USINDIA BusinessCouncil

TEL: 202-463-5679 | FAX: 202-463-3173 | usibc@uschamber.com

November 6, 2017

Shri Arind Kumar
Advisor (BB&PA)
Telecommunications Regulatory Authority of India (TRAI)
New Delhi

Subject: **USIBC response for TRAI's consultation paper on privacy, security and ownership of data in the telecom sector**

Dear Sir,

The U.S-India Business Council (USIBC) supports light-touch privacy policy principles that are balanced, flexible, globally interoperable, and protect the free movement of data which is central to India's digital transformation and the Prime Minister's *Digital India* vision. Following the Indian Supreme Court ruling in August 2017 that declared privacy to be a fundamental right for Indian citizens, the Indian government has a challenging task ahead to balance the high standard set by the court with the need to create a framework that is flexible enough to enable innovation and economic growth while encouraging foreign investment and trade without stifling global business. This historic ruling provides the foundational legal framework from which multiple Indian institutions – from the Parliament to the Telecommunications Regulatory Authority of India (TRAI) – must subsequently craft and implement a privacy policy that not only adheres to an evolving legal standard, but critically, must balance the socio-economic benefits of innovation and efficiency, with lawful limits on enforcement and national security. But perhaps most importantly, this undertaking will frame the opportunities and limits of the Prime Minister's *Digital In*dia vision. USIBC, which represents more than 350 American, Indian and global organizations is pleased to provide its perspectives as TRAI and other Indian Institutions begin to define and regulate privacy.

India is not alone in its efforts to develop privacy regimes. As evidence of the challenge of striking the right balance, of the more than 85 countries with privacy laws in place, 68 are currently updating or revising their regulations, and many jurisdictions are creating entirely brand-new laws. From the European Union (EU) to India, governments are struggling to address privacy interests within the context of their unique legal, political and law enforcement architectures. Thankfully, there are some useful international principles and frameworks from which to draw. The Organization for Economic Cooperation and Development (OECD) has laid out some useful principles on privacy and the Asia-Pacific Economic Cooperation (APEC) Cross Border Privacy Rules (CBPR) offer forward-thinking and flexible models to both protect privacy and facilitate the cross-border transfer of data and connectivity that underpins modern economies.

1615 H Street, NW | Washington, DC 20062 | uschamber.com

U.S. CHAMBER OF COMMERCE

There is no doubt that digital-enabled communications and connectivity drive innovation and economic growth. India's economy has benefitted tremendously from the increase in connectivity brought about by market liberalization as well as the growth of Indian information technology (IT) services and business process outsourcing (BPO) industries. The ability of innovative Indian firms to process data sent from all over the world has been critical to the development of India's information and communications technology (ICT) sector. It is important that as India embarks on the process of developing a national privacy framework, it bears in mind the important economic benefits created by flexible approaches to the use of data, and the importance of enabling cross-border data flows, particularly as India seeks a leadership role in advanced IT sectors such as cybersecurity, Internet of Things (IoT), cloud computing, and artificial intelligence. In order for India to become a data-driven economy, it must ensure that its data privacy framework builds trust and certainty, and enables the flexible use of data to drive innovation.

Developing India's privacy regime requires a judicious and thoughtful approach that both draws on the best global privacy principles that balance privacy, innovation and global interoperability, while designing a regime that is aligned to work within India's existing legal structure in an effective and efficient manner.

USIBC proposes the following recommendations to TRAI and other Government of India (GOI) institutions assessing and recommending options and strategies for India's policy regime:

- **Develop a Holistic Privacy Framework**: India's privacy regime should outline an overarching set of privacy norms that will apply horizontally across different industries and data processing activities rather than have numerous regulatory bodies regulating different industry sectors. Such a framework could also be tailored in limited circumstances to apply special protections to sensitive data as needed, e.g., medical health data. As TRAI develops its input to the Ministry of Electronics and Information Technology (MeitY) committee, which is drafting a comprehensive data protection law, it is important to seek a balanced, flexible, and light-touch privacy framework for the digital services ecosystem, based on the sensitivity of information and how it is used, and not determined based on the provider of the service.

