AT&T Global Network Services India Pvt. Ltd.
Registered Office
13th Floor
Mohan Dev House
13, Tolstoy Marg
New Delhi-110 001, India
CIN: U72900DL2005PTC142096

Tel: 91.11.4240 8774
91.11.4240 8775
Fax: 91.11.4240 8774
www.ap.att.com

AGNSI/TRAI/CP-PSOD/2017-18
November 6, 2017

Shri Arvind Kumar
Advisor (Broadband & Policy Analysis)
Telecom Regulatory Authority of India
Mahanagar Doorsanchar Bhawan,
Jawahar Lal Nehru Marg, Old Minto Road,
New Delhi – 110 001

Sub.: Response to TRAI Consultation Paper [No. 09/2017 dated August 9, 2017] on Privacy, Security and Ownership of the Data in the Telecom Sector

Dear Sir,

AT&T Global Network Services India Private Limited (AGNSI) is pleased to submit its response to TRAI consultation paper No. 09/2017 dated August 9, 2017 on Privacy, Security and Ownership of the Data in the Telecom Sector.

We trust that our submission will merit the kind consideration of the Hon'ble Authority.

Thanking you,

Respectfully submitted,
for **AT&T Global Network Services India Private Limited**

Naveen Tandon

Naveen Tandon
Authorised Signatory

Encl.: As above

Telecom Regulatory Authority of India
Consultation on Privacy, Security and Ownership of Data in the Telecom Sector

I. Introduction:

AT&T Global Network Services India Private Limited (hereinafter AT&T) respectfully submits its input to the Telecom Regulatory Authority of India (TRAI) in response to the invitation for comment on the *Consultation on Privacy, Security and Ownership of Data in the Telecom Sector* released 9 August 2017 (Consultation). AT&T welcomes the opportunity to provide its input to the TRAI as it prepares its recommendations to Government of India for consideration in developing a privacy and data protection framework, and we will be pleased to support this effort throughout the process.

AT&T has a firm company commitment to the privacy and security of our customers and users. Our privacy program is based on a set of principles that explain our commitments to transparency, respect, choice and control, and security, and it is reflected in our Code of Business Conduct, as well as our Privacy Policy.[1] We appreciate this opportunity to share our views with the TRAI as the Government considers the evolution of its overarching Privacy and Security policy.

As expressed by TRAI in the Consultation, AT&T agrees that government policy should be sufficiently flexible to enable industry to grow and create new services. We commend the TRAI for recognizing that the global trend of new services emerging on the basis of data provides value to customers and business alike, and that such benefits will be stifled by restrictive policies that have the effect of impeding this growth and risking the digital economy of India falling behind. As the TRAI develops recommendations from this Consultation, AT&T urges TRAI to draw from existing global privacy regimes and to encourage the Government of India to adopt a consistent policy, built upon rules and protections that are tailored to context and strike the balance of targeting potentially harmful uses of consumer data while allowing for its many beneficial uses. Specifically, the privacy frameworks developed by Asia Pacific Economic Cooperation (APEC) and the Organisation for Economic Co-operation and Development (OECD) represent widely accepted international standards for the collection, use, and transfer of personal data which contain accountability mechanisms for individuals and state actors who wish to challenge data management practices. AT&T would recommend that the Government look to these frameworks when considering new rules on the protection of personal data.

---

[1] See www.att.com/privacy

As we discuss in greater detail below, an effective privacy policy should adhere to the following pillars:

- Privacy rules should be consistent across the global digital ecosystem.
- Privacy rules should be based on the sensitivity of the information collected and used.
- The legitimate interests of government in addressing important objectives must be handled through fair, accountable and uniform procedures that govern when and how private companies may be compelled by the government to provide information.
- Cross-border data transfer mechanisms are essential to the global digital economy, and governments should ensure that these are predictable and interoperable.

Because this Consultation is one of many privacy policy or rule makings under consideration in parallel in India, AT&T urges the TRAI to work towards an end-state that establishes a competitively and technology neutral privacy framework that applies based on the sensitivity of the information collected and used and avoids the implementation of sector privacy regimes that apply based on the operations of the service provider.

Rules should be consistent across the ecosystem.

