Jan 30, 2018

ITI Comments on White Paper of the Committee of Experts on Data Protection Framework for India

The Information Technology Industry Council (ITI) welcomes the Government of India (GOI) Committee of Experts' and the Ministry of Electronics and Information Technology (MEITY)'s initiative in preparing this comprehensive white paper on a data protection framework for India. ITI is the premier advocate and thought leader around the world for the global information and communications technology (ICT) industry. ITI's membership is comprised of the world's leading innovative technology companies from all corners of the ICT sector, including hardware, software, digital services, semiconductor, network equipment, cybersecurity, and Internet companies. Our members are global companies, headquartered around the world with business in every major market and deep investments in India. Privacy, security and trust are central to our companies' continued success and we take seriously our obligation to protect and responsibly use the personal information of our customers, consumers, users, and employees.

Because of our diverse membership and widespread business presence, our companies have extensive on site, practical experience with the privacy and data protection regimes[1] of nearly every country. Informed by our global perspective and broad expertise, ITI encourages governments, as they consider developing or updating their privacy frameworks, to do so in a way that promotes the responsible use of personal information, encourages domestic innovation, attracts foreign investment, promotes the growth of trade and facilitates the free flow of information.

We are aware that each of the countries in which our members operate present a unique combination of challenges and opportunities in developing sustainable data protection policies. We welcome the Supreme Court of India's recent ruling that privacy is "intrinsic to life and liberty" and is inherently protected under the fundamental freedoms enshrined in the Indian Constitution, as well as the formation of the Expert Committee on Data Protection, under the Chairmanship of Justice B. N. Srikrishna, by India's Ministry of Electronics and Information Technology (MEITY). These events signal the beginning of a new stage in India's advancement on the world stage and we hope to be a resource during upcoming discussions to support the development of robust, globally interoperable data protection policy in India.

We respectfully offer the following recommendations to GOI's White Paper consultation questions and look forward to discussing these and other ideas in more detail as this dialogue progresses.

[1] While the exact meanings of these terms depend on the country and idiosyncrasies of the languages in which they are communicated, as used in this document, privacy and data protection both refer to the rules and practices regarding the handling of personal information or personal data (such as the concepts of notice, consent, choice, purpose, security, etc.).

Jan 30, 2018

SCOPE AND EXEMPTIONS

1. Territorial and Personal Scope

Policymakers often ignore international law obligations and principles to protect their citizens' data, particularly when data leaves their national jurisdictions. Privacy laws asserting extraterritorial applicability – for instance by proclaiming they apply to any entity providing a service that is accessible by citizens or persons located within that country – are incongruous in the online environment, where users can access almost any service from anywhere in the world. Such laws in turn create difficult conflicts of laws issues, not just for multinational corporations but for any data controller that wishes to use technologies involving cross-border data transfers, such as cloud computing. Similarly, obligations to host data domestically and restrict data transfer beyond national borders hamper innovation, productivity, and growth, for both local companies and companies with global operations. In short, the extraterritoriality of privacy rules , cross-border personal data transfer restrictions and data localization requirements create challenges for compliance and enforcement, work against efforts to establish global norms of privacy protection, limit opportunities for innovation, and distort the global marketplace.

An effective privacy and data protection regime should attempt to reconcile the equally important goals of ensuring both global data flows and a high standard of privacy and protection for personal data, regardless of its location. Policymakers attempting to create such a regime should forgo data localization measures and should establish laws with a sensible territorial scope applying only to organizations established in or targeting data subjects residing in a certain country.

2. Other issues of Scope

ITI cautions that retrospective application of the legislation could create huge burdens on businesses – both Indian and international – as it would impact the countless contracts already entered into by companies in addition to any new ones. GOI should keep this in mind and provide reasonable timeframes for organizations to prioritize achieving compliance with the new law in all aspects of their business.

We also recognize that governments all over the world investigating criminal activities increasingly require extraterritorial access to electronic evidence. To increase public safety and security and make investigations and prosecutions more efficient, India should expand investment in cross-border data request mechanisms for law enforcement and counterterrorism purposes, including making Mutual Legal Assistance Treaties (MLATs) more effective tools for cross-border investigations, and leverage existing multilateral agreements, such as the Budapest Convention on Cybercrime. We support a call to action to all governments to prioritize global law enforcement coordination to better address these issues.

3. Definition of Personal Data

Definitions of personal data are fundamental to privacy regimes as they frame how the relevant protections and obligations apply in practice. The definition of personal data should balance protecting a data subject's rights and enabling innovation and access to information. While some definitions of

"personal data" often appear quite broad, regulators should avoid overly rigid or expansive applications of the definition of personal data. Instead, we encourage flexibility in applying definitions.

The EU's Article 29 Working Party guidance on the concept of personal data,[2] for example, lays out the various contexts in which information can be considered personal data. It also notes that a mere hypothetical possibility of singling out an individual is insufficient for considering the information as "identifiable." Instead, the guidance requires an assessment of all potential reasonable uses of data by the controller or any other person to identify an individual before deciding whether the information should be considered "identifiable" and, therefore, "personal data." Ultimately, the Article 29 Working Party indicated that the test of whether information is personal is a dynamic one and should consider the state of the art in technology at the time of the processing.

While the definition of personal data set forth in India's IT Act (Section 43A) is similarly broad, it is important to recognize that identifiability alone may no longer meaningfully determine the scope of data protection rules. For this reason, we encourage Indian policymakers to build the concept of risk into their data protection regime, measuring the likelihood of concrete harm to individuals if their personal data is transmitted or disclosed, and thus preventing an overbroad application of data protection obligations.

