EBG FEDERATION

EBG Federation response to TRAI CP On Privacy, Security & Ownership of Data in the Telecom Sector

EBG Federation (EBG) was established on 11th March, 2015 as a Section 8 company under the Companies Act 2013 in order to ensure long term stability and clarity on its purpose as a not for profit organization offering support and advocacy for European businesses in India. Founded as the European Business Group (EBG), in 1997, as a joint initiative of the European Commission and the European Business Community in India, EBG has come to be recognized by the Indian Government and the European Commission as the industry advocacy group representing the interest of European companies in India.

EBG Federation is supported by the Delegation of the European Union to India and represents the 27 Member States of the European Union, UK as well as accession countries and its partners in European Economic Area (EEA). The EU Ambassador is our Patron. Currently EBGF has Chapters in Delhi, Mumbai, Bangalore and Chennai with approximately 170 companies as Members including a number of companies from the Telecom Sector. Mr. TV Ramachandran is currently the Chairman of the Telecom Sector Committee of the EBGF.

The primary objective of EBGF is to actively support growth in India-EU trade relations, become the most relevant advocate for European business in India and ensure that the needs of European business are well presented to policy and decision makers.

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?

EBG Answer

EBG Federation lauds the Regulator's commendable efforts for inclusive regulation and referencing best practices of nations that have gone through the process like USA and EU Countries.

EBG submits that understanding and expectations of privacy differ across societies and therefore while global developments and best practices must be considered, India should define a data protection regime which is contextually relevant and meets the country's requirements & priorities - job creation, economic development, entrepreneurship, etc

While internet is gathering momentum in India and by sheer number of users, rather than the percentage of users, India is becoming an important market for online services. There needs to be as light a regulation as possible on privacy issues in India, to allow free and rapid growth of services.

Care should be taken not to rush into introduction of new legal provisions without adequate justification, to avoid burdensome compliance requirements.

EBG Federation avers that Europe is a vastly different internet market with users long educated in the use of the net. India still has large parts of the population without access to the internet but to whom outreach is being actioned.

The EU's Cookie Law - the so called "cookie provision", which resulted in an overload of consent requests for internet users, will be streamlined/revised this year to make it simpler. New rules will allow users to be more in control of their settings, providing an easy way to accept or refuse the tracking of cookies and other identifiers in case of privacy risks. The proposal clarifies that no consent is needed for non-privacy intrusive cookies improving internet experience (e.g. to remember shopping cart history). Cookies set by a visited website counting the number of visitors to that website will no longer require consent.

According to Mary meeker of Kleiner Perkins Caufield & Byers - While the global Internet users growth rate remained flat at 10%, Internet user numbers in India grew more than 28% to 355 million users until mid-2016. Internet Penetration in India stands at 27%, suggesting there is room for significant growth ahead. there is still potential approximately 80% or more of users still in rural India who are yet to become Internet users. They need to be reached out properly and innovatively.

TSPs in India are bound by a number of requirements relating to the protection of user data. These requirements flow both from sector specific laws and conditions provisioned in the Indian Telegraph Act, 1885, as well as general provisions contained in the Information Technology Act, 2000 (IT Act). The Unified License agreement contains further requirements relating to the protection of user data, which include (a) An obligation on the licensee to "ensure the protection of privacy of communication and to ensure that unauthorized interception of message does not take place" (Clause 37). And (b) The licensee is only permitted to divulge or use such information insofar as it is necessary in the course of providing its services and information should only be sought to the extent necessary for the purpose of providing services to the concerned person.

Under Section 43A and Section 72A of the (Indian) Information Technology Act, 2000, privacy is adequately covered with imposition of criminal liability and further defined as mentioned in the Consultation Paper, through the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011(IT Rules) (**"SPDI Rules"**) enacted pursuant to Section 43A of the IT Act define "Personal information" to mean any information that relates to a natural person, which can be used, either directly or indirectly for identifying such person. "Sensitive personal

data or information" is defined to be a sub-category of this information, to include items such as passwords, financial information, health conditions, sexual orientation, etc.

Data protection requirements are currently applicable to all the players in the eco-system in India sufficient to protect the interests of telecom subscribers

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?

EBG Answer

India has a low internet penetration of 34% with even Bangladesh showing a 44% internet penetration. But if we look at it in real numbers India is second only to China globally for number of internet users. America, who is 3rd after China and India has an internet penetration of 88% with 286mill internet users. India has 462million users already.

Our 34% penetration implies that we still have a huge population to reach out to thereby further implying huge opportunities for online business.

The rapid growth of the internet worldwide has been fueled by revenues generated from online advertising. Online advertising, without which the internet would no longer be a free resource, is enabled by online identifiers and location data.

India has its own social and economic ecosystem which needs to be fostered. It may not be conducive to the growth of our ecosystem at this early stage to follow EU's GDPR treatment of personal data to include online identifiers, location data, and genetic information. These pieces of information are crucial to ad-based based free content on the Internet.

India's data protection framework is anchored by the principle of informed consent. Rules 4 and 5 of the Personal Data Rules mandate 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 also be given the names of people responsible for their personal data.