Throughout this Consultation, the TRAI solicits input as to whether differential treatment is required of telecommunication service providers (telcos) and Internet service providers as compared to providers of other services (see specifically questions 1, 8, 9, 10 and 11). As the Government develops a national privacy framework, we cannot under emphasize the importance of establishing a uniform privacy policy framework applicable across industries in India. The TRAI must work with other stakeholders to recommend a privacy policy that is based on the sensitivity of information collected and used. A light touch policy framework that is competitively and technologically neutral and avoids duplicative and inconsistent regulation will benefit consumers, competition and innovation.

Current Indian regulation differentiates between data protection for 'telco subscribers,' who use licensed services directly from the telcos and Internet service providers (ISPs), and the users of unlicensed services (which could be provided by the telco itself), including apps that are delivered over the telecom or Internet infrastructure. For the licensed services, telco subscribers are provided protection under the Indian Telegraph Act and the licensing agreement. For the unlicensed services, users are protected through the Information Technology Act (IT Act) and related rules covering protection of sensitive personal information, in addition to generic laws covering matters of contractual relationship between a service provider and a user, which also apply to telcos and licensed services.

This regulatory inconsistency should be reconciled. Regulation of privacy and technology should reflect the realities of the modern digital economy. In a connected world where individuals use multiple devices and services from different providers, privacy regulations that apply to only one set of technologies, data class or industry players can create customer confusion: consumers expect that one set of rules will apply to the processing of their personal data, regardless of whether a device manufacturer, an application provider, or a connectivity provider does the processing. Promoting consistency helps mitigate this confusion and satisfy customer expectations.

The existing paradigm in India that only applies to telcos is based on a premise that specialized privacy regulations are appropriate for telecommunication services (provided by telcos and ISPs); however, this basis paradigm is out of step with other economies. On the contrary, as a recent study by Peter Swire explains, in today's online ecosystem, consumer data is collected and used by many different types of entities using a wide variety of sophisticated technologies (see Peter Swire et al., Online Privacy and ISPs: ISP Access to Consumer Data is Limited and Often Less than Access by Others, February 29, 2016 at 3, attached). In this environment, network provider access to user data is neither comprehensive nor unique. In fact, Swire concludes that "other companies often have access to more information and a wider range of user information than [network providers]." (Swire et al., Online Privacy and ISPs at 2).

Furthermore, although some countries continue to maintain separate regulations aimed at protecting the confidentiality of communications, consumers are increasingly adopting messaging and other communications services that operate as applications over broadband connectivity. Because these services are not offered by traditional telecommunications operators, they fall outside the scope of antiquated, narrow regulations that target the telecommunications sector. India should avoid a policy framework in which different rules apply to communications based on the company that processes them.

The best way to for the Government to ensure the protection of consumer privacy is through a competitively neutral framework based on the sensitivity of the information collected and used. The objective for India going forward should be to establish a technology and platform neutral data protection law that applies horizontally across the ecosystem. The Ministry of Electronics and Information Technology (MEITY) has already constituted an expert committee and is working to draft a comprehensive data protection law that would cover all the sectors and bring uniformity and the Honorable Supreme Court has declared privacy as a fundamental right recognized in its recent ruling.

at&t

Specific questions posed in the TRAI consultation

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?

We live in a connected world where individuals use multiple communication devices and services from different providers. In this world, privacy rules should be consistent across the global digital ecosystem. Privacy regulations that apply to only one set of technologies, data class or industry players can create confusion. Rather, consumers expect that one set of common rules will apply to the processing of personal data, regardless of whether a device manufacturer, an application provider, or a connectivity provider does the processing. Promoting consistency helps mitigate this consumer confusion and satisfy expectations.

As recognized by the TRAI in this Consultation, Internet-enabled services and apps and data driven innovation are significant contributors to the economy. A recent study[2] by ICRIER estimates that apps contributed a minimum of USD 20.4 billion in the year 2015-16 to India's GDP, and this contribution is expected to grow to USD 270.9 billion by 2020. This would be nearly eight percent of India's GDP. A report by Analysys Mason[3] estimates that data driven innovation contributed USD 10 billion to India's Gross Value Added (GVA) in 2015 and this contribution is expected to rise to USD 50 billion by 2020.

To make data driven innovation compatible with data privacy, it is critical to empower users, without over-regulating data controllers or data collection. The public policy focus should be on providing regulatory certainty and consistency, and support the principles of choice, user control and security, making companies accountable through self-regulation without being prescriptive. The framework should recognize the market/industry driven developments have led to an increase in user transparency and trust.