4. Definition of Sensitive Personal Data

Many economies, like India, have designated a special category of data called "sensitive data" that receives especially stringent protections because of the risk of inappropriate use. Others, like Singapore, Hong Kong and Canada, adopt an escalating risk management approach, which precludes the need to develop a specific category of sensitive data.

The most common list of categories for sensitive data in comprehensive privacy legislation includes data about racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union memberships, health, criminal offenses and sex life. Alternatively, sectoral approaches, such as in the United States, create targeted laws pertaining to certain types of data that are considered to need greater protection, such as financial data, Social Security Numbers (or similar identifiers), certain types of health information, children's information, login credentials and/or full dates of birth. India's hybrid approach combines both in its definition.

Given the additional protective measures traditionally applied to sensitive data, economies that choose this path should limit the number of categories of such data and keep the list closed. This would help economies avoid overbroad or vague definitions or terms that can cause confusion or inadvertently lead to inappropriate categorization of personal information as "sensitive." Taking an overbroad approach to sensitive data could weaken an economy's competitiveness by limiting foreign investment, increasing the difficulty of doing business, and impeding innovation, job creation, and economic growth, particularly in India's flourishing and critical outsourcing industry. The Indian Supreme Court's suggestion to classify "Personal Data" as "Intimate," "Private," and "Public" and treat these accordingly could be a good way of doing this. This 3-tier approach will remove a lot of ambiguities surrounding

[2] Article 29 Working Party Opinion 4/2007 on the concept of personal data.

classification of Personal Data and ensure deserving Privacy for "Intimate Data," and to some extent to "Private Data."

Further, Indian policymakers and regulators should recognize processing of data that falls under the sensitive category can have beneficial results for the individual and for society (*e.g.*, in the health sector[3]). To promote these potential benefits, lawmakers should avoid being overly prescriptive and should develop effective mechanisms and legal bases to habilitate the processing of sensitive data. For example, the Protection of Personal Information Act (POPI)[4] in South Africa prohibits the processing of "special personal information" (religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information, and certain information relating to the criminal behavior of an individual), subject to various exceptions. These exceptions apply if the processing: (1) is carried out with the consent of a data subject; (2) is necessary for the establishment, exercise, or defense of a legal right or obligation; (3) is necessary to comply with international law; (4) is for historical, statistical or research purposes if certain criteria are met, such as the purpose serves a public interest and the processing is necessary for the purpose concerned; or (5) involves information that has deliberately been made public by the data subject.

In addition to these general exemptions, the POPI devotes several sections to cases concerning the legal processing of each category of special personal information. In doing so, the law codifies that reasonable exemptions should accompany the prohibition of the processing of sensitive categories of data. Similarly, the European General Data Protection Regulation also includes exceptions such as: (1) carrying out obligations and exercising rights of the controller or the data subject in the field of employment, social security and social protection law; (2) protecting the vital interests of the data subject or of another natural person; (3) reasons of substantial public interest, including in the area of public health and or (4) preventive or occupational medicine, assessment of the working capacity of the employee, medical diagnosis, provision of health or social care.

5. Definition of Processing

Addressing the complex questions at the intersection of security, technology, privacy, and economic growth requires collaboration between a diverse set of stakeholders, including law enforcement, tech and other business sectors, academia, and privacy and civil liberties advocates. Protecting and defending against national security and terrorist threats and upholding and enforcing criminal laws are fundamental missions of governments around the world. While we recognize that technology and data can be a central tool in furthering these missions, we believe that the protection of individual privacy requires that governments also be held to the same standard as private actors handling personal data. We therefore suggest, that India's data protection framework address data processing by private and public sectors wherever possible.

We also support exploring the possibility of classifying processing as low risk processing, medium risk processing and high risk processing. The basis of such classification could be the volume of data, nature/quality of data and level of protection provided. Complex and expensive regulatory compliance

[3] For instance, http://www.huffingtonpost.co.uk/entry/twins-4-use-iphone-assistant-siri-to-save-unconscious- mothers-life_uk_58d5049ce4b03692bea47ac0, or http://www.vocativ.com/418862/ai-privacy-assistants-expose- sensitive-info/

[4] Act no. 4 of 2013: Protection of Personal Information Act, 2013.

for small enterprises doing a low risk data processing would adversely impact businesses and innovations.

6. Definition of Data Controller and Processor

We welcome the concept of establishing clear roles for data controllers and data processors, but It is important to clearly establish that the rights of data controllers and data subjects are not, and should not be, at odds.

Regarding responsibilities of controllers, we respectfully suggest that India adopt an accountability-based system that clearly defines and apportions liability between data controllers and data processors. Accountability is a well-established principle of data protection. Accountability shifts the focus of privacy governance to the organization level, requiring organizations to accept responsibility for collecting, processing or otherwise using personal data, irrespective of legal requirements.[5]

Forward-looking privacy and data protection models focus on how data controllers can ensure that their processing operations do not violate individuals' rights or overburden individuals. This is the basis of the accountability model to data protection. Australian Privacy Principles (APPs),[6] for example, call for "privacy management programs" that require organizations to incorporate "privacy by design" into their products. Organizations seeking to comply with the APPs must take reasonable steps to (1) implement practices, procedures and systems relating to their functions or activities and (2) deal with privacy inquiries or complaints.

Data controllers have the primary obligation for ensuring compliance with applicable data protection law, while data processors should be required to comply with data controller instructions and ensure the implementation of technical and organizational measures as well as security of the data they process. These are the customary responsibilities placed upon data controllers and data processors in other data privacy laws globally. A controller ensures that the data subject can exercise his/her rights and ensures respect for the established data protection principles. Data processors' responsibilities are determined bilaterally between controllers and processors depending on the circumstances and normally defined in a detailed contract.

