ITI Recommendations to the Telecom Regulatory Authority of India (TRAI)'s Consultation on Privacy, Security and Ownership of Data in the Telecom Sector

The Information Technology Industry Council (ITI) welcomes TRAI's initiative in opening this preliminary consultation on data protection in India. ITI is a 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 presents 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 an 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 TRAI's 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.)

Q1. Are the data protection requirements currently applicable to all the players in the eco-system in India sufficient to protect the interests of telecom subscribers? What are the additional measures, if any, that need to be considered in this regard?

As the consultation paper (CP) identifies, 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). As acknowledged in the CP, 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 CP identifies several non-TSP stakeholders – such as content and application service providers, device manufacturers, browsers, operating systems, etc. – that collect, use, disclose or control user data in the process of carrying out their operations. However, even the expanded group of digital ecosystem players set forth in the CP represents a narrow slice of India's economy that is either replying 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). 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.

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 [2]. Rather, it is possible and likely

[2] For a fuller explication of the various privacy and data protection models available to policymakers, please see Annex A.

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.

Q2. In light of recent advances in technology, what changes, if any, are recommended to the definition of personal data? Should the User's consent be taken before sharing his/her personal data for commercial purposes? What are the measures that should be considered in order to empower users to own and take control of his/her personal data? In particular, what are the new capabilities that must be granted to consumers over the use of their Personal data?

A. 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,[3] 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.

B. Sensitive 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,

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

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.

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[4]). 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) in South Africa[5] 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

[4] 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/

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

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.

C. 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),[6] 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

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

voluntarily provide the data.

Singapore's Personal Data Protection Commission (PDPC)'s "Advisory Guidelines on Requiring Consent for Marketing Purposes"[7] 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 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"[8] and hold the State accountable to the funds dedicated to these programs. Several countries that have a flexible

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

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

and principled approach to consent have started to explore implementing additional habilitations to process personal data, so they too can derive similar additional benefits. [9]

D. Data Portability

The CP 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.

Q3. What should be the Rights and Responsibilities of the Data Controllers? Can the Rights of Data Controller supersede the Rights of an Individual over his/her Personal Data? Suggest a mechanism for regulating and governing the Data Controllers.

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

[9] 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.

personal data, irrespective of legal requirements.[10]

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),[11] 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.

Q4. Given the fears related to abuse of this data, is it advisable to create a technology enabled architecture to audit the use of personal data, and associated consent? Will an audit-based mechanism provide sufficient visibility for the government or its authorized authority to prevent harm? Can the industry create a sufficiently capable workforce of auditors who can take on these responsibilities?

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 (see answer to Q.3), 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.

[10] 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.

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

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 very complementary.

Q5. What, if any, are the measures that must be taken to encourage the creation of new data based businesses consistent with the overall framework of data protection?

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[12] 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[13] mechanism to acknowledge good actors in the privacy space.

Q6. Should government or its authorized authority setup a data sandbox, which allows the regulated companies to create anonymized data sets which can be used for the development of newer services?

We support the GOI in this effort and humbly offer our expertise to help actualize its goal of promoting innovative uses of data while protecting the privacy interests of all Indian citizens.

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

[13] 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.

Our members have extensive experience with open data initiatives and we are glad to see that India is considering whether to introduce incentives designed to promote the innovative use of anonymized data sets. However, it is important to underscore that any such initiatives are both voluntary and developed in in consultation with industry, to drive consensus approaches. We urge GOI to not contemplate mandating across-the-board requirements on companies to create such anonymized data sets.

We further suggest that the GOI 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[14] to anonymization and re-identification. 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. As the CP points out, 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,

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

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).

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.

Q7. How can the government or its authorized authority setup a technology solution that can assist it in monitoring the ecosystem for compliance? What are the attributes of such a solution that allow the regulations to keep pace with a changing technology ecosystem?

As discussed in answers to Q3, 4, 6, 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.

Q8. What are the measures that should be considered in order to strengthen and preserve the safety and security of telecommunications infrastructure and the digital ecosystem as a whole?

Security is complex and there is no one-size-fits-all security solution for the digital ecosystem and telecommunications infrastructure as a whole. Effective regulations take a risk-based approach to digital and telecom security and we recommend a similar approach for India. Two examples of risk-based approaches are enshrined in the Health Insurance Portability and Accountability Act (HIPAA) in the US and the GDPR in the EU, both of which require organizations to develop and implement security measures that correspond to the risk level associated with the type and planned use of data.

We urge GOI to take a risk-based view of cybersecurity rather than an approach that attempts to guarantee or "ensure" security. Cyberattacks can never be entirely prevented. Security is a continuous process of risk management, technology development, and process improvement that must evolve with today's highly complex and dynamic computing environment. Thus, heavy-handed regulatory or legislative solutions will not provide a lasting solution to cybersecurity concerns, as they can quickly become outdated as technology changes. Effective approaches to cybersecurity demand a greater emphasis on consensus driven industry, international, standards-based approaches, such as that embodied in the Framework for Improving Critical Infrastructure Cybersecurity ("Framework"), developed via a public-private partnership in the U.S. between the National Institute of Standards & Technology (NIST), the

private sector and other stakeholders. The Framework provides an excellent example of a public-private collaboration to protect networks and stay one step ahead of hackers and cyber criminals, and is serving as a model for governments globally. For instance, Italy recently developed its own National Cybersecurity Framework, inspired by the Framework developed in the U.S.

The tech sector recognizes that cybersecurity is an essential element of data protection and that advancing the trustworthiness and security of technology and services is indispensable to protect citizens' data from hackers, cyber thieves, and those who would inflict physical harm. To this end, our companies incorporate strong security features into their products and services. Robust encryption is fundamental to building trustworthy and reliable technology products, services, and systems.

