TRAI Consultation on Privacy, Security and Ownership of the Data in the Telecom Sector

(IBM RESPONSE)

1. Are 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?

The current legislative and regulatory system in India is inadequate to address the emerging digital ecosystem, where management of Data is the key issue. Existing legislations that are covering the subject of Data namely The Information Technology (IT) Act of 2000 and the Telegraph Act of 1885 are NOT good enough to protect the interest of the Telecom Service Providers (TSP) and consumers. Protecting Data was not adequately addressed in these legislations primary because Data was not thought to be an area to be regulated and protected at the time of framing/amending these legislations.

Even "the Telecom Commercial Communication Customer Preference Regulations, 2010" is inadequate to protect the growing concerns of the telecom users with respect to the multiple types of Data being generated by telecom users – call records, meta-Data, user generated contents of text, sound and video, GPS Data/location services etc.

It is a welcome effort that the Consultation Paper has attempted to identify various stakeholders of Data management such as device manufactures, content and application service providers, operating systems, browsers etc. that gather user Data. However, this too is only incomplete list of players in Data Generation and Management Ecosystem.

However, since Data is not only generated by devices/services of communications, it should be appropriate to limit this Consultation to Data generated through devices/ services of communications, and the larger issue of Data Protection and Regulation should be left to the expert committee set up for the purpose by Ministry of Electronics and Information Technology.

Data management should be seen from FIVE basic pillars – 1) Ownership 2) Storage 3) Movement 4) Security and 5) Business.

Ownership should define different methods of Data sharing/licensing. Ownership should be defined on the basic premise that individual owns his/her data and user works on it then returns it. User keeps it on a permission granted by the Owner, but has no right on the Data and therefore cannot share it. However, user is permitted by an agreement to use it and share any value addition created on the basic Data. The only exception on sharing by User is when an explicit licence agreement is given to the User to share it.

Storage should cover different types of storage options ranging from conventional server storage and Data centres to Cloud storage. It should also cover Public Cloud, Private Cloud and Hybrid Cloud, besides including various storage mediums of movable nature.

Movement of Data is critical in Data management. There is a need to define Data movement across the border and Data stored within the borders. Data movement section should make sure to include the Distributed Ledgers and Blockchain wherein Data is moved and stored in a borderless manner through shared ledgers but in a secure way.

Security of Data is ensured through Encryption and various Cyber security tools. This could include encrypted machines to encryption software. Various security software that would prevent malware, spyware and backdoors are important be covered in this area.

Finally, Data leads to business, and **Business** is at the core of generation, storage and sharing of Data. Principles for Data management should be well thought out in a manner that facilities creation and growth of Data related businesses in Big Data and Analytics, leading to employment generation and economic growth.

We recommend a comprehensive approach covering all these five areas as essential in managing Data in a way that supports innovation, job creation, and economic growth. Indian policymakers seeking to address challenges in Data management have an assortment of policy approaches and legal regimes from around the globe to derive inspiration, information and inferences.

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?

Beyond defining the Ownership, this section should point out the importance and necessity for transparent license agreements that explicitly spell out the terms of Data ownership and sharing.

A. Definition of Personal Data

Definitions of "Personal Data" and "Sensitive Data" are basic tenets of regulation of Data Management and protection of Privacy rights. **We believe that people's Data is their own, and that Data policies and regulations should be fair and equitable, prioritize openness, and respect intellectual property.** A glance at the definitions of "Personal Data" in policies and legislations around the world reveal that it is often all inclusive and flexible. This consultation could pick up some vital threads from these global examples.

European Union GDPR defines[i] “Personal Data’ as “information relating to an identified or identifiable natural person (‘Data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location Data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person”.

Hong Kong’s CAP 486 Personal Data (Privacy) ordinance[ii] defines “Personal Data” as (a) relating directly or indirectly to a living individual; (b) from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and (c) in a form in which access to or processing of Data is practicable. It also defines “Personal Data System” as any system, whether or not automated, which is used, whether in whole or in part, by a Data user for the collection, holding, processing or use of personal Data, and includes any document and equipment forming part of the system; and “Personal Identifier” as an identifier (a) that is assigned to an individual by a Data user for the purpose of the operations of the user; and (b)that uniquely identifies that individual in relation to Data user, but does not include an individual’s name used to identify that individual.