We further advise that there should be flexibility for controllers and processors to negotiate processing contracts that might be most appropriate for their particular business and data processing activities. Processors and controllers should be able to negotiate processing contracts which set out parties' respective responsibilities and liabilities (providing controllers with 'sufficient guarantees' of processor compliance), whilst also effectively operating their businesses and accepting only those obligations that

[5] Mexico's data protection law incorporates provisions that address "accountability" and acknowledge that personal data often needs to travel internationally. It also avoids uncertainty as to what obligations and rights exist as personal data move among data "controllers" and "data processors", and what documentation is needed to assure fulfillment of legal responsibilities. The controller remains accountable, together with any entity to which it transfers data.
Similarly, Canada, through PIPEDA, implements an organization-to-organization approach that is not based on the concept of adequacy. PIPEDA does not prohibit organizations in Canada from transferring personal information to an organization in another jurisdiction for processing. However, organizations are held accountable for the protection of personal information transfers under each individual outsourcing arrangement. The Office of the Privacy Commissioner of Canada can investigate complaints and audit the personal information handling practices of organizations.

[6] Office of the Australian Information Commissioner, Privacy fact sheet 17: Australian Privacy Principles.

are appropriate under the circumstances of the relevant data processing. We also suggest that the GOI include an acknowledgment that the parties can agree commercial terms regarding the processor obligations on the assumption these will not impact the protection of the data. For example, controllers and processors should be able to decide amongst themselves, based on what is reasonable in that circumstance who would bear the costs of any audit and/or the processor providing assistance to subject-access requests and addressing notice requirements, and what the appropriate business hours might be appropriate to provide any audit rights.

7. Exemptions (from Data Protection Law)

We are glad to see that India is considering whether to introduce incentives designed to promote the innovative use of anonymized data. We urge GOI to consider offering decreased compliance burdens or liability protections for organizations voluntarily creating such anonymized data sets. Additionally, if GOI pursues this initiative, we urge GOI not to overlook the potential value of making the anonymized data held by GOI stakeholders available more broadly.

To promote use of anonymized data more broadly, Indian policymakers should remain technologically neutral and avoid mentioning specific technologies, sectors or measures that would define "sufficient anonymization," because standards of anonymization naturally evolve over time as new technical capabilities and privacy enhancing technologies enter the marketplace.

The United Kingdom's Information Commissioner's Office (ICO) has laid out an advanced risk- based approach to anonymization and re-identification[7]. The ICO's approach recognizes the ideal of "perfect anonymization" is superfluous and often unachievable, and opts instead to encourage companies to use technical and contractual measures to mitigate risk until the probability of re-identification is remote. Where anonymization is not possible, competent authorities should grant organizations decreased liability or lessen their compliance burdens as incentives for partially anonymizing, or "pseudonymizing" data. For example, the GDPR permits organizations pseudonymizing data to further process that data for additional purposes that are compatible with the original purpose of that data's collection – without needing to get consent again.

As we collectively cross new milestones on the technological frontier, anonymization and pseudonymization of data can yield large benefits for society. The concept of data minimization – the practice of limiting the collection of personal information to that which is directly relevant and "necessary" to accomplish a specified purpose – is a foundational data privacy and security principle. However, digital technologies such as big data analytics and machine learning should encourage lawmakers to revisit this principle's underlying cost-benefit analysis and reinterpret thoughtfully to maximize the socioeconomic benefits of these innovations.

Big data analytics – which involves examining large data sets to uncover hidden patterns, unknown correlations, market trends and other useful information – should lead policymakers to carefully consider the concept of "necessity" in achieving the goals of the processing while protecting personal data (e.g., carve-outs from privacy legislation for anonymized data).

[7] Information Commissioner's Office, Anonymisation: managing data protection risk code of practice.

Creating carve-outs that reduce the compliance burden for companies that anonymize data creates incentives for organizations to adopt such anonymization practices. These incentives promote better privacy protections for individuals without limiting the promise of digital technologies that rely on data.

Any requirements regarding automated decision making should also take into consideration the scalability of providing worldwide Internet services. There are many activities, such as abuse detection, that require automation in order to make processes scalable when dealing with hundreds of millions of users. Similarly, bad actors will try to circumvent rate limits to influence trending hashtags and send unsolicited messages to users. Therefore, spam detection and the algorithms that guide it should be considered and appropriate exceptions made for such activities.

8. Cross Border Data Flow

The free flow of data is fundamental to the health of the modern global economy, delivering countless benefits and enabling access to knowledge and tools for people around the world. India has historically understood and managed to leverage this reality, as evidenced by the rise of its booming outsourcing industry. It is equally important now for the GOI to acknowledge that international data transfers and meaningful privacy protection are not mutually exclusive or antagonistic goals. Many existing regimes reflect the need to preserve multiple approaches to cross-border data transfers without weakening privacy safeguards and India should leverage and take inspiration from these approaches, which are highlighted in the below examples.

<u>Mexico</u>

Mexico's data protection law incorporates provisions that address "accountability" and acknowledge that personal data often needs to travel internationally. It also avoids uncertainty as to what obligations and rights exist as personal data move among data "controllers" and "data processors", and what documentation is needed to assure fulfillment of legal responsibilities. The controller remains accountable, together with anyone it transfers data to.

<u>Canada</u>

Canada, through PIPEDA, implements an organization-to-organization approach that is based on the concept of accountability. PIPEDA does not prohibit organizations in Canada from transferring personal information to an organization in another jurisdiction for processing. However, organizations are held accountable for the protection of personal information transfers under each individual outsourcing arrangement. The Office of the Privacy Commissioner of Canada can investigate complaints and audit the personal information handling practices of organizations.