- **Conduct a Detailed Analysis of Various International Privacy, Security and Data Ownership Regimes and International Norms**. As noted, some 68 countries are evaluating privacy and data ownership policies, but there lacks clarity on which model balances privacy, innovation and global harmonization of data protection rules. As a global leader in the digital economy and outsourcing domains, Indians and Indian companies regularly handle private data of other citizens, so TRAI should establish privacy norms that enable India to remain open to digital innovation and maintain its leadership in the global digital economy without impeding the free flow of data.

- **Focus on Consensus and Global Norms**: To ensure compatibility and portability with emerging global norms and developing Indian jurisprudence, and also to ensure that India's privacy regime doesn't lock out Indian companies from accessing global markets, TRAI should move slowly and avoid laying out, or recommending the enactment of, restrictive models, norms, or prescriptive measures that could stifle innovation and sub-optimize the economic benefits. Adoption of global standards improve uniformity of data protection while reducing compliance costs. Global standards should be leveraged to the fullest extent practicable before governments consider adding other data protection obligations.

USIBC appreciates TRAI's challenge ahead – and indeed the larger global privacy discussions ahead. USIBC stands committed to assist TRAI and the GOI in its efforts. USIBC and our members hope that our comments will be given a timely and sympathetic consideration. We welcome an opportunity to meet you at your convenience, and are happy to provide further information or clarification in relation to the issues in this representation. In the meanwhile, please do not hesitate to contact me or my staff: Jay Gullish, jgullish@usibc.com, in Washington, D.C., and Abhishek Kishore, akishore@usibc.com, in New Delhi. Once again, I would like to personally thank you for your leadership, and the Council and its members hope to discuss these recommendations at your convenience.

Sincerely,

Nisha Biswal
President
U.S.-India Business Council

General Inputs

Throughout our response to the consultation question below, USIBC recommends that the GOI develop a set of privacy principles similar to those developed by the OECD[1] and APEC[2] frameworks, which side-by-side outline similar privacy principles. It's important to highlight that these frameworks demonstrate how you can have data flows coexist with strong privacy protections

Table 1: OECD and APEC Privacy Frameworks Significantly Overlap

OECD Framework	APEC Framework
Collection Limitation	Preventing Harm
Data Quality	Notice
Purpose specification	Collection Limitation
Use limitation	Uses of Personal Information
Security safeguards	Choice
Openness	Integrity of Personal Information
Individual participation	Security safeguards
Accountability	Access and Correction
	Accountability

Regardless of which mechanisms India opts as its baseline, USIBC supports the development of clear, consistent data privacy regimes that protect consumers while promoting innovation through the movement of data. We believe the ability to move data across borders can coexist with strong data protection rules and recommend that India first prioritize the movement of data. Approaches to privacy must remain collaborative, flexible, and innovative over the long term—enabling solutions to evolve at the pace of the market. Thus building on the OECD and APEC frameworks, USIBC provides the core principles based on context of India's privacy debate and its focus on digital development encompassed by the PM's *Digital India* initiative:

- Ensure that Privacy Policy Is Central to *Digital India* and a Data-centric Economy
- Establish a Light Touch Regulatory Model for Privacy
- Focus on a Balanced, Technology-neutral and Flexible Regime across Sector

[1] http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

[2] http://publications.apec.org/publication-detail.php?pub_id=390

- Underscore a Horizontal Privacy Regime that Apply across Different Data Collection Activities
- Emphasize Interoperability and Consistency across Geographies, Technology and Sectors
- Contextualize Consent Policy
- Utilize Codes of Conduct and Self-regulatory Approaches around Good Data Governance

Based on the above principles, USIBC supports privacy efforts that first emphasize voluntary efforts, international best practice codes and norms, and multi-stakeholder initiatives that drive privacy protections in ways that make sense for the providers and consumers. Information is an essential input and output to the digital economy, and central to the *Digital India* vision. Thus, USIBC discourages a strict, inflexible or unclear data protection regulatory regime that impedes the free flow of data and global business transactions.