---

2 http://icrier.org/pdf/Estimating_eValue_of_Internet%20Based%20Applications.pdf 2

3 http://report.analysysmason.com/DDI_Emerging_APAC/DDI%20in%20emerging%20APAC%20-%20Final%20report%20-%202016%2008%2006%20-%20FINAL.pdf

The existing provisions under the telecom licenses aptly cover the privacy requirements and there is no requirement for any addition as it binds the licensee. For example the following clauses of the internet service license clearly state the privacy and data protection requirements which a licensed ISP has to adhere with few stated exceptions: These are sufficient and have been mandated ever since licenses were issued.

32.1 .....However, the LICENSEE shall have the responsibility to ensure protection of privacy of communication and to ensure that un-authorised interception of MESSAGE does not take place.

32.2 Subject to conditions contained in these terms and conditions, the LICENSEE shall take all necessary steps to safeguard the privacy and confidentiality of any information about a third party and its business to whom it provides the SERVICE and from whom it has acquired such information by virtue of the SERVICE provided and shall use its best endeavors to secure that:

(i) No person acting on behalf of the LICENSEE or the LICENSEE divulges or uses any such information except as may be necessary in the course of providing such SERVICE to the Third Party; and
(ii) No such person seeks such information other than is necessary for the purpose of providing SERVICE to the Third Party.

Provided the above para shall not apply where:

(i) The information relates to a specific party and that party has consented in writing to such information being divulged or used, and such information is divulged or used in accordance with the terms of that consent;
or
(ii) The information is already open to the public and otherwise known.

32.3 The LICENSEE shall take necessary steps to ensure that the LICENSEE and any person(s) acting on its behalf observe confidentiality of customer information.

32.4 The LICENSEE shall, prior to commencement of SERVICE, confirm in writing to the LICENSOR that the LICENSEE has taken all necessary steps to ensure that it and its employees shall observe confidentiality of customer information.

34.10 The LICENSEE shall be responsible for ensuring privacy of communication on its network and also to ensure that unauthorized interception of message does not take place.

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?

(i) Definition

The Rules framed under Sec 43A of the Information Technology Act define personal information *as any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person.* This definition is generally consistent with that which underlies other data protection frameworks, and Indian authorities have correctly recognized that purpose and context play a role in determining whether a particular piece of information in isolation or in combination with other information constitutes personal information. As Justice A.P. Shah observed,

> *The same piece of information can be personal in the hands of a certain data controller and functionally anonymous in the hands of another data controller- e.g.- possession of license plate number in the hands of an insurance company can be considered as personal information but the same plate number in the tape of a security camera in a petrol station will not be personal information, as the station has to take considerable efforts for determining the identity of the person."* (Justice A P Shah Report, 2012; Page 67).

Justice Shah's statement reflects the position of experts that data can fall on a spectrum of identifiability,[4] and the ease with which it can be linked to an individual may impact the controller's responsibilities. The European Union's General Data Protection Regulation reflects this spectrum, recognizing that pseudonymization and encryption of personal data are effective safeguards for managing privacy risk and encouraging the innovation and development of the future consumer and societal benefits.[5]

Finally, any data protection framework should recognize that information that is de-identified or part of an aggregate and anonymous dataset does not constitute personal information.

---

[4] See, e.g., Jules Polonetsky, Omer Tene, and Kelsey Finch, "Shades of Gray: Seeing the Full Spectrum of Practical Data De-Identification," Santa Clara Law Review vol. 56, p. 593 (2016).

[5] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1-88, recitals 28-29, Articles 6(4)(e), 32, 40, 89.

at&t

(ii) Consents

International standards for the protection of personal data establish that individuals should receive timely notice regarding the collection of their personal data and be able to exercise choice and control over its collection, use, and disclosure. At the same time, data protection principles are inherently flexible, aimed at restricting potentially harmful uses of data while allowing for many beneficial uses. A regime that limits collection and use to circumstances in which the data subject has consented may foreclose beneficial uses of data and fail to keep pace with technological developments that may render consent impractical or undesirable.