In Singapore’s Personal Data Protection Act 2012[iii], “Personal Data” is defined as Data, whether true or not, about an individual who can be identified (a) from that Data; or (b) from that Data and other information to which the organization has or is likely to have access.

However, in some regions “Personal Data” is not defined, instead it is defined as “Personal Information”. For instance, in the Canadian Personal Information Protection and Electronic Documents Act (PIPEDA)[iv] “Personal Information” means information about an identifiable individual, and in the South African Protection of Personal Information Act (POPI)[v] “Personal Information’’ means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person.

Lot of deliberations have happened at the Working Party and finally the Article 29 Working Party[vi] concluded that the test of whether information is personal or not is a dynamic one and should also consider the state of the art in technology at the time of the processing and the possibilities for development during the period for which Data will be processed.

Since the definition of “Personal Data” in India’s IT Act (Section 43A) is similarly broad, it is worth noting that identifiability may not be a meaningful differentiator to determine what should and should not be covered by Data protection rules.

<u>B. Sensitive Data and SC’s 3-Tier Approach Suggestion</u>

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 nations like Singapore, Hong Kong and Canada, adopt an escalating risk management approach vis-a-vis designating “Sensitive Data”.

Sensitive Data, wherever it is specifically defined in Privacy legislations, have described as Data on racial/ethnic origin, political opinions, religious or philosophical beliefs, trade-union memberships, health, criminal offenses and sex life.

There is a third option similar to that of the United States, where specific laws covering certain types of Data that require greater protection such as financial Data, Social Security Numbers, specific health information, children’s information, login credentials and/or full dates of birth, are in force.

We recommend this Consultation should ensure that the types “Sensitive Data” is well defined to include all information that are intimate to the Data subject. Indian Supreme Court’s suggestion during the hearing of the Privacy Case to classify “Personal Data” as “Intimate,” “Private,” and “Public” and treat these accordingly while regulating Data should be worth following. This proposed three-tier approach should remove a lot of ambiguities surrounding classification of Personal Data and ensure deserving Privacy for “Intimate Data,” and to some extent to “Private Data.”

C. Consent – What, When and How

The collection, use and disclosure of personal Data should be done recognising the right of individuals to control their personal Data. Any regulation in this space should take into account the fact that the organisations/platforms collect Data with elaborate Privacy Statements and Terms and Conditions which are hardly read by the users. Therefore, it is the responsibility of the State to ensure that such elaborate documents should not be used as a ploy by the collector of Data to deceive the user at any given point in time.

Today, most service providers and online platforms including ‘apps’ use the “Notice” through a ‘Consent’ to collect Data. However, users in their eagerness to access certain services or benefits, press the ‘accept’ button and share their personal information. Therefore, regulating what Data can be collected and what cannot should come within the purview of the governments in the interest of protecting the safety, Privacy and security of its citizens.

Opt-out option is one way of securing the user’s Data beyond the time of contract or consent for which it was originally given for. Once a user has opted out of a service or a platform, Data collector should not be allowed to use the Data which has already been collected and kept with the collector. Data collector should destroy the collected Data, the moment Data provider has opted out. Any violation by retaining Data, selling Data, using in any other forms for any purpose by Data collectors needs regulation.

India being a multi-linguistic company, any Consent and terms of Consent provided only in English or Hindi will be limiting Data providers’ ability to comprehend the details. Data

collector should provide the Consent form and terms of Consent in the language of the user and/or in the language of choice.

In order to frame the “Consent” it is advisable to explore global legislations and policies in this space. For instance, the concept of reasonableness is key to Singapore’s Personal Data Protection Act (PDPA), which requires consent before personal Data can be collected, used or disclosed, which is classified as deemed and actual. Under section 15 of the PDPA, consent is “deemed” if: (1) an individual, without actually giving consent, voluntarily provides the personal Data to the organisation for the relevant purpose; and (2) it is reasonable that the individual would voluntarily provide Data.

Canada’s PIPEDA prescribes different forms of Consent depending on the sensitivity of the information and the reasonable expectations of Data provider. Further, the Office of the Privacy Commissioner of Canada’s 2014 Guidelines on Online Consent suggests that an online statement or behaviour that can reasonably be interpreted to mean consent, either explicitly or implicitly, may be acceptable depending on the circumstances.