<u>APEC</u>

The APEC framework's foundational principles are flexible enough to be adopted on a broad scale and are gaining traction. The principle of "accountability," a key underpinning of the framework, makes the original data collector legally "responsible" for data by making sure the obligations of the data controller follow the data as it crosses borders. The United States, Mexico, Canada, Japan and Korea are already participating or have committed to participate in the CBPRs, while the Philippines, Chinese Taipei and Singapore have all taken steps to participate, and other APEC economies have signaled their interest in

joining. The CBPRs offer a scalable system that holds the potential to be less burdensome to economies and companies than other systems (like EU's BCRs, which under the Directive had been very resource-intensive, tied to administrative rules, and subject to a complex approval process, but may become less so under the GDPR).

Malaysia

Malaysia's PDPA allows for government to designate a list of places that ensure an adequate level of protection; however, it also lays down instances where cross border transfer is permitted notwithstanding the designated places. Such instances include where:

(a) the data subject has given his consent to the transfer;

(b) the transfer is necessary for the performance of a contract between the data subject and the data controller; or

(c) the transfer is necessary for the conclusion or performance of a contract between the data controller and a third party which—

(i) is entered into at the request of the data subject; or

(ii) is in the interests of the data subject;

Some of the instances listed above will certainly make the transfer less burdensome and less bureaucratic.

Other Mechanisms

Model clauses (pre-approved, voluntary contractual commitments that are endorsed by national privacy regulators for providing adequate safeguards with respect to the protection of the privacy for international transfers of data from data controllers to data controllers or from data controllers to processors abroad) are a transfer mechanism that can be a similarly straightforward and low-burden way for organizations to comply with their obligations to protect personal data, even when it is being transferred elsewhere.

Third-party certifications, codes of conduct and privacy seals are also examples of co-regulatory tools that place binding and enforceable privacy commitments on participating organizations while providing compliance certainty for regulators, consumers, stakeholders and other industry partners.

9. Data Localization

Mandating local storage of data vastly increases the cost of doing business for companies. Data storage and processing relies on the economies of scale that can be found in large data centers. Companies, even very large multinational companies, use very few facilities for their global data processing needs. This allows them to provide effective low costs, high quality services. Mandating that this process take place within certain borders can raise the cost for companies to procure data services by 30-60%.[8] Not only is this cost crippling for SMEs, it translates to massive macroeconomic costs: economy-wide data localization in India could cost up to .8% of its GDP and decrease investments by 1.3%, causing economy-wide welfare losses per worker equivalent to 11% of the average monthly salary.[9] The result of these large costs

[8] "Quantifying the Cost of Forced Localization" Leviathan Security Group, 2015.

[9] "The Costs of Data Localisation: Friendly Fire on Economy Recovery" ECIPE, 2014.

includes a dampening of technological adoption and would be a significant challenge for India firms to overcome in order to compete in the global economy.

For these reasons, obligations to host data domestically and restrict data transfer beyond national borders hampers innovation and growth, for both budding domestic industry as well as companies with global operations. Both extraterritoriality of privacy rules and data localization create challenges for compliance and enforcement, work against efforts to establish global norms of privacy protection, and hamper opportunities for innovation by distorting the global marketplace.

An effective privacy and data protection regime should attempt to reconcile the equally important goals of protecting global data flows and ensuring a high standard of privacy and data protection for personal data, regardless of where it is located. Policymakers wishing to create such a regime should forgo data localization measures and should seek to establish a sensible territorial scope applying only to organizations established in or targeting data subjects residing in a certain country.

The POPI in South Africa strikes this balance well and only applies to the processing of personal information where the responsible party is (1) domiciled in the Republic; or (2) not domiciled in the Republic, but makes use of automated or non-automated means in the Republic, unless those means are used only to forward personal information through the Republic.

In addition, accountability and data stewardship should serve as core principles for modern privacy and data protection regimes. Implementing these concepts entails organization-level commitments to appropriate, responsible, risk-based approaches to data protection, regardless of an organization's size or location. The accountability-based approach to data protection along with examples are discussed in the following section.

10. Allied Laws

The existing legal infrastructure in India only covers a minority of actors in its rapidly growing digital ecosystem, with the Information Technology (IT) Act of 2000 and the Telegraph Act of 1885 heavily focused on the obligations of "telecommunications service providers and certain intermediaries" (TSPs). The obligations on TSPs contained therein fall short of fulfilling certain basic data protection principles. While TRAI's efforts to fill these gaps via its 2010 Directive are commendable, we understand that India is looking towards promoting robust privacy protective behaviors across the digital ecosystem in a technology neutral way. The group of digital ecosystem players that fall under the scope of these laws represents a narrow slice of India's economy that is either relying on personal data processing today, or might do so in the future. For this reason, it is essential that any future data protection regime in India aspires to protect not only telecom subscribers, and considers adopting a risk-management approach balancing the interests of individuals, companies, and other ecosystem players, including these stakeholders' rights to responsibly access, collect, use or disclose different types of data. To this end, we suggest that the future "data protection requirements applicable to all the players in the ecosystem" stem from, and be enforced by, an agency or regulatory body empowered to take such a holistic perspective (rather than a sector specific body).

Above all, a consistent, across-the-board approach to privacy and data protection is essential to supporting innovation, job creation, and consumer confidence in India, while further strengthening the country's credibility in the global marketplace and bolstering its economic growth. The Government of India (GOI) has a diversity of policy approaches and legal regimes from around the globe from which it can take inspiration to address emerging data protection policy challenges while also taking advantage of new opportunities, without necessarily being limited to a single country's or geography's regime or approach. Rather, it is possible and likely more beneficial for India to take the best ideas from established systems in other countries to develop strong privacy regimes that preserves both individual rights and the free flow of data.