In India today, sections 4 and 5 of the Reasonable Security Practices and Procedures and Sensitive Personal Data or Information Rules of 2011 ("Personal Data Rules") require data controllers to give users understandable privacy policies that explain how their data will be used. No data can be collected without voluntary, written consent, and users must be given the names of people responsible for personal data. These provisions reflect the principles of Notice and Choice contained in the APEC Privacy Framework and other international standards regarding the protection of personal data.[6]These standards recognize that while consent is a fundamental legal basis for the collection and use of personal data, data protection law should recognize alternative bases as well. The APEC Privacy Framework establishes that personal information "should be obtained by lawful and fair means, and where appropriate, with notice to, or consent of, the individual concerned." The commentary notes that "there are circumstances where providing notice to, or obtaining consent of, individuals would be inappropriate."[7] Such circumstances might include where information is in the public domain, or where it is collected through the use of connected devices in the context of a Smart City. Similarly, the OECD Privacy Framework specifies that data should be used for the purposes for which it was collected, as well as other purposes that "are not incompatible with those purposes" when notice is provided to the data subject; consent may be unnecessary to use or disclose data for different purposes when this is done "by the authority of law."

---

[6] The similar principles of Collection Limitation, Purpose Specification, and Use Limitation are contained in the *OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, C(80)58/FINAL, as amended on 11 July 2013 by C(2013)79 ("OECD Privacy Framework"), and they reflect the principles stated in the Madrid Resolution (2009) of the International Conference of Data Protection and Privacy Commissioners.

7 See, APEC Privacy Framework, Collection Limitation Principle and commentary. See also, APEC Privacy Framework, Uses of Personal Information.

Data protection frameworks in the European Union, United States and Singapore, to cite a few examples, provide multiple bases for the collection and use of personal data in addition to the consent of the data subject. The EU General Data Protection Regulation establishes six bases for the lawful processing of data. These include for the purposes of the controller's legitimate interests, which encompasses the prevention of fraud and for direct marketing purposes.[8] In the United States, an individual is permitted to opt out of most uses of personal information for purposes that are distinct from the original purpose of collection. In Singapore, the Personal Data Protection Act of Singapore recognizes consent as the primary basis for the collection and use of personal data, but creates exceptions to consent where data is publicly available, where it is necessary in the national interest, where it is necessary to cooperate with a law enforcement investigation, and for certain research purposes, among other bases.[9]

Any privacy framework should also give individuals greater power to control the collection and use of their information depending on its sensitivity. For example, collection and use of sensitive personal information requires the individual's opt-in consent under both the U.S. Federal Trade Commission's privacy framework and the EU General Data Protection Regulation (GDPR).[10]

The TRAI should recommend that any new Indian privacy framework provide data subjects with transparency and means to exercise choice and control over collection and use of their data, while allowing for the flexibility that is critical to facilitate other beneficial uses of data. For example, public authorities can gain valuable insights related to transportation and health through the analysis of pseudonymized datasets. It is likely that not all data subjects would consent to these uses of non-sensitive personal information, rendering the datasets, and the benefits that they might provide, incomplete. For all of these reasons, a flexible regime based on the sensitivity of data and how it is used is preferable to one which depends exclusively on consent.

---

8 According to Article 6, processing of data is lawful "only if and to the extent that at least one of the following applies: (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes; (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; (c) processing is necessary for compliance with a legal obligation to which the controller is subject; (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person; (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child." See also, recital 47.

9 Personal Data Protection Act (No. 26 of 2012) (Singapore), sections 13 et seq., Second, Third, and Fourth Schedules.

10 "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers," U.S. Federal Trade Commission, March 2012; General Data Protection Regulation, Article 9.

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.

To apportion the rights and responsibilities of a data controller, the legislative framework should clearly define a data controller and recognize the rights of the data controllers and users are not necessarily in conflict. To make data-driven innovation compatible with data privacy, it is critical to empower users, without over-regulating the data controllers or data collection. The public policy focus should be on preventing harm to users, misuse of personal information and making companies accountable without being overly prescriptive.

AT&T recommends that in drafting a new policy framework for data protection, the Government look to well-established international standards governing data protection. For example, the APEC Privacy Framework is a business-friendly and user-centric framework which also supports cross border data flows. It recommends privacy principles of *Preventing Harm*, *Notice*, *Collection Limitations*, *Uses of Personal Information*, *Choice*, *Integrity of Personal Information*, *Security Safeguards*, *Access & Correction* and *Accountability*. The principles of *Preventing Harm* and *Accountability* particularly stand out for being pragmatic and outcome focused by making organizations responsible without stifling trade and innovation. These principles are informed by the Fair Information Practice Principles (FIPPs) and the OECD Privacy Framework, and they were drafted with the digital economy in mind.