D. Data Portability to Empower Data Subject

It is a welcome step that the Consultation has contemplated introduction of a Data portability in order to empower the Data subject. Portability is a way to end Data monopoly by the select few, but it can have far reaching consequences impacting the small and medium enterprises, if not well thought out while regulating.

The right to Data portability will require businesses to ensure that they hand over the personal Data provided by an individual in a usable and transferable format to the regulator/Government or to a third party. European GDPR provides that the right to Data portability is not just limited to social networking sites but it cover cloud computing, web services, smartphone systems and other automated Data processing systems. It applies to a wide range of Data collection sources such as social media, search engines, photo storage, email or online shops. It is equally applicable to banks, pharmaceutical companies, energy providers, airlines - even small businesses like pizza shops or tailors if they are Data controllers. Article 20 of the EU GDPR “Right to Data Portability”[vii] provides that “Data subject shall have the right to receive the personal Data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those Data to another controller without hindrance from the controller to which the personal Data have been provided.”

While the concept of Data portability is generally aimed at online service providers including social networks, search engines and online retailers, broad interpretations can also have a large impact on the insurance, banking, telecommunications, healthcare, transport, and retail industries.

3. What should be the Rights and Responsibilities of 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 Data Controllers.

World over the new school of thought is arriving that deploying Data Controllers many not be a right option to deal with monitoring. It will be very difficult to create a capable workforce of auditors and the industry will not welcome auditing of proprietary information. Instead, a framework of accountability should be the right way forward.

This consultation should explore adopting the well-established accountability-based system. Accountability fixing can have the focus of Privacy governance covering all entities to accept responsibility for collecting, processing and/or using personal Data, irrespective of legalities involved.

This should require sufficient protection measures which may include various security measures such as encryption, anti-hacking security, filtering out malware/spyware and avoiding 'back doors' by entities who collect, process, store and transmit Data as vendor or business partners.

4. Given the fears related to abuse of 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?

It is not feasible to create a capable workforce of auditors, nor for auditing systems to keep up with the rapidly evolving technology. The viable alternative is to allow industry to self-regulate based on government provided data standards. For example, government policy can offer standardized data verification tools that industry can use to self-regulate quality control of its data.

Unauthorized access of Personal Data can be detected by reviewing a record of system like an Audit Log. Maintaining a chronological record of system activities (by both internal and external users) is often the best way for reviewing activity on a computer system to detect and investigate Privacy incidents. Audit Logs should also be named using a clear naming convention. Audit trails are used to reconstruct and examine a sequence of activities on a system that leads to a specific event, such as a Privacy incident.[viii]

Access monitoring software that provides real time (or close to real time) dynamic review of access activity can also be useful for detecting unauthorized access to personal information.

Since most of the audit work can be done with technological solutions, question of skilling workforce on this domain is not a priority requirement. However, given the nature

of dynamic and learning workforce in India, availability of pool of workforce for Data Audit is not a concern for the industry, and should not be to the Government as well.

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?

Businesses using Data for Analytics is growing exponentially, and they play around the grey area, and therefore, there is an urgent need to bring in rules of the game to create level playing field for the benefit of all businesses.

Entities should use analytics through accountable processes with accountability beginning with an acknowledgment that Analytics can have a negative as well as a beneficial impact on individuals. Entities should implement appropriate safeguards to protect the security of information that it uses in Analytics. Data security should be reasonable when measured against the kind of information that is collected and processed, and the decisions that are made with it[ix].

6. Should Government or its authorised authority setup a Data sandbox, which allows the regulated companies to create anonymised Data sets which can be used for the development of newer services?

Entities should not be encouraged to dump “Personal Data” as “Anonymous Data” by masking the relevant field. First type of anonymous Data should be Data received as anonymous from Data subject he/she is not interested or keen on revealing identity. Similarly a Consent for anonymization can also obtained at the time of Data collection or later by Data Controllers. In addition, if Data subject has given the Consent to use Personal Data for Analytics and Data thus derived from the Analytics of multiple Primary Data sets could also be treated as Anonymous Data. Thirdly, for the interest of citizens, the State should be able to classify certain Personal Data as “Anonymous” after masking/deleting certain Data identification information. However, using such Data for Business and commercial purposes or allowing trade in such ‘Personal Data’ converted as ‘Anonymous Data’ can attract widespread criticism.