Q.1 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?

In general terms, USIBC supports the current data protection eco-system in India which is governed by Section 43A of the Information Technology Act (IT Act) 2000 of India. This provides for a redress mechanism in the event of a failure to provide reasonable security mechanism/practices in the protection of sensitive personal data resulting in a wrongful gain or loss. Moreover, the Reasonable Security Practices and Procedures and Sensitive Personal Data or Information Rules 2011 formed under section 43A of the IT Act 2000 define a data protection framework for the processing of digital data by a corporation. Lastly, the Justice Ajit P Shah committee outlined National Privacy Principles providing a positive set of principles around notice, consent, collection limitation, purpose limitation, storage, disclosure, access, security, openness, and accountability. The Shah principles also include the notion of accountability that requires organizations to have in place appropriate policies and procedures that promote good practices. Accountability puts the onus on the organization to develop such a program as well to demonstrate compliance with it upon request.

But while the IT Act and Shah Committee provide a positive foundation, USIBC strongly encourages the GOI to leverage international best practices outlined by the OECD[3] and the APEC CBPR.[4] These frameworks offer India a guidepost to develop light-touch, flexible and balanced regulation that promote the country's integration into the global digital economy. There are also plenty of other global mechanisms that can be incorporated into the law such as model contract clauses, certifications, seals, and best practices corporate codes.

As the GOI moves to develop privacy guidelines, in the first instance, governments should support privacy in a multi-stakeholder process that includes government, industry, and other stakeholders. If/when regulation is

[3] See http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm for "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data."
[4] See http://www.cbprs.org/ for more information on the APEC cross-border privacy rule system.

pursued, it should be as light-touch and flexible as possible. Any regulation should be based on general standards and not be overly prescriptive. Otherwise, regulation will not keep pace with rapidly evolving technology and market development, could diminish foreign investment and trade, and ultimately, undermine other critical GOI priorities around innovation, economic growth and job creation.

Q. 2 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?

USIBC believes it is important and necessary for transparent consent (for business-to-consumer) and/or license agreements (business-to-business) that explicitly spell out the terms and conditions for how a data controller will use personal and sensitive data. With respect to the definition of "Personal Data" in India, such definition is contained in IT Act 2000 rule 2(1)(h) of the Personal Data Rules as data which directly identifies a person or can be connected with other data to indirectly identify a person. The Indian definition of personal data is in line with international norms. The direct/indirect dual classification of personal data is found in the laws of the United States, most European countries, Australia, Singapore, Japan, and others.

The definition of "Personal Data" in India's IT Act (Section 43A) is broad. Many countries that have data protection regimes have designated a special category of data namely "Sensitive Data" that receives especially stringent protections because of the risk of inappropriate use. Many other nations, like Singapore, Hong Kong and Canada, adopt an escalating risk management approach vis-à-vis designating "Sensitive Data." Similarly, there are examples of heightened privacy requirements for data related to finances, medical health, children, dates of birth, and or login credentials. We recommend that India ensure that "Sensitive Data" and its specific applications be well defined to avoid any ambiguity and uncertainty. Further, there should be reasonable exceptions to the prohibition of collecting sensitive data, such as when the data is made public by the data subject, when data is being used for historical or research purposes, or when the data is necessary to exercise a right or obligation under the law.

We also suggest recognizing that anonymization is an important tool for data protection. We believe that anonymization helps decrease the risk to individuals. We suggest adding a clarification that personal data does not include de-identified or anonymized data. De-identified and anonymized data is that which cannot be reasonably identified and certain measures have been taken to reasonably guard against de-anonymization. Personal data should only include data or processed data sets related to reasonably identifiable individuals. This removes uncertainty and allows for responsible entities to conduct risk assessments for realistic scenarios, in particular benefitting small businesses that have fewer resources.

Many types of data collected are de-identified and/or aggregated in such a way that it would take great expense and time to determine the identity of the individual. Therefore, it is highly unlikely that the individual will be identified. In fact, in some circumstances additional data would need to be collected and retained in order to comply with the requirements in this draft. Narrow language will serve to encourage greater use of anonymization.