GROUNDS OF PROCESSING, OBLIGATION ON ENTITIES AND INDIVIDUAL RIGHTS

1. Consent

We recommend that organizations collecting, using, and disclosing personal data should do so in a manner that recognizes both the right of individuals to control their personal data, and their own need to collect, use or disclose it. Consent is an important mechanism to help balance these rights. However, we caution against prescriptive and detailed requirements around the timing and nature of "consent," as these often prove problematic and ineffective in practice.
It is our understanding that this is the case with the current implementation of the Shah Principles through the 2012 Personal Data Rules 4 and 5, which has become excessively burdensome, bureaucratic and prescriptive (requiring written consent and a disclosure of the names of the people responsible for the personal data collected).

For consent to be effective, it needs to be sensitive to context. As the nature of data processing activities is constantly evolving, privacy regimes should allow the methods and techniques of requesting consent to evolve at the same pace. Such regimes allow for consent to remain, where appropriate, a meaningful and effective instrument of protection. In calculating which type of consent would be most reasonable, useful factors include both the nature of the data and the value generated by its processing to the individual, to society and to the controller itself. The concept of reasonableness appears in Singapore's Personal Data Protection Act (PDPA),[10] which requires consent before the collection, use or disclosure of personal data, but does not prescribe conditions that define consent. Rather, the PDPA recognizes two kinds of consent - deemed and actual. Under section 15 of the PDPA, consent is "deemed" if: (1) an individual, without expressly giving consent, voluntarily provides the personal data to the organization for the relevant purpose; and (2) it is reasonable that the individual would voluntarily provide the data.

Singapore's Personal Data Protection Commission (PDPC)'s "Advisory Guidelines on Requiring Consent for Marketing Purposes"[11] outline ways for reasonably considering consent to be valid or invalid. Industry standards, societal expectations and practices, and the organization's role and purposes for

[10] Republic of Singapore Government Gazette No. 26 of 2012 Personal Data Protection Act 2012.

[11] Advisory Guidelines on Requiring Consent for Marketing Purposes 8 May 2015.

which it has collected, used or disclosed the data all factor into determining what is reasonable in any given circumstance. This approach is sensitive to how consent is obtained in practice. It is also dependent on the type of activity or method used to collect it, as well as the overall context of its use. Another possible approach is to include principled exceptions that remove restrictions on the use of personal data for low-risk instances. An example is Canada's Personal Information Protection and Electronic Documents Act (PIPEDA), which sets out specific scenarios loosening the limits on processing personal data for certain types of information appearing in specified publicly available sources, where the data subject had the option of removing his or her data from those sources or had directly provided the information (a concept not far removed from the National Customer Preference Register (NCPR) in India's telecom sector). Canada's PIPEDA also provides that the form of consent can vary based on the sensitivity of the information and the reasonable expectations of the individual. Moreover, the Office of the Privacy Commissioner of Canada's 2014 Guidelines on Online Consent declared that, although a data subject must give consent, an online statement or behavior that can reasonably be interpreted to mean consent, either explicitly or implicitly, may be acceptable depending on the circumstances. Organizations can also infer consent by non-action, for example, where an opt- out option has not been exercised.

It is increasingly becoming clear that large-scale, low-risk personal data processing (*e.g.,* for statistics research) can have far-reaching positive impacts and even enable greater transparency and accountability from governments in carrying out their public policies. An example of this is Brazil, where anyone can access aggregate information about the beneficiaries of public social programs such as the "Bolsa Família"[12] and hold the State accountable to the funds dedicated to these programs. Several countries that have a flexible and principled approach to consent have started to explore implementing additional habilitations to process personal data, so they too can derive similar additional benefits.[13]

2. Children's Consent

Any requirements regarding children's privacy should be consistent with current legal regimes. Specifically, it is important that a children's privacy requirement include an "actual knowledge" standard, and that companies should not be held liable if they do not have knowledge that they are collecting information from a child.

It is also important that the age of consent be consistent across legal regimes. While the EU has allowed Member States to define their own ages (between 13 and 16), COPPA in the United States sets the age at 13. Any similar requirements in India should be set to age 13 to bring more consistency across legal regimes.

Given that social media is not a fad, but in fact, if used properly, can be used as an information and entertainment source for children. Keeping the age of consent to 13 ensures the approach towards social media is educative and not borne out of fear. The most constructive approach is to educate

[12] Bolsa Família: http://www.caixa.gov.br/programas-sociais/bolsa-familia/Paginas/default.aspx

[13] In Singapore, the Personal Data Protection Commission of Singapore announced that it will be conducting a public consultation on its proposed amendments to the Personal Data Protection Act (PDPA) from 27 July to 21 September 2017. These amendments would introduce two new legal bases for data collection. In Canada, the Office of the Privacy Commissioner has also published a discussion paper exploring potential enhancements to consent under the Personal Information Protection and Electronic Documents Act.

teenagers on how to make their online experience pleasant, positive and safe. Maintaining an age of consent at 13 also allows them to connect with essentially service, educative campaigns, peer support groups at a time when they will be naturally inclined to explore the online world. Further, Increasing the age of consent could incentivise young people to lie about their age. This would result in an unhealthy relationship with online services and, perhaps, create conflict in the home.

It undermines the increasing role of social media in schools: Social media is being used in schools with increasing regularity. Whether it's for sharing information between peers, sharing information and stories between schools, or discovering new teaching methods, social media has become a crucial tool in education. Lowering the age of consent would inhibit this progress, putting Indian students at a disadvantage internationally.