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 GDPR does not apply to anonymized Data.

While promoting anonymization, regulations should prescribe technology neutral method and should not advise specific technologies because standards of anonymization naturally evolve over time as new technical capabilities and Privacy enhancing technologies enter the marketplace. The UK’s 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[x].

Where anonymization is not possible, entities should also be granted decreased liability or compliance burdens as incentives for partially anonymizing, or "pseudonymizing" Data. For example, under the GDPR, entities who pseudonymize Data are permitted to further process that Data for additional purposes that are compatible with the original purpose for Data's collection, without needing to get consent.

Anonymization and pseudonymization of Data can yield large benefits to the society as the world cross new milestones on the technological frontier. The concept of Data minimization – limiting the collection of personal information to that which is directly relevant and "necessary" to accomplish a specified purpose – has been a foundational Data Privacy and security principle. Recent technological developments in the areas of Big Data Analytics and Machine Learning encourage lawmakers to revisit the underlying cost-benefit analysis of this principle. Big Data Analytics, which involves examining large Data sets to uncover hidden patterns, unknown correlations, market trends and other useful information, require that policymakers carefully consider what constitutes "necessity."

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?

As laid out in the 9-judge ruling of the Supreme Court, the county needs to move to a regime wherein Privacy will be enshrined as a fundamental right of its citizens.

For a country or a national regulatory authority, it is not advisable to work on a centralized, compliance and monitoring approach, instead incentivize the development and use of new Privacy enhancing technologies and methods as part of the risk-based accountability approach to Data protection.

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?

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.

Encryption hardware/servers that offers higher level of security to Data and Data processing would be another option to strengthen security of national assets of critical nature including telecommunications infrastructure.

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 instil trust, including using published algorithms as default cryptography approach as it has greatest trust among global stakeholders, and limiting access to encryption keys. Government of India should move towards leveraging strong, globally accepted and deployed cryptography and other security standards that enable stronger safeguards for Data.

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?

Not only that vital Data collected by telecom services need to be protected with clear ownership rights to the user with authority to use, transact and delete Data, Government should also be restricted to access and use Data, except in rarest of rare circumstances, and only with proper legal authorisation from courts.

Apps and Platforms require certain information from the user in order to provide him with certain services. Therefore, with a valid legal basis for data collection, such as consent, apps can be allowed to collect personal information/Data. However, it would be the responsibility of the Apps to ensure that Data collected thus should not be used or diverted for anything beyond which it is originally meant and the legal basis on which its collection is based.

Browsers and Operating Systems have a key role to play here and need to be regulated as well as they indirectly access Data collected by the apps and platforms, and their Data access may not include the legal basis upon which the original collector relied. By being party to Data collection process and participating as a party to the process, Browsers and Operating Systems are, by default, Data owners and need to be regulated in the same way Data collector is regulated, with the same set of rights, responsibilities and accountabilities.

The last category in this space is the Search engines who often collect Data from the search words and queries. Search engines use Artificial Intelligence protocols and algorithms to gather, compile and create patterns of the user, without an explicit legal basis such as Consent of the user. In some cases, the search engines which have email

clients as well, go beyond the search words/queries, and even prey on the subject line and in some instance mail texts for key words to understand and analyse the user and his/her interests. While this may be a natural progression of the evolution of AI and Machine Learning technology, the user need to be made aware of the way it works and a proper legal basis, such as Consent should exist in order for the Search Engines and Email clients to operate in such an intrusive manner. Regulating this intrusion of Privacy need to be in measured appropriateness in terms of Definitions, Legal Basis such as Consent, Portability and any other aspect that may be required to be considered.

10. Is there a need for bringing about greater parity in 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?

Difference between the TSPs and ISPs have been narrowing down with the entry of smartphones. Both service providers today offer IP-based voice and messaging services in some form or other. Therefore, for all regulatory purposes on Data protection there exists no reason why they should be treated separately.

There is a third set of players who is not licensed by Government – Service providers who completely ride on Internet using Internet protocols, but offer voice, video-cum-voice and real time chat and messaging services. This segment has been one of the reasons for the spurt in social media growth and are accessible over mobile, web and hybrid forms. In fact, most of the social media platforms offer these services in some way or other. In addition, there are Instant messaging platforms and video telephony platforms, and in some cases offering both from the same platforms. In terms of pure Data protection perspective, they should have complete parity because the type of Data collected by them are similar to what is being collected by TSPs.