On consent, USIBC recommends the Indian government set forth a reasonable "Notice Principle" system that ensures data subjects receive notification about the type of data to be collected and how they will be put to use. Data subjects may review and accept/decline the privacy policies in the notification before data collection. This enables data subjects to make informed decisions about whether they are comfortable with the data collection practices. The data collected can then be used to the extent such uses are consistent with the terms described in the notification.

As India is a multi-linguistic country, any consent and terms of consent provided only in English or Hindi will be limiting data providers' ability to comprehend the details. Data collectors should voluntarily provide the consent form and terms of consent in the language of the user and or the language of choice.

There should be a balance between empowering the individual to exercise choices about their privacy and not overloading privacy policies with too much detail that can confuse consumers or cause them to ignore the policies altogether. If the requirements for consent are restrictive, that would hinder many widely accepted business-to-business practices and commercial data usage, raise costs for businesses and consumers, and deprive consumers of desired products and services.

A context-driven, risk-based approach to consent has proven successful worldwide. There are a wide range of mechanisms that enable data subjects to control and consent to collection and use of their information, and some of the more robust opt-out mechanisms provide stronger protection for data privacy than weaker opt-in mechanisms. The GOI should not impose a separate obligation to obtain consent prior to any use of such data. Such a requirement is, as a practical matter, untenable in the modern cloud environment. If the policy is interpreted as requiring separate consent every time before making use of personal data, in addition to the prior notification regarding the intended collection and use of such data, it threatens to impose significant and unnecessary burdens on businesses and the data subjects. Such an interpretation is inconsistent with many carefully-struck, balanced international best practices.

While publicly available data should be subject to access rights and data security obligations, users of that data should not be subject to all consent requirements. Since the data is obtained from public sources, obtaining consent is not feasible since the user does not interact with the data subject. Specific guidance could be taken from the proposed "Notification of Purpose" requirement being introduced by the Singapore Personal Data Protection Commission as per the Public Consultation for Approaches for Managing Personal Data in the

Digital Economy issued on July 27, 2017. The Consultation seeks to replace consent where it is not practically possible to seek user consent before sharing his/her personal data for commercial purposes. Such challenges for a consent regime may be present in the context of Smart Cities, the use of unmanned aerial vehicles or in retail centers that employ Wi-Fi hotspots. As the paper notes, the fast emerging digital economy is presenting challenges for consent-based approaches to personal data protection. The growth of IoT devices, machine learning, and artificial intelligence has given rise to the ability to collate and analyze large amounts of data, opening up new possibilities to derive insights that can yield enormous benefits for individuals and society. Relying only on consent for the collection, use, and disclosure of data may create unnecessary obstacles in the development of the digital economy. An approach such as the one being proposed in Singapore that calibrates the balance of responsibilities and adopts pre-emptive measures through a "Notification of Use" can meaningfully address privacy concerns while creating the conditions to unlock the benefits of big data.

Finally, while consent is an important ground for processing data, consent should not be the only ground for processing data. In particular, express consent should be limited to situations where consent is the sole basis for collecting and processing data. Provisions related to consent in general should consider the context of the data processing and allow for a flexible approach to avoid confusing consumers with repeated requests for consent in often trivial situations. Any framework needs a range of options which can be applied pragmatically and in appropriate contexts to enable the full range of beneficial data uses in the modern information age while also protecting the individual.

With the above in mind, data privacy continues to be a rapidly developing area on a global scale. Any regulation in India should follow a legal framework that relies on strong principles and business-level accountability to avoid over-inclusive regulations, and enable greater flexibility.

Q.3 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.

USIBC supports the current distinction in responsibility between a data controller, which determines the means and purposes of processing data and a data processor, which processes the data on behalf of another organization. A data controller should remain primarily responsible for meeting privacy obligations and for providing redress to individuals. So long as a data processor merely processes data on behalf of a data controller its responsibility is to follow its data controller's instructions and to assist the data controller in meeting its privacy and security obligations. Liability should be allocated among organizations that process data within an ecosystem according to their demonstrated fault giving rise to the liability. Future data protection law should expressly recognize that data controllers have proprietary rights over anonymized, purposely-designed datasets.