The tech sector is committed to working with the GOI to collectively help counter online terrorist propaganda, and support law enforcement in protecting Indian citizens. However, we discourage imposing legal mandates on technology providers to decrypt information when they do not retain physical possession of encryption keys or other technical means to decrypt such information, as well as other requests to circumvent or compromise data security features.

We encourage the GOI to move towards leveraging strong, globally accepted and deployed cryptography and other security standards that enable stronger safeguards for data. To preserve the interoperability and trust necessary for economic growth and stability, the GOI should also avoid policies that threaten the borderless Internet, such as data localization requirements, the extraterritorial application of laws, market access restrictions, and design requirements for technology products and services, including requirements related to encryption or communications access.

Q9. What are the key issues of data protection pertaining to the collection and use of data by various other stakeholders in the digital ecosystem, including content and application service providers, device manufacturers, operating systems, browsers, etc.? What mechanisms need to be put in place in order to address these issues?

Please refer to answer to Q1 and Annex 1.

Q10. Is there a need for bringing about greater parity in the data protection norms applicable to TSPs and other communication service providers offering comparable services (such as Internet based voice and messaging services). What are the various options that may be considered in this regard?

Please refer to answer to Q1 and Annex 1

Q11. What should be the legitimate exceptions to the data protection requirements imposed on TSPs and other providers in the digital ecosystem and how should these be designed? In particular, what are the checks and balances that need to be considered in the context of lawful surveillance and law enforcement requirements?

A. Legitimate Exceptions

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 CP 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.[15] The GDPR also includes in its recitals examples of types of processing that could

[15] 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

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.

B. Lawful Surveillance and Interception

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. The tech sector is committed to constructively engaging in efforts to transparently convene representatives of these groups in India in task forces or roundtables to inform policymaking and encourage public participation by publishing proposed policies and regulations for public comment.

Protecting and defending against national security and terrorist threats and upholding and enforcing criminal laws are fundamental missions of governments around the world. Technology can be a central tool in furthering these missions. Consistent with the tech sector's unwavering commitment to security and privacy, we are prepared to work transparently as a part of collaborative efforts with the GOI to improve the technical competencies of their workforce, to build capacity to understand the rapidly evolving nature of technology, to help prioritize resources, and to leverage technological innovation to assist in conducting lawful investigations.

Q12. What are the measures that can be considered in order to address the potential issues arising from cross border flow of information and jurisdictional challenges in the digital ecosystem?

A. Jurisdictional Challenges

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

legitimate 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.

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, both extraterritoriality of privacy rules 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.

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.

B. Flow of Information

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 Annex 2.

Annex 1 – Privacy Models

The Fair Information Practices principles (FIPPs) are at the core of the U.S. Privacy Act of 1974 (which governs the collection, maintenance, use and dissemination of personal information by federal agencies) and have formed the foundations of the laws of many economies and international organizations. Since that time, varied approaches to privacy legislation have evolved from these principles. No single approach is inherently superior or better at protecting privacy than another. Different approaches can yield different outcomes for privacy in different places, based on resourcing, implementation, legal culture, and other elements of domestic context. Therefore, various approaches have different advantages and characteristics that may make them suitable for the cultures and societies they are adopted in and may also be worthy of emulation and incorporation into more globally interoperable approaches. Below we highlight some of the dominant models of privacy legislation around the world.

Sectoral Approach

The United States has long maintained specific sectoral laws for privacy regulation relating to financial services, healthcare, children's' data, credit reporting and government agencies, among others, together with state laws. It embraces a risk-based approach to information practices and leverages the subject matter expertise of agencies that regulate specific sectors. Rather than pursuing a comprehensive domestic privacy law like the European Union (see below), these sectoral laws are supplemented with rigorous enforcement of privacy matters under the Federal Trade Commission's general consumer protection mandate, relying on Section V of the FTC Act, which prohibits "unfair and deceptive trade practices" and confers on the FTC the authority to prevent and punish such practices. The numerous FTC enforcement actions serve as a form of jurisprudence. This model reflects an overall U.S. approach that relies on a discrete separation of powers between the federal government and state and local governments, as well as between the various sector-specific agencies that have their own mandates.

Comprehensive Privacy Legislation

Other economies have chosen the path of adopting overarching privacy or data protection laws that establish comprehensive coverage of the collection and processing of personal information. These laws are often accompanied by oversight bodies to ensure compliance with the legislation. This comprehensive model is favored by the EU, where the General Data Protection Regulation (GDPR), is set to replace the EU's Data Protection Directive of 1995 ("95 Directive") in May 2018. In the context of the EU, comprehensive EU-level legislation aims to create a single market with a harmonized data protection standard across Member States. Other countries around the world like Japan, Argentina, Canada and South Africa also represent variances of this comprehensive approach.

Multilateral Accountability-Based Models

The countries of the Asia Pacific Economic Cooperation (APEC) forum endorsed a Privacy Framework in 2005 to establish an interoperable approach to data protection and promote the free flow of information in the region. The Framework is an accountability-based privacy system that can be implemented in different economies via or alongside their own privacy legal and regulatory regimes. It also sets out an enforceable co-regulatory tool for data transfers, called the Cross Border Privacy Rules (CBPRs). Operationalization of this system relies on certification bodies and third-party trust programs, backed by domestic enforcement the Privacy Framework and CBPRs together aim to improve information sharing among government agencies and regulators and facilitate the safe transfer of information between economies, while establishing a common set of privacy principles and providing technical assistance to those economies that have yet to address privacy from a regulatory or policy perspective.

Annex 2 – Cross Border Data Transfers

Mexico

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.

Canada

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.

APEC

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).

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.