11. What should be the legitimate exceptions to 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. Governmental Access to Data:

Governmental access to Data is not significantly stronger or weaker in any one country, and that any perceived locational advantage of Data insulation from Governments can be rendered irrelevant by Mutual Legal Assistance Treaties (MLAT). There has been cases where some regional businesses mislead their customers that if Data is stored with their Cloud service, it will be insulated from Governmental Access and will be more secure than that of other providers whose Cloud services are located at another geographical jurisdiction. It is in the interest of the businesses to offer restricted Access

to Governments for matters related to National Security, Safety of citizens and Economic Security.

The United States and member states of the European Union have bilateral MLATs that allow governmental authorities on both sides of the Atlantic to request access to Data stored on the servers of a Cloud service provider physically located in or subject to the jurisdiction of the foreign nation. Pursuant to an agreement governing MLATs between the U.S. and EU member states, a request for Data shall only be denied on Data protection grounds in “exceptional cases.” Article 13(3) of Framework Decision 2008/977/JHA of the Council of the European Union allows transfers of personal Data for law enforcement purposes even to countries whose Privacy regimes have not been found “adequate” by the EU where there are “appropriate safeguards.” The phrase “appropriate safeguards” is widely interpreted to include international agreements such as MLATs[xi].

Therefore, it could be reasonably argued that there emerges a strong international collaboration on Data Sharing, irrespective of the location of the Storage. This is going to be stronger and stronger as the countries realise the need to reinforce their Data sharing regimes, very similar to tax treaties and extradition treaties.

The below chart shows that the in Australia, Canada, Denmark, France, Germany, Ireland, Japan, Spain, UK and US, companies are required to provide Data to governments in order to facilitate in any legal or investigative purpose. Except Germany and Japan, countries have made it mandatory to share Data even in case of a request from a foreign country, though Japan and Germany insist for bilateral cooperation on the subject.

The only argument some countries voice in favour of localisation of Data for the purpose of Governmental Access does not and will hold much water as Access to Cloud is not impaired by location as it can be accessed by the Governments irrespective of the base location. The below chart shows the status of Governmental Access to Data in major countries around the world:

	May government require a Cloud provider to disclose customer data in the course of a government investigation?	May a Cloud provider voluntarily disclose customer data to the government in response to an informal request?	If a Cloud provider must disclose customer data to the government, must the customer be notified?	May government monitor electronic communications sent through the systems of a Cloud provider?	Are government orders to disclose customer data subject to review by a judge?*	If a Cloud provider stores data on servers in another country, can the government require the Cloud provider to access and disclose the data?
Australia	Yes	Yes, except for personal data without a legal purpose	No	Yes	Yes	Yes
Canada	Yes	Yes, except for personal data without a legal purpose	No	Yes	Yes	Yes
Denmark	Yes	Yes, except for personal data without a legal purpose	No	Yes	Yes	Yes
France	Yes	Yes, except for personal data without a legal purpose, electronic communications	No	Yes	Yes	Yes
Germany	Yes	Yes, except for personal data without a legal purpose, electronic communications	Yes, except may withhold until disclosure no longer would compromise the investigation or an investigation of serious criminal offenses, national security, or terrorism	Yes	Yes	No, not without cooperation from the other country's government, except for telecommunications content data
Ireland	Yes	Yes, except for personal data without a legal purpose	No	Yes	Yes	Yes
Japan	Yes	No – must request data through legal process	No	Yes	Yes	No, not without cooperation from the other country's government**
Spain	Yes	Yes, except for personal data without a legal purpose	No	Yes	Yes	Yes
United Kingdom	Yes	Yes, except for personal data without a legal purpose	No	Yes	Yes	Yes
United States	Yes	No – must request data through legal process	Yes, for content data, except when the government obtains a search warrant or orders disclosure would compromise the investigation	Yes	Yes	Yes

* "Review by a judge" encompasses either an initial review when issuing the court order, warrant, etc. or subsequent review when the court order, warrant, etc. is challenged by the service provider or customer.