Q. 4 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?

USIBC would like to caution against any technology-enabled mandatory audit-based architecture covering privacy for multiple technical, commercial, and practical reasons. A technological audit mechanism is not only dangerous as it could increase the impact of cyber breaches or unlawful surveillance, it is also not practical solution as it would lead to more regulations. USIBC members would prefer a mechanism that incentivizes privacy protective practices through self-regulation. Organizations should be encouraged to develop voluntary ***self-enforced risk-based frameworks*** based on government-established data standards developed through multi-stakeholder consultation (e.g., personal and sensitive data). This would allow them to focus efforts on high-risk data uses to minimize harms while monitoring low-risk situations such as B2B data processing or other common and everyday uses of data. We note that an accountability-based approach obligates companies to undertake assessments to ensure they are adhering to their stated practices. Creating a framework based around government visibility into an organizations' privacy practices is not consistent with such an accountability-based approach which already include self-assessment requirements.

Q. 5 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?

Data is both a resource for, and product of, the digital economy. It is vital to the growth of the digital economy that any framework implemented to protect personal and sensitive data be balanced to enable flexibility and innovation to spur growth in the digital economy and ensure continuing foreign investment in India. Critical to the growth of the digital economy is the ability to move data across borders. Similar to investment, human capital and technology, data has emerged as a critical input into innovation, entrepreneurship and economic growth. In a free market, the proper role for government is to balance risk with enabling innovation and economic growth. Over-regulating the market can interfere with the freedom of trade that businesses are guaranteed by the Indian Constitution and dis-incentivize competition, investment, and trade, and create business inefficiencies. Further, like other forms of commerce, data competition is good, if not fundamental to innovation. When businesses compete, consumers benefit. For technology companies to develop products that offer the most convenience to users, they must invest in R&D and constantly find better ways of using data to deliver consumer benefits. Such techniques include data aggregation, analytics, and behavioral analysis. The direct result of these techniques is innovation and market disruption.

The world's leading big data companies started small but grew because they constantly innovated and disrupted existing market monopolies. New data-based businesses that are successful have followed the same high-innovation, disruptive-market approach. Several Indian businesses have succeeded in winning consumers and

capturing the market based on the superiority of their products. The government has an understandable interest in promoting Indian businesses. However, it should do that without sacrificing the interests of Indian consumers who continue to benefit from existing big data businesses. As India moves forward in developing its data privacy framework, policymakers should keep as a foundation of any future regulation the economic benefits that India has received from the flexibility permitted to its ICT services industry to send and receive data from all over the world, and maintain a flexible and clear approach going forward to enable Indian digital innovators.

Q.6 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?

With respect to sandboxes for data covered by regulation and licenses, USIBC would support efforts to utilize data to develop and trial new services, however, such efforts should be voluntary in nature, and ensure that aspects of proprietary information and liability are clearly defined. In other words, USIBC would not support regulations that mandate companies to provide anonymized data for use in a public data sandbox. Singapore is looking to utilize sandboxes with an initial focus on fintech, and could provide an example of how these types of activities can occur based on voluntary cooperation.

Here, the Consultation could look at the benefits of anonymization of data implemented by Mexico and Japan. Under both countries' laws, an organization that commits to anonymizing personal information is permitted to process data and disclose it to third parties without requiring the consent of data subjects or being held to the same obligations that apply to identifiable data. Similarly, in the EU, the General Data Protection Regulation (GDPR) does not apply to anonymized data.

While promoting anonymization, regulations should enable technology-neutral methods and should not require specific technologies because standards of anonymization naturally evolve over time as new technical capabilities and privacy enhancing technologies enter the marketplace. The UK Information Commissioner's Office (ICO) has laid out an advanced risk-based approach 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.