Instead of prescribing privacy practices in form of administrative requirements, the privacy framework should define the broad principles and requirements and allow organizations to design their own privacy programs that could be based on due diligence guidelines. While organizations should be allowed to self-regulate, they should be held accountable for any violations. In case of any breach or complaint, the onus to prove due diligence should lie with the organizations.

Given that the Ministry of Electronics and IT is already working on a comprehensive data privacy law which would be applicable across sectors, this issue should be addressed horizontally across the digital economy and should be outcome driven and focus on building the necessary ecosystem rather than just exclusively focusing on regulating data controllers.

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?

There is no need for proactive government monitoring, as market forces are sufficient to drive this change and there are positive developments to show this evolution. Technology platforms are already building such capabilities to empower users to better understand their personal information usage and control their data. Also, given the scale and volume of transactions happening on the Internet at every second and the multiple players involved in each transaction, it may not be practically possible to create a centralized *ex ante,* tech-based compliance architecture / system. It is recommended that policy responses focus on building understanding among users through education and awareness, making organizations accountable through self-regulation and strengthening grievance redress.

Any policy must take into account that the digital economy is thriving in part because most businesses work hard to maintain user trust and confidence. For example, AT&T's commitment to transparency, respect, choice and control and security for our customers is reflected in our Privacy Policy, and security for our customer and end-user data is one of AT&T's core privacy principles. Consumers, industry and government will be better served by government and industry collaborating to develop guidelines that reflect international standard and best practices, and forego mandated external audits.

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?

New technologies, including Big Data and the Internet of Things (IoT) solutions, do not require the invention of new regulations for privacy and security. For example, privacy in the IoT requires a balance of traditional standards and new methods: principles such as data minimization remain relevant, but they should be flexible to allow for innovation and development of future consumer and societal benefits of collecting and using such data. De-identification and pseudonymization of data are effective practices for addressing privacy risk and should be encouraged.

Instead of taking specific measures tailored to specific industries, the TRAI should work with other stakeholders to recommend a privacy policy that follows the pillars outlined in our introductory comments and reiterated herein below. These pillars strike the balance needed to both encourage business growth and innovation and protect consumer data:

- Privacy rules should be consistent across the global digital ecosystem.
- Privacy rules should be based on the sensitivity of the information collected and used and not established based on industry collecting the information.
- The legitimate interests of government in addressing important objectives must be handled through fair, accountable and uniform procedures that govern when and how private companies may be compelled by the government to provide information.
- Cross-border data transfer mechanisms are essential to the global digital economy, and governments should ensure that these are predictable and interoperable.

It is also essential that enforcement of policies be managed through a transparent, consistent and stable review process that incorporates fundamental principles of due process.

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?

If the Government were to establish such a tool, industry participation should be voluntary and industry should not be compelled to surrender proprietary data. Data is an important asset which is utilized by business to create useful products and to gain insights derived from such data.

For example, in the United States, AT&T is developing its own type of "data sandbox," utilizing its software-defined networking, which includes access technologies like LTE Advanced and 5G. AT&T Network 3.0 Indigo will feature a data communities platform, which will enable dynamic, on-demand combinations of data to be sourced from multiple entities and merged into shared communities to derive insights in a highly secure environment. It will connect the best human intellect and machine learning capital in order to scale capacity for learning and enhance collaboration among community members to help solve problems.[11]

---

[11] *Data Communities on AT&T Network 3.0 Indigo*, © 2017 AT&T Intellectual Property, available at: http://policyforum.att.com/att-innovations/indigo/.

Rather than compete with industry-driven solutions such as these, the Government should seek to learn from and encourage the development of industry best practices related to these efforts.

Industry should be able to use public data sets and share data responsibly, but a government mandate is not justified or necessary and should not be viewed as an exclusionary alternative to the private sector collecting, processing and analyzing data to deliver new and innovative services. To the extent such a tool is established, strong encryption and other safeguards will be essential.

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?

A government owned and operated monitoring system is unlikely to be able to maintain pace with changes in such a dynamic industry without placing an enormous burden on the government. It is also likely that if the government installs a system of monitoring and surveillance it privacy concerns would be raised. Industry is best placed to comply with the privacy principles under a self-regulatory framework, and putting users in control is critical. Instead of government monitoring, the legislator should be encouraged to recognize and endorse a culture of corporate accountability, that would limit the ex-ante enforcement approach to a minimum. This has been the approach of other privacy enforcement authorities who have seen how effective privacy and data protection are better achieved by incentivizing companies to adopt best practices and demonstrate that they are accountable to their users. This approach, which is perfectly compatible with effective enforcement, constitutes the essence of the APEC Cross Border Privacy Rules (CBPRs) regime.