3. Other Grounds of Processing

We recommend that Indian policymakers take steps to ensure their privacy framework does not unnecessarily restrict the processing of personal data. GOI should avoid *ex ante* restrictions and limitations on the processing of personal data, as these can be overly burdensome and hamper innovation and economic growth, without necessarily providing heightened levels of privacy protection. The United States, for instance, generally permits data collection and processing, unless a specific rule prohibits it. The United States has a series of targeted privacy rules that cover certain industries or types of data. On top of these specialized rules, the Federal Trade Commission (FTC) has the power to evaluate and bring enforcement action against entities in instances where it determines data processing to be deceptive or unfair. If economies choose to place greater *ex ante* limitations on the kind of data that can be processed, we recommend they offer expansive grounds for legal processing beyond consent, including the legitimate interests of the controller.

The White Paper mentions that consent has traditionally been an important mechanism of protection. Consent seeks to empower data subjects to make informed decisions about whether and how their data can be used, particularly in the offline environment. However, with the rise of innovations that rely on cloud computing, big data and the Internet of Things (IoT), relying exclusively on notice and consent mechanisms as the primary means for legitimizing data collection is no longer practicable. Consent may still be appropriate in many circumstances. But as the only basis for legitimate processing, it inevitably leads to fatigue (and even rejection) among data subjects, who confront myriad choices and may struggle to meaningfully choose among them. Furthermore, in the absence of an interface or a direct relationship with the data subject, obtaining consent is often impossible in practice. Data controllers then must choose between avoiding certain markets or risking non-compliance.

In the EU, the drafters of the General Data Protection Regulation (GDPR) acknowledged the challenges inherent in consent as a legal basis. They made sure to re-emphasize, in the list of legal grounds for processing, the importance and validity of legitimate interest grounds for processing.[14] The GDPR also

[14] It is worth noting that the Data Protection Directive of 1995 ("95 Directive") contains a variety of options to process data, including the legitimate interest basis. In fact, in 2011, the Court of Justice of the European Union (CJEU) required amendments to the Spanish implementation of the 95 Directive for overly restricting the use cases of this legal basis. In 2014, the Article 29 Working Party issued an Opinion (Opinion 06/2014 on the notion of
l egitimate interests of the data controller under Article 7 of Directive 95/46/EC) in which it explicitly states the importance of legitimate interest as a ground for processing.

includes in its recitals examples of types of processing that could be in the legitimate interests of a data controller, such as processing for: (1) direct marketing purposes or preventing fraud; (2) transmission of personal data within a group of undertakings for internal administrative purposes, including client and employee data; (3) purposes of ensuring network and information security, including preventing unauthorized access to electronic communications networks and stopping damage to computer and electronic communication systems; and (4) reporting possible criminal acts or threats to public security to a competent authority. Legal grounds in the GDPR typically found in other privacy regimes include contractual necessity, the fulfillment of a legal obligation, or the protection of vital or national interests.

4. Purpose Specification and Use Limitation

GOI should not overly restrict the processing of personal data and instead should offer ample and expansive grounds for legal processing and avoid broad & general *ex ante* limitations. Consent should not be the only legal basis for processing. Legitimate interests should be considered a legal basis for processing, even if such a basis is better defined in Indian law than it is under the GDPR.

In considering how to define a basis like "legitimate interests," it may be worthwhile to consider a use-case model. If a proposed use for data has limited impact on individual privacy (e.g., the serving of contextual ads that does not involve behavioral tracking or the creation of an interest profile), then a company should be able to rely on legitimate interests for the collection of such data. However, if the data is used for purposes that would have a significant impact on individual privacy (e.g., the creation of an interest profile for targeted ads), then consent would be required. This balanced approach would be consistent with the FTC's approach in the United States and under COPPA. India should not follow the model that the EU is now proposing under the draft e-Privacy Regulation, which would require consent even for collecting a device ID for innocuous activities such as serving contextual ads.

Companies may also have a legitimate interest in processing data for purposes of fraud detection, abuse detection, and other purposes for which one could not receive consent without defeating the purpose of the data processing activity.

5. Individual Participation Rights 1 – Transparent to Data Subject

Currently the 'sensitive personal data and information" (SPDI) Rules under the IT Act provides for access and modification rights of data subjects but do not provide the instances where the access may be refused. Lack of clear legal backing for refusal to give access may lead to wasteful litigation. The Singapore PDPA lays down an exhaustive list of instances where a body corporate may refuse to provide access. The new law in India should similarly provide the instances where a body corporate could refuse to provide access such as it being frivolous, encroaching someone else's right, etc.

6. **Individual Participation Rights 2 – Right to Object to Processing**

The White Paper contemplates the introduction of a data portability obligation in India. While the goal of promoting competition by allowing users to transfer personal data between different service providers and avoiding potential 'lock-in' is theoretically sound, we caution against the misperception that such an obligation will be straightforward to interpret, enforce or implement. It is important to

recognize the variety and diversity of services and sectors which a broad "right to data portability" might affect, as well as the intrinsic differences between a right to access and a right to 'port'. It is unrealistic to create an expectation that every piece of accessible personal information will be immediately 'portable' to another service, whether of similar nature or not. As such, we urge Indian lawmakers to fully consider the complexity inherent in a general data portability obligation and recommend that India consider narrow instances where introducing such an obligation could have a clear added value for the data subject.

REGULATION AND ENFORCEMENT

1. Enforcement Models

In our experience, the reliance on audit-based mechanisms and on a workforce of auditors is not an effective or efficient way to promote best practices, nor to avoid, or even minimize, harm. Rather than investing efforts in ex-post, audit-based mechanisms, we encourage GOI to focus on developing incentives for data handlers to develop responsible and privacy protective practices, through accountability.