Q. 7 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?

TRAI should consider non-technical solutions for monitoring privacy based on the principles outlined, emphasizing the specific context and self-enforced risk-based frameworks. A mandated technology solution could create new, or increase existing compliance hurdles, and could create a user backlash towards "a big

brother approach" that adds onerous compliance issues and negatively impact the growth of the digital economy. As part of the U.S. Chamber of Commerce, USIBC points to a recently published report, Seeking Solutions: Attributes of Effective Data Protection Authorities, which outlines seven key traits that effective data protection authorities (DPAs) share and offers examples of how DPAs have incorporated these traits. Overall, the key finding is that the most effective and efficient data protection authorities encourage compliance through treating the regulatory community as partners rather than adversaries. Based on the Chamber's publication, USIBC recommends that any authorized authority that will oversee data protection follow these seven traits:

1. Promote Education and Awareness
2. Seek Feedback
3. Offer Guidance and Assistance
4. Act Judiciously
5. Act Transparently
6. Strive for Coordination and Cooperation
7. Be Business and Technology-Savvy

DPAs should also adopt a public-private-partnership (PPP) model, collaborate and work with leading industry stakeholders to use the latest technologies to enhance their efficiency, effectiveness and transparency. They might publish blog posts and newsletters, host webinars or use social media platforms to raise awareness, such as by hosting pages and videos on YouTube, Twitter and Facebook, enabling them to informally interact with the public and regulated community to raise awareness about data protection issues.

Because the data ecosystem is globalized, Indian IT companies have been able to connect to data generated internationally in order to do business, thus the global nature of the internet should be protected. There should be no technical controls on cross-border data flows. Such controls would alter the internet's fundamental architecture. That would slow the growth of the internet in India. India's privacy framework must preserve the flexibility to move data in and out of India.

Q. 8 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?

USIBC would encourage the government to issue the encryption policy as envisaged under Section 84 of the IT Act. While Indian Internet service providers (ISPs) are bound to 40-bit encryption keys, the rest of the internet is significantly more secure. The Department of Telecommunications (DoT)'s ISP license restricts the use of encryption to key lengths of 40 bits and below, which is an antiquated low standard. Specific regulators such as the Reserve Bank of India (RBI) and the Securities and Exchange Board of India (SEBI) stipulate the use of longer encryption keys for certain purposes, which has resulted in multiple, inconsistent encryption standards. Hence, USIBC encourages the GOI to enable the use of end-to-end encryption wherever businesses determine it

is necessary. Encryption regulations should be harmonized and based on global standards to promote the use of strong encryption. Moreover, since weak encryption is a competitive disadvantage in privacy-conscious markets, the government should encourage Indian businesses to make strongly-encrypted products to compete in global markets.

Robust encryption is fundamental to building trustworthy and reliable technology products, services, and systems, and therefore, plays an important role in data protection. No one should be allowed to deliberately undermine the security of data and data-related products, services, systems, and maintain confidentiality of source code and protect the security of customers' data. It is not advisable to impose 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.

Third, cybersecurity is an essential element of data protection. Security of technology and services is indispensable to protect data from hackers, cyber thieves, and those who would inflict physical harm. To this end, the tech sector incorporates strong security features into its products and services to instill trust, including using published algorithms, and limiting access to encryption keys. The GOI should move towards leveraging strong, globally accepted and deployed cryptography and other security standards that enable stronger safeguards for data.

Q. 9 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?

On consent, there should be a balance between empowering the individual to exercise choices about their privacy and not overloading privacy policies with too much detail that can confuse consumers or cause them to ignore the policies altogether. If the requirements for consent are restrictive, that would hinder many widely accepted business-to-business practices and commercial data usage, raise costs for businesses and consumers, and deprive consumers of innovative products and services. While consent is an important ground for processing data, it may not always feasible/practical to obtain.

Data protection regimes can incorporate a range of mechanisms into their frameworks that enable flexibility for companies and better protect data subjects. For example, even the EU GDPR offers six legal bases for processing and collecting that does not just rely upon consent. In another example, Singapore recently initiated industry consultation proposing notification of purpose instead of consent where it is not practically possible to seek consent. Further, we recommend legitimate interest as a legal basis for processing data. Legitimate interest

protects individual data, often better than a consent approach, by requiring that a risk-based assessment be made in each instance.