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?

We highly recommend the TRAI support raising the current 40-bit encryption key to which the Indian ISPs are bound under their license. This standard of 40 bits and below is far below the industry norm and below the standards employed by OTT providers and email service providers.

While governments around the world are grappling with how to best address safety and security of the digital ecosystem, India's licensing conditions imposes an artificially low standard on ISPs that disadvantages consumers and hamstrings the ISPs ability to compete for business from privacy conscious consumers. India should modernize and the existing policy as it has not proved to be practical given the dynamic nature of keys and absence of any framework to accord approval. Instead, the Government should work cooperatively with industry to frame a flexible encryption policy which promotes the security of services, networks and data.

AT&T advocates for the development of polices that utilize existing frameworks and international standards will not only support innovation and growth, will also promote better security. In applying those policies, it is important that one technology not be favored over another. In the United States, the National Institute of Science and Technology ("NIST") Framework (the "Framework")[1] is built around the concept of risk management, which we believe is the best means to address cybersecurity, particularly given the rapidly changing nature of the threats. The Framework can be a useful tool for companies to evaluate their cybersecurity risks and build a risk management plan specific to their business.

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?

As stated above, regulation of privacy and technology around the world should reflect the realities of the modern digital economy. In today's online ecosystem, consumer data is collected and used by many different types of entities using a wide variety of sophisticated technologies. As stated above, privacy regulations that apply to only one set of technologies, data class or industry players can create customer confusion: consumers expect that one set of rules will apply to the processing of their personal data, regardless of whether a device manufacturer, an application provider, or a connectivity provider does the processing.

Promoting consistency helps mitigate this confusion and satisfy customer expectations. Furthermore, privacy rules should provide a level playing field and avoid distorting competition.

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?

As stated previously, the objective for India going forward should be to establish a technology/platform neutral data protection law that applies horizontally across the ecosystem to all parties that collect and use personal information.

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?

We recognize that governments can have a legitimate interest in addressing important objectives such as national security, public safety, law enforcement, and preventing harm to children. We also believe that government legal regimes should respond to technological changes through fair, accountable and uniform procedures that govern when and how private companies may be compelled by the government to provide information. The law should clearly establish the circumstances under which public authorities may issue demands for personal information, the forms that such demands must take, and the specific authorities that are empowered to make them. Companies should be permitted to challenge demands that appear inconsistent with the legal framework in court.

Before AT&T responds to any legal demand, we determine that we have received the correct type of demand based on the applicable law and the type of information sought. AT&T validates the legality of the restriction under applicable law and seeks to minimize any adverse impacts on our users.

Q.12 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?

Cross-border data transfer is essential to the global digital economy, and governments should ensure that these transfer mechanisms are predictable and interoperable. Governments can build trust in the global economy – and specifically in the cloud computing and IoT industries – by creating an environment for service providers to follow industry best practices and guidelines regarding the cross-border use and protection of personal data, while providing appropriate accountability mechanisms for those who wish to challenge data management practices. Agreements such as the APEC Cross-Border Privacy Rules Framework, Privacy Shield, and the EU-US Principles for ICT Services are positive examples of such mechanisms.

India, an established global hub of data processing and development and with a robust Information Technology and IT-enabled services industry that revolves around processing and handling of data received by it from across the globe, should be particularly sensitive to and supportive of cross border data flows. Any adoption of a restrictive regime in this behalf by the Government can boomerang as it may lead to other outsourcing countries placing similar restrictions on data flows to this country, which in turn will hurt the Indian economy and employment. In fact, TRAI in its recommendations on cloud computing has not recommended any restriction on cross border data flow.

Finally, government should commit to using Mutual Legal Assistance Treaties (MLAT) and similar processes when they seek access to data that is stored beyond their borders. AT&T supports government efforts to streamline these processes, for example by updating MLATs to cover communications associated with evolving networks and services.

Conclusion

AT&T thanks TRAI for the opportunity to provide input to the *Consultation on Privacy, Security and Ownership of Data in the Telecom Sector.* We remain at your disposition in the event that we can provide further input or participate in the process as it progresses.