One of the greatest benefits of accountability based privacy regimes is the ability to shift responsibility to the organizational level, lessening the burden on a centralized enforcement authority. In addition, a range of instruments exist that can supplement a robust and less resource-intensive data protection model than the techno- consent solution suggested in the consultation.

These instruments include self-regulation, co-regulation, 3rd party certifications, independent seals, and multilateral frameworks such as the Cross-Border Privacy Rules (CBPR), all paired with explicit legal incentives such as statutory presumptions of compliance (by, for instance, limiting the scope of investigations or the frequency of audits or enabling paths for legitimate data transfers) and statutory reductions of fines. We recommend that privacy regimes officially recognize and develop a suite of alternative co-regulatory tools that will reduce the compliance costs of an international patchwork of data protection regulations. We encourage GOI to explore all of these avenues, given the high degree of compatibility amongst them. These instruments are not mutually exclusive - on the contrary, they are complementary.

Further, we suggest that sanctions always be proportionate to the infringement. The complexity of an increasing digital economy in which various industry sector actors are involved, requires a nuanced and balanced approach. The focus should be first on deliberate, flagrant violations of the rules that could result in significant adverse effects to individuals rather than circumstances of unintentional or unforeseen violations that result in no harm to the data subject.
It is important to ensure meaningful enforcement by creating an enforcement framework that distinguishes between actors who willfully or in a grossly negligent way breach their legal obligations and cause harm to users from those who invest significant resources in not only complying with legal obligations, but often in putting in place data management practices, technologies and security measures that go beyond these requirements to ensure customer data is treated carefully. The authorities should be encouraged to use discretion in enforcement to ensure dissuasive, but fair

penalties. We suggest fostering an approach that promotes innovation, business and competitiveness, while putting the necessary controls and balances in place.

2. Accountability and Enforcement Tools

a) Accountability

Companies around the world are making significant investments to operationalize the accountability principle, such as building comprehensive privacy programs, assigning dedicated personnel to oversee privacy matters, and documenting best practices. We recommend that Indian policymakers recognize and incentivize such "good actors" and accountability practices. For example, policymakers could offer presumptions of compliance (in the ways described in the answer to Q4.) or reductions in penalties for actors maintaining such programs.

For example, in Colombia, the Statutory Law 1581 of 2012[15] establishes that the Superintendency of Industry and Commerce, during its assessment of penalties for the breach of duties and obligations of a data controller, shall take into account the specific measures and policies of the data controller in its management of personal data. It also empowers the Colombian administration to develop modern, forward-thinking supplementary regulations on binding corporate rules and on the certification of good practices in data protection. Mexican regulators have followed a similar approach; in 2016, the National Institute for Transparency, Access to Information and Personal Data Protection (INAI) launched a certification[16] mechanism to acknowledge good actors in the privacy space.

b) Enforcement Tools

i) Codes of Practice

The free flow of data is fundamental to the health of the modern global economy, delivering countless benefits and enabling access to knowledge and tools for people around the world. International data transfers and meaningful privacy protection are not mutually exclusive or antagonistic goals. Many existing regimes reflect the need to preserve multiple approaches to cross-border data transfers without weakening privacy safeguards.

One tool for cross-border data transfers is the European "adequacy model", which involves designating what is essentially a white list of countries that are judged to offer "adequate" levels of privacy protection. However, even the European Commission acknowledged that the adequacy approach alone is insufficient to handle the pressures and challenges of a hyperconnected world, and drafted the GDPR to include various alternative data transfer mechanisms. The adequacy model also presents resource challenges for regulators by requiring them to accurately assess both the privacy frameworks and respective implementations of every country on a bilateral basis (and of regularly verifying the validity of each assessment). We therefore do no recommend this approach for India.

[15] Law 1581/2012 the General Regime of Personal Data Protection, Colombia.

[16] Premio De Innovation 2017 y Buenas Practicas en la Proteccion de Datos Personales. Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

A range of other instruments exists that can act as robust and less resource-intensive data transfer models. These instruments include model clauses, binding corporate rules (BCRs), certifications, independent seals, and multilateral frameworks such as the CBPRs, consent and other available mechanisms or exceptions. We recommend that India officially recognize and develop alternative co-regulatory tools that will reduce the compliance costs of an international patchwork of data protection regulations.

Although the APEC CBPRs currently are limited in their uptake, the framework's foundational principles are flexible enough to be adopted on a much broader scale. The principle of "accountability," a key underpinning of the framework, makes the original data collector legally "responsible" for data by making sure the obligations of the data controller follow the data as it crosses borders. The United States, Mexico, Canada, Japan and Korea are already participating or have committed to participate in the CBPRs, while the Philippines, Chinese Taipei and Singapore have all taken steps to participate, and other APEC economies have signaled their interest in joining. The CBPRs offer a scalable system that holds the potential to be less burdensome to economies and companies than other systems (like EU's BCRs, which under the Directive had been very resource-intensive, tied to administrative rules, and subject to a complex approval process, but may become less so under the GDPR).

Model clauses (pre-approved, voluntary contractual commitments that are endorsed by national privacy regulators for providing adequate safeguards with respect to the protection of the privacy for international transfers of data from data controllers to data controllers or from data controllers to processors abroad) are a transfer mechanism that can be a similarly straightforward and low-burden way for organizations to comply with their obligations to protect personal data, even when it is being transferred elsewhere.