Providing consumer services through digital channels requires a flexible consent framework that allows for the movement of data taking into account the potential risk of harm to the data subject. As an example, data licensed by regulators, certified for data security standards and governed by specific purposes or use limitations entail far less risk than the transfer of data to other institutions with no legitimate purposes. Therefore, implied or informed consumer consent for data use and transfer, rather than express or affirmative consent, is an appropriate default. Such a proportionate consent framework should be implemented to avoid increased costs, limits on access to the best available technology, and curtailing the provision of services.

Additionally, organizations need to protect their data, intellectual property, IT systems and networks, and other assets against fraudulent uses or cybersecurity attacks. Such measures often require the processing of personal data of individuals, including those who may be engaged in fraudulent activity or cybersecurity attacks. Obtaining consent in those circumstances would defeat the purpose of processing. These examples of processing could also be based on a legitimate interest exception.

India's privacy regime should outline an overarching set of privacy norms, combined with a policy framework that can be tailored to meet the specific requirements of the varying types of personal data processed by different industries with differentiated data risks profiles and stakeholder communities. Thus, as the GOI regulates privacy, there are a common set of norms and processes that can be applied to data, but that may vary based on specific privacy profiles, cyber security risks, and other generally-accepted criteria. As TRAI develops its input to the MeitY committee, which is drafting a comprehensive data protection law, it is important to seek a balanced, flexible, and light-touch privacy framework for the digital services ecosystem, rather than apply different privacy regimes to different providers of digital services.

To reiterate our recommendation on consent from Q.2, in order to encourage innovation and avoid unnecessary costs to businesses, we suggest indicating that for less sensitive data there should be an informed, implied, opt-out, or implicit consent standard. A context-driven, risk-based approach to consent has been proven successful worldwide. It may also be beneficial to allow for legitimate interest-based processing of sensitive data in contexts where obtaining consent would be impossible or impracticable.

Consent should be implied for commonly accepted data collection and use practices, such as processing a transaction requested by the consumer, risk management, data security, and service and app performance analytics. We also suggest allowances for data transfers for processing for disaster recovery purposes, whether in-country or internationally, provisions should be made to allow transfers, without consumer consent, pursuant to contract clauses that permit the processor to abide by reasonable administrative, technical and physical safeguards.

Q. 10 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?

The data protection framework should also aim to promote a light-touch regulatory regime for all market players including internet based voice and messaging services to encourage investment and innovation in these new types of services. Therefore, there is no need for introduction of additional data protection requirements to bring parity as the data protection requirements as incorporated in the IT act apply to all the stakeholders in the internet ecosystem. Further, the data protection law needs to be flexible to enable and support new age digital services which can flourish only when international cross border data flows are enabled. India needs to keep its approach to data protection dynamic so that it can remain nimble and responsive to a constantly changing global privacy environment.

Q. 11 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?

When addressing this question, USIBC recommends that TRAI differentiate between privacy and products within the consumer space versus those utilized within a business or enterprise environment. Building trust and confidence in digital services, as well as regulatory certainty for both individuals and businesses are essential to the growth of digital services. However, there needs to be recognition of the specificity between the services that are sold to consumers versus services typically provided to large enterprise customers to avoid extending the expansive data protection obligations to such providers of enterprise services. Therefore, for any data protection regime to be future proof it needs to explicitly recognize a distinction between residential services (sold to consumers) and non-residential services (sold to (large) business customers) to avoid a one-size-fits-all approach.

USIBC also recommends that when government agencies do submit requests for information for a variety of reasons, those requests should follow certain principles such as:

- Requests must follow an established process
- Requests should be narrowly drawn
- Request must satisfy legal requirements, and should generally include legal process and judicial review (i.e., a subpoena, court order or search warrant)

With respect to the legitimate exceptions to the data protection requirements imposed on TSPs and other providers in the digital ecosystem, USIBC firmly believes that providers should be responsible for

implementing a privacy program and should be able to demonstrate compliance upon request. We do not encourage the inclusion of sanctions that are related to total or partial suspension or prohibition of the personal information treatment activities. For instance, sanctions that would terminate a database's operations or suspend/prohibit data processing, even if for a limited period of time, would shut down business activities which could harm consumers. Such a measure could limit investment and services offered in India due the burdensome nature of such a regulation. Any type of sanction aimed at suspending data processing should only affect the data collected while breaching the law's provision, and should not result in a suspension of all data collected and stored in a given database.

