should be sufficient to cover the nuance between different kinds of data collectors. Other customisation only for this particular right may not be required.

Are there any other views relating to the concepts of storage limitation and data quality which have not been considered above?
Firstly, the notion that lack of information can reduce market growth can be unfounded. For example, children's digital media, which is enforced by a legally enforceable anonymous engagement model, has grown at 25 percent annually, now topping $1.2B. Secondly, innovations around decentralised storage should be considered. For example, certain kinds of data (such as SPD) could be mandated to be stored in a decentralised way in individual-controlled, device-based digital lockers. Some of these measures might not be practical today, and therefore the law should provide enough space for such innovations in future.

CHAPTER 8: INDIVIDUAL PARTICIPATION RIGHTS - I

What are your views in relation to the above?
In general, all the individual participation rights outlined in the white paper should be included in the data protection law and made available to individuals. Operationalising all of them might be challenging in the short run and, therefore, a transition period should be provided. For example, the RTI Act provided for a transition period of 120 days. This transition period should be shorter for larger organisations (eg. govt. departments, telcos). Technology can be deployed to reduce the cost of adherence. To enable such rights, there should be a regulatory push towards data standardisation. In particular, the right to confirm, access and rectify personal information are the building blocks of all other privacy-related rights. Without the knowledge of what information is held about them, individuals cannot be expected to be in a position to take any further action. Therefore, these three rights should be extended to citizens with very few exceptions such as law enforcement.

Should there be a restriction on the categories of information that an individual should be entitled to when exercising their right to access?
Restrictions should be very few. A possible principle could be that only information whose access is likely to create a negative externality for society should be blocked. Law and order would be one such restriction. A criminal accessing information held about her can misuse it and therefore should be denied.

What should be the scope of the right to rectification? Should it only extend to having inaccurate data rectified or should it include the right to move court to get an order to rectify, block, erase or destroy inaccurate data as is the case with the UK?
Inaccurate data can cause immeasurable harm to an individual's well-being. Therefore, an individual should be empowered to rectify, block, erase or destroy inaccurate data. However, since the rest of data-related complaints are envisaged to be handled by the DPA, such complaints should also fall within the remit of the DPA.

Should there be a fee imposed on exercising the right to access and rectify one's personal data?
A graded approach is required here. Anything that violates the fundamental rights of an individual should be free of cost. For example, if any incorrect information (eg. wrong Aadhaar number) is resulting in denial of food or education, such access and rectification should be free of cost. Access to data that is required for commercial activities may be subject to a reasonable fee that can be determined by sectoral regulation.

Should there be a fixed time period within which organisations must respond to such requests? If so, what should these be?
Since data generation and transmission is extremely fast, data-related rights need to be time-bound for them to be effective. The data protection committee can set an upper bound on what this time limit should be (possibly a month, or less), with sectoral regulators having the power to fix shorter time-frames. For example, the health regulator might choose to have much shorter time-frame because of the critical nature of the service being rendered.

Is guaranteeing a right to access the logic behind automated decisions technically feasible? How should India approach this issue given the challenges associated with it?
While understanding the logic behind some automated decisions might not be technically feasible, it is imperative to ensure that such decisions are fair. Therefore, two aspects are critical. First, individuals must have the right to access inputs into such decisions. Second, such algorithms should be audited randomly by the DPA to ensure that using the same inputs results in the same output, and no extraneous circumstances of data is being used by the algorithm.

What should be the exceptions to individual participation rights?
As discussed above, only information whose access is likely to create a negative externality for society should be blocked. Financial reasons (eg. high cost of compliance) should not be a reason for exceptions. In such cases, data controllers should be able to charge appropriate fees, which can be set or approved by the DPA. One should also think of situations in which *all* data-related rights should be available. One should be cases where data is mandatorily collected on a large scale. The second should be cases of denial of services. Other such cases should be established.

Are there any other views on this, which have not been considered above?
Since the data protection law will be in force for generations to come, it should be mindful of the fact that technology will evolve and, among other things, bring down the cost of compliance. Therefore, the law should frame the high-level principles that can be interpreted and re-interpreted for years to come. Low usage of rights should be a reason to not provide these rights. To draw a crude analogy, the rights emanating from striking down Section 377 will not benefit a large majority of the population – but this shouldn't be a reason to not do so.