Third-party certifications, codes of conduct and privacy seals are also examples of co-regulatory tools that place binding and enforceable privacy commitments on participating organizations while providing compliance certainty for regulators, consumers, stakeholders and other industry partners.

ii) Personal Data Breach Notification

The obligations imposed on organizations that face personal data breaches differ widely across the world. Some countries impose breach notification requirements only on specific types of data, such as health or financial data. Others impose firm notification requirements once a certain threshold is triggered, like the number of data subjects, quantity of data breached, etc. The most sophisticated of these models considers that the mere act of notification itself does not yield better security or privacy for data subjects. Such models impose notification requirements in a flexible and context-dependent manner, taking into account the risk of harm, with the ultimate aim of protecting individuals in instances where breaches do happen. These regimes tend to view notification as a possible means to the end goal of protecting the subjects of breached data rather than as the end in itself.

Effective harm-based breach notification legislation recognizes the delicate balance between over- and under-notification with respect to when notices should be sent to consumers and allows organizations

to communicate with their customers in a manner that is consistent with previous communications, rather than prescribing a specific format.

Effective data breach legislation, like the U.S. State of Virginia's Breach of personal information notification statute, should not impose strict time limits for notification - it should instead create an obligation to notify without unreasonable delay once the organization has gathered information after becoming aware of an incident. The law should also apply different standards for notifying regulators and notifying data subjects. Notifying customers can be counterproductive should the alleged breach prove false or if the breach does not create a risk of identity theft. Furthermore, the sophistication of today's hackers, and the challenging nature of a post-data breach forensic investigation, calls for legislation that creates realistic, flexible, and workable time requirements. Compromised data that is encrypted or otherwise rendered inaccessible should also be exempted from notification requirements.

While Hong Kong imposes no strict legal obligation or requirement to notify the affected data subjects or the PCPD of a data breach, Hong Kong has published guidance recommending an action plan for handling breaches and encouraging data controllers to take remedial measures promptly to mitigate the loss and damage data breaches may cause to data subjects. The PCPD's action plan is sensitive to the unique circumstances surrounding different personal data breaches and includes guidance to organizations to immediately gather essential information relating to the breach, adopt appropriate measures to contain the breach; assess the risk of harm; and if deemed appropriate, give data breach notification.

Singapore's Personal Data Protection Commission follows a similar model, in its Guide to Managing Data Breaches, indicating that it is good practice to notify individuals affected by a data breach, but does not impose any general obligations. It also puts forth several mitigating factors in the event of a breach to incentivize good self-regulatory behavior: whether the organization informed individuals of the steps they could take to mitigate risk caused by a data breach; and whether the organization voluntarily disclosed the personal data breach to the PDPC as soon as it learned of the breach and cooperated with the PDPC's investigation.

iii) Categorization of Data Controllers

We strongly recommend that India steer away from a universal, across-the-board, technology-based compliance and monitoring approach to protecting privacy. Instead, we encourage incentivizing the development and use of new privacy enhancing technologies and methods as part of the risk-based accountability approach to data protection.

Registration of data controllers (even for some as yet undefined category of data controllers) has limited utility, is inconsistent with the layered approach of government and self-regulation (White Paper pg. 38) and artificially raises the costs of doing business in India, a disadvantage to India in the competitive global environment. The same is true for Data Personal Impact Assessments and Data Audits (which also can conflict with the protection of intellectual property).

Indian policymakers should look to the principles of accountability and data stewardship in the APEC Privacy framework, which help animate the concept of global privacy policy interoperability, as they

create an organizational commitment to adhere to appropriate, responsible, risk-based approaches to data protection, regardless of an organization's size or location. Policymakers should also develop clear definitions and delineations of liability between data controllers and data processors in order to ensure appropriate assignment of roles and responsibilities throughout the lifecycle of personal information that is processed.

iv) Data Protection Authority

Ultimately, an independent regulatory body will be critical to the successful implementation and enforcement of the privacy framework India develops, as it India with a centralized and "expert" authority that can keep up with the rapid evolution of technology and global privacy trends. A central authority will also be able to provide consistent guidance and interpret and enforce the law in a coherent manner.

The White Paper has asked our views on appointment of Data Protection Officers by data controllers. Making appointment of DPOs across the board as mandatory would create large compliance costs and would not be economically viable for many small and middle sized enterprises. The DPO's appointment should be based on the nature and volume of personal data being handled. The same criteria could be used to classify processing as low risk processing, medium risk processing and high risk processing. Complex and expensive regulatory compliance for enterprises doing a low risk data processing would adversely impact businesses and innovations.

Companies should be able to rely on one DPO worldwide. Any requirement to have a DPO should not require that such an officer be based in India. Rather, there should be a central point of contact for the company that can ensure that the company's approach to privacy and responses to regulatory authorities around the world is consistent.

3. Adjudication Process

India's designated DPA should aim to be collaborative and non-adversarial in its enforcement functions. Given the nascence of this space in India, as well as the potential for rapidly changing technological developments, ITI recommends that the DPA is mandated to first go through a consultative process with any industry body/ individual data controller, and only then exercise any powers to issue orders or directions. The DPA should also be given powers to reach negotiated settlements with parties prior to formal enforcement.

4. Remedies

a) Penalties

While the White Paper raises the concept of DPA discretion in allocating fines, it fails to specify any criteria bounding that discretion. This could mean that small violations risk maximum penalties, just like large ones. The risk for India is that (unlike the EU, as mentioned in the White Paper), some businesses will find the risk for fines too great to do business and will exit the Indian market.

Given this, any such mechanism should allow a “compounding” process for minor/ inadvertent errors and omissions, which will allow the company to quickly redress the underlying issues, and move on without fear of potential long-drawn criminal or other legal proceedings. A “one-size fits all” penalty should not be prescribed; rather, the penalty regime should distinguish between inadvertent errors and malicious intent to misuse data, which should fall within the ambit of existing criminal laws.