** Under a recently revised criminal procedure law, Japanese law enforcement officials may obtain copies of data located on a remote server if a computer in Japan is able to create, change, or delete data on the server, even if the server is located outside of Japan. Although computers of Cloud providers may be able to change or delete customer data, the Japanese Ministry of Justice currently takes the position that computers of Cloud providers are not subject to the law. It is not certain, however, whether Japanese courts would read this same limitation into the law.

B. Legitimate Exceptions

Any new policy on Privacy framework should not unnecessarily restrict the processing of personal Data. The Government of India 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 policy makers of the General Data Protection Regulation (GDPR) in EU acknowledged the challenges inherent in using Consent as a legal basis and made sure to re-emphasize, in the list of legal grounds for processing, the importance and validity of legitimate interest grounds for processing. The GDPR also includes in its recitals examples of types of processing that could be in the legitimate interests of a Data controller, such as processing for: (1) direct marketing purposes or preventing fraud; (2) transmission of personal Data within a group of undertakings for internal administrative purposes, including client and employee Data; (3) purposes of ensuring network and information security, including preventing unauthorized access to electronic communications networks and stopping damage to computer and electronic communication systems; and (4) reporting possible criminal acts or threats to public security to a competent authority. Other legal grounds in the GDPR that are also typically included in Privacy regimes are contractual necessity, the fulfillment of a legal obligation, or the protection of vital or national interests.

In the United States, for instance, Data collection and processing is generally permitted, unless prohibited by a specific rule. As the CP acknowledges, the United States has a series of targeted Privacy rules that cover certain industries or types of Data. Outside of these specialized rules, the FTC has the power to evaluate and bring enforcement action against entities in instances where Data processing has been determined to be deceptive or unfair. If India does choose to place greater ex ante limitations on the kind of Data that can be processed, we recommend offering expansive grounds for legal processing, beyond consent and including legitimate interests of the controller.

B.Lawful Surveillance and Interception

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 Government of India 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.

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?

A.Jurisdictional Challenges

Countries that enact barriers to Data flows make it harder and more expensive for their companies to benefit from the ideas, research, technologies, and best practices that accompany Data flows.

For a variety of reasons, policymakers often ignore international law obligations and principles to protect their citizens' Data, even when Data leaves their national jurisdictions. Privacy laws that proclaim extraterritorial applicability – for instance by providing that they apply to any entity providing a service that is accessible by citizens or persons located within that country – are disproportionate in the online environment, where almost any service could be accessed from anywhere and create difficult conflicts of laws, not just for multinational corporations but for any Data controller that wishes to leverage the advantages of modern technologies involving cross-border Data transfers, such as cloud computing. Similarly, obligations to host Data domestically and restrict Data transfer beyond Indian borders hamper innovation and growth, for both budding domestic industry as well as companies with global operations. In short, both extraterritoriality of Privacy rules and Data localization should be avoided, because they create challenges for compliance and enforcement, work against efforts to establish global norms of Privacy protection, and hamper opportunities for innovation in India.

Data flows and privacy are not zero-sum. An effective Privacy and Data protection regime will protect legitimate cross-border data flows while ensuring a high standard of Privacy and Data protection for personal Data, regardless of where it travels. Indian policymakers should forgo Data localization measures and should seek to establish a sensible territorial scope applying only to organizations established in or targeting Data subjects residing in the 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. 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 take inspiration from these approaches.

As the Indian government considers policies related to Data, urge that any regulations that impact cross-border Data flows take into account the following principles:

- The movement of Data across borders is imperative for today's global economy;

- Data localization requirements disrupt the free flow of Data;
- Data localization requirements are incompatible with the Internet's distributed infrastructure that enables optimal system architecture;
- The security of Data does not hinge on the national boundaries of where such data resides; and
- Data localization requirements create barriers to market access, particularly impacting small- and medium-sized enterprises, which are eager to attract customers not only domestically, but also in foreign markets;
- Any exceptions to these provisions, such as to protect personal data privacy, should be limited to legitimate public policy objectives and be in full compliance with the provisions of the General Agreement on Trade in Services.