CHAPTER 9: INDIVIDUAL PARTICIPATION RIGHTS - 2

What are your views on the above individual participation rights?
Since the data protection law will be in force for generations to come, more rights are preferable to few. Among the rights listed in this section, data portability is extremely important to usher in a regime of user-controlled data. Starting with the recognition of the user being the ultimate owner of her data, the law must ensure that she can store and transfer it to any medium she chooses. The processing-related rights are also important, because processing may allow data to be combined in ways that enable further violations of privacy. The right to not be subject to a decision based solely on automated processing may need further consideration that can be left to sectoral regulators.

The EU GDPR introduces the right to restrict processing and the right to data portability. If India were to adopt these rights, what should be their scope?
The right to data portability is extremely important for user-centricity of data. Therefore, such a right should be unrestricted. Current technology may not allow organisations to comply immediately and therefore a transition period should be provided. The right to restrict processing is also important and therefore should be made available, though some narrowly-drawn exceptions might be needed (eg. law enforcement).

Should there be a prohibition on evaluation decisions taken on the basis of automated decisions?
This aspect of data protection may be left to sectoral regulators because the efficacy of automated decisions might be very different in, say, health and finance. Such regulators should be equipped to come up with the relevant restrictions based on the strength of evidence in their respective fields.

Given the concerns related to automated decision making, including the feasibility of the right envisaged under the EU GDPR, how should India approach this issue in the law?
As discussed above, this aspect of data protection may be left to sectoral regulators because the efficacy of automated decisions might be very different in, say, health and finance.

Should direct marketing be a discrete privacy principle, or should it be addressed via specific sectoral regulations?
Since marketing principles, channels and strategies are fairly uniform across sectors, a discrete privacy principle covered in the overarching data protection law would be more appropriate.

Are there any alternative views which have not been considered?
First, standardisation and shared data ontology is a necessary pre-requisite for data portability. The US, for example, has struggled with data portability, despite an in-principle nod, because of the lack of a shared ontology. Therefore, there is a need for a regulatory push towards data standardisation, and this can be done by sectoral regulators. Second, Iceland has shown an approach towards data portability by opening up health data to its citizens.

CHAPTER 10: INDIVIDUAL PARTICIPATION RIGHTS - 3

What are your views on the right to be forgotten having a place in India's data protection law?
The right to be forgotten is important in an Indian context. A large number of Indians will be coming to digital platforms for the first time and may therefore not be aware of the functionalities and risks of these platforms. They may undertake activities without fully comprehending their consequences. Therefore, the right to be forgotten will reduce the risk that they expose themselves to.

Should the right to be forgotten be restricted to personal data that individuals have given out themselves?

In general, there should be no distinction between personal data that the user has given our herself and that data controllers have generated about the user. For example, an individual's social media data, which is mostly voluntarily given out, should be treated no differently from call record data, which is generated by a telco. Following from this principle, the right to be forgotten should cover all personal data provided by and generated about an individual.

Does a right to be forgotten add any additional protection to data subjects not already available in other individual participation rights?

A right to erasure does not exist in the other individual participation rights outlined in Chapters 8 and 9 of the report. The other participation rights provide for transparency (through confirmation and access), rectification, portability, and control over processing. A right to be forgotten, or right to erasure, is important to complete the suite of individual participation rights.

Does a right to be forgotten entail prohibition on display/dissemination or the erasure of the information from the controller's possession?

Since the data should be viewed as the individual's digital property, the right to be forgotten should include complete erasure of the information from the controller's possession. A mere prohibition on display/dissemination will continue to expose the data subject to risks emanating from the controller's data security practices. The data subject should have the agency to choose whether to subject herself to such risks.

Whether a case-to-case balancing of the data subject's rights with controller and public interests is a necessary approach for this right? Who should perform this balancing exercise? If the burden of balancing rests on the data controller as it does in the EU, is it fair to also impose large penalties if the said decision is deemed incorrect by a data protection authority or courts?

Firstly, the DPA should clearly and narrowly define 'public interest' in the context of data rights. Data controllers should be provided some autonomy to perform the 'public interest' test as laid out by the DPA. If the data subject is dissatisfied by the data controller's decision, she should be able to reach out to the DPA. The DPA should then be authorised to impose large penalties.

Whether special exemptions (such as the right to freedom of expression and information) are needed for this right? (over and above the possible general exemptions such as national security, research purposes and journalistic or artistic expression)?

Since research, journalistic and artistic expression are already covered as general exemptions, special exemptions just for the right to be forgotten may not be required.