As noted previously, one important protection requirement includes the use of encryption to protect against malicious actors, hostile countries, and cyber criminals. TRAI should also note that strong encryption is a competitive market edge and driver of innovation that facilitates usage and new applications, and the availability of encrypted products and services will allow Indian products to better compete in privacy-conscious markets. If end-users believe that data is secure, they may be more willing to "trust" innovations that might require additional user information, such as medical health or financial data, by increasing the adoption rate for digital products. Managed effectively, improving trust and encryption offer India – its industry and citizens –socio-economic benefits and industrial competitive advantage.

Q.12 What are the measures that can be considered in order to address the potential issues arising from cross border flow

In support of our mission to promote commercial ties and socio-economic well-being of people in both the United States and India, USIBC emphasizes our support for the free flow of all economic resources – capital, people, technology, and data. Privacy versus the cross-border flow of data is not an "either/or" proposition. The flow of data is essential both to a modern economy and to the use of data for commercial purposes and for societal progress.

Instead of forcing rules that endeavor to protect privacy through limiting data transfers, narrowly tailored and proportionate laws will provide better oversight and protect individual privacy. Data protection requirements should not be so restrictive that companies have to keep data local, such as policies that require consent for any data transfers.

The APEC CBPR system[5] is a good model, which recognizes more legitimate mechanisms such as privacy marks and organizational codes of conduct that are certified by a competent authority or third party. Although India is not an APEC member, it could allow recognized certification bodies to authorize such mechanisms, such as the Accountability Agents in the APEC CBPR system to avoid approval bottlenecks within this

[5] See http://www.cbprs.org/ for more information on the APEC cross-border privacy rule system.

competent body. Mexico is an example of a country taking steps in this direction and has recently put in place a self-regulatory mechanism in order to be compatible with the CBPR system and allow for even more secure and reliable data flows.[6]

Including widely-accepted concepts of "model contracts and clauses", "standard contractual clauses", and "global corporate standards" or "global corporate rules" (known in Europe as "Binding Corporate Rules" or "BCRs.") will also help India seamlessly integrate into the global digital economy. Such clauses should allow a company or group of companies engaged in joint economic activity to use the same structure for international data transfers in order to ease the cost and time of doing business. These clauses typically include minimum conditions such as detailing the structure of the company, information about the data and transfer process, and how to apply general data protection principles. Recognizing these mechanisms will allow the seamless flow of data and will position India as an active player in the global digital economy. India should endeavor to make its privacy framework interoperable with global practices in order to maintain the flexibility to enable an innovative and dynamic digital economy.

We believe that concepts of country-level "adequacy" are often problematic, inconsistent, and deter innovation. By limiting data transfers to the countries on a list, India will find it more difficult to interact with the global digital economy, prone to global security risk and will deprive its citizens of the cutting-edge products and services they seek. International data transfers are responsible for the rise of new businesses around the world and the digital economy. The Internet and its capacity to enable the free flow of information is a major boost to economic trade and new business models operating exclusively online. If there is a need for a formal authorization from the competent authority for international data transfers, day-to-day business operations as well as the development, growth, and spread of innovation and new technologies, such as the IoT, would be negatively impacted.

Lastly, and a critical point, is that any measures to restrict international data flows of Indian citizens could produce a backlash among key commercial partners as India, via its outsourcing business, handles private data of citizens of many other countries, including financial and legal information processed as part of back-end offices and third-party outsourcing contracts. A data protection framework that facilities cross-border data flows will enable business of all sectors and sizes to reach new customers in foreign markets inexpensively and manage relationships with foreign clients.

End Comments

[6] See http://www.rea.ifai.org.mx_catalogs /masterpage /Home.aspx