[i] EU General Data Protection Regulation (GDPR) - https://gdpr-info.eu/art-4-gdpr/

[ii] CAP 486 PERSONAL Data (PRIVACY) ORDINANCE Section 2 Interpretation - http://www.hklii.org/eng/hk/legis/ord/486/s2.html

[iii] Singapore Personal Data Protection Act 2012 - http://statutes.agc.gov.sg/aol/search/display/view.w3p;page=0;query=DocId%3Aea8b8b45-51b8-48cf-83bf-81d01478e50b%20Depth%3A0%20Status%3Ainforce;rec=0#pr2-he-

[iv] Canada Personal Information Protection and Electronic Documents Act - http://laws-lois.justice.gc.ca/eng/acts/P-8.6/page-1.html#h-3

[v] South Africa Protection of Personal Information Act (POPI Act) - http://www.banking.org.za/what-we-do/market-conduct/regulatory-framework/popia

[vi] EU Article 29 of Working Party - http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

[vii] EU GDPR Article 20 "Right to Data portability" - https://www.Privacy-regulation.eu/en/20.htm

[viii] Audit log' and 'audit trail' are defined in the Australian Signals Directorate Information Security Manual, https://www.asd.gov.au/publications/Information_Security_Manual_2016_Controls.pdf

[ix] Data Protection Law anD the ethicaL Use of anaLytics -https://iapp.org/media/pdf/knowledge_center/Ethical_Underpinnings_of_Analytics.pdf

[x] Anonymisation - https://ico.org.uk/for-organisations/guide-to-Data-protection/anonymisation/

[xi] A Global Reality: Governmental Access to Data in the Cloud, A Hogan Lovells White Paper http://www.cil.cnrs.fr/CIL/IMG/pdf/Hogan_Lovells_White_Paper_Government_Access_to_Cloud_Data_Paper_1_.pdf

Data Responsibility @IBM

IBM believes organizations that collect, store, manage or process data have an obligation to handle it responsibly. That belief—embodied in our century-long commitment to trust and responsibility in all relationships—is why the world's largest enterprises trust IBM as a steward of their most valuable data. We take that trust seriously and earn it every day by following these responsible principles and practices:

1. Data Ownership and Privacy

OWNERSHIP: We believe that our clients' data is their own, and that government data policies should be fair and equitable and prioritize openness. Our client agreements are transparent; clients are not required to relinquish rights to their data—nor the insights derived from that data—to benefit from IBM's solutions and services.

PRIVACY: IBM is fully committed to protecting the privacy of our clients' data. While there is no single approach to privacy, IBM complies with the data privacy laws in all countries and territories in which we operate; we support global cooperation to strengthen privacy protections.

2. Data Flows and Access

FLOWS: We believe clients, not governments, should determine where their data is stored and how it is processed. IBM therefore supports digital trade agreements that enable and facilitate the cross-border flow of data and that limit data localization requirements.

ACCESS: IBM has not provided client data to any government agency under any surveillance program involving bulk collection of content or metadata. We do not provide access to client data stored outside the lawful jurisdiction of any government requesting such data, unless the request is made through internationally recognized legal channels such as mutual legal assistance treaties (MLATs). If we receive a request for enterprise client data that does not follow such processes, we will take appropriate steps to challenge the request through judicial action or other means.

more>

3. Data Security and Trust

ENCRYPTION: IBM opposes any effort to weaken or limit the effectiveness of commercial encryption technologies that are essential to modern business. IBM does not put 'backdoors' in its products for any government agency, nor do we provide source code or encryption keys to any government agency for the purpose of accessing client data. We support the use of internationally accepted encryption standards and algorithms, rather than those mandated by individual governments.

CYBERSECURITY: IBM believes in public-private partnerships and voluntary, real-time sharing of actionable cyber threat information between government, business and academia to collaboratively prevent and mitigate cyber attacks.

4. AI and Data

We firmly believe that artificial intelligence cannot and will not replace human decision-making, judgment, intuition or ethical choices. Companies must be able to explain what went into their algorithm's recommendations. If they can't, then their systems shouldn't be on the market. IBM therefore supports transparency and data governance policies that will ensure people understand how an AI system came to a given conclusion or recommendation. As society debates the implications of AI systems, IBM opposes efforts to tax automation or penalize innovation.

5. Data Skills and New Collar Jobs

IBM is leading efforts to ensure workers worldwide are prepared for data-driven changes that are reshaping how work gets done, and that are driving productivity, economic growth and job creation. We are working with policymakers to modernize education systems to emphasize in-demand skills rather than specific academic degrees, preparing more workers for new collar jobs.