The Indian definition of personal data is in line with international norms and more than adequately protects user rights. In India, the definition of personal data ("personal information") is contained in rule 2(1)(h) of the Personal Data Rules1 (Information Technology Rules 2011 (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) as data which directly identifies a person or can be

connected with other data to indirectly identify a person. Moreover, SPDI Rules already provide for a consent-based model for handling personal data, including collecting, disclosing and transferring it. Users must be provided privacy policies explaining how their data will be used, and also names of people responsible for their personal data. Consent under contract laws of India has to be free, *ad idem* and without undue influence or misrepresentation.

Creating new capabilities for users, which is a primary goal of the technology industry, is welcome. The industry is constantly innovating to develop new products that offer convenience to users. If the government chooses to dictate a new capability, it must do so only after an economic analysis of the costs of intensive regulation.

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.

EBG Answer

The responsibilities of data controllers being identified in the SPDI Rules there is no conflict between Data Controllers and user.

The Responsibilities being:

- ✓ to give users notice of data practices
- ✓ to seek informed consent before collecting personal data
- ✓ not to collect more personal data than is required
- ✓ not to repurpose personal data
- ✓ not to store personal data after its collection purpose is accomplished
- ✓ to seek consent before disclosing personal data to third parties
- ✓ to make personal data available to the users to whom it pertains
- ✓ to handle data securely
- ✓ to be accountable to users for how their personal data is handled
- ✓ to handle sensitive personal data with special care.

Internet users voluntarily submit their personal data in return for the convenience of getting customised services; provision of which services is the revenue earner for the data controllers. It is a mutually win-win situation for both parties concerned.

However, while the Responsibilities of Data Controllers are provided through the Personal Data Rules for users rights, the rights of data controllers are per se are not identified anywhere. Future data protection law should expressly recognise that data controllers have certain rights over anonymised, purposively-designed datasets.

Furthermore, with reference to UK's Data Protection Act from the Information Commissioners Office (ICO) they have suggested a distinction between Data Controller's and Data Processor's as it was considered essential for organisations involved in the processing of personal data to be able to determine whether they are acting as a data controller or as a data processor in respect of the processing. This is particularly important in situations such as a data breach where it will be necessary to determine which organisation has data protection responsibility.

ICO definition of a "data controller" means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be processed and definition of "data processor", in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

Where personal data are processed only for purposes for which they are required by or under any enactment to be processed, the person on whom the obligation to process the data is imposed by or under that enactment is for the purposes of this Act the data controller.

This means that where an organisation is required by law to process personal data, it must retain data controller responsibility for the processing. It cannot negate its responsibility by 'handing over' responsibility for the processing to another data controller or data processor. Although it could use either type of organisation to carry out certain aspects of the processing for it, overall responsibility remains with the organisation with the statutory responsibility to carry out the processing.

For the rights and responsibilities of a data controller to be apportioned, the legislative framework should clearly define a data controller/data processor.

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?

EBG Answer

Section 43A of the IT Act provides that anybody corporate that possesses, deals or handles any "sensitive personal data" or information in a computer resource is required to maintain reasonable security practices and procedures relating to such data.

Proactive government monitoring, given the nature, scale and volume of transactions happening on the Internet every second and multiple players involved in each transaction, may not be practically possible. Market forces are sufficient to drive this change and there are positive developments to show this evolution. The regulation itself must allow for positive and beneficial uses of data this may not be efficiently achieved by creating a technology-enabled architecture to audit the use of personal data and consent.

Incentivising self-regulation and accountability measures for practices related to privacy protective measures may be a more effective in the long run.

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?

EBG Answer

TSP's/ISP's, as observed in the Consultation Paper and mentioned in Answer 2, are subject to ITA1885 and IT Act 2000 ruling as well as Unified Licence conditions.

Meanwhile, internet based services at best should not be burdened with a regulated environment as it has developed to where it is globally in total freedom. There may be guidelines and ex-post laws to penalize wrong doings. These are very much in place through the current IT Act.

A strongly competitive market is in the best interest of the consumer. In the present context, data analytics, behavioural analysis, aggregation and anonymization are the best techniques for improving services and user experience.

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?

EBG Answer

Mandating or Regulating the introduction of a Common pool "sandbox" may be detrimental to big business where Data is an important asset which is utilized by businesses to create useful products.

As far as TSP's are concerned, sharing of their data may not benefit them or the user. Rather, they need to build more secure repositories for their data to ensure crucial Sensitive Personal Data is kept well protected.

There is also the question of ownership rights of the data held by an organisation since the right to property is a constitutional right under Article 300A of the Constitution, which prohibits the state from depriving someone of their private property except through statutory law.

Businesses should be able to use public data sets and share data responsibly, but mandating that businesses share data is not justified and in fact per se does little to nothing in favor of innovation.

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?

EBG Answer

The internet has developed globally since its start with no little or no regulations. Free-trade and competition have driven business on the net. Global players have competed with local players improving quality of service and introducing new business techniques. Over-all, these internet businesses have had to build their brands and credibility in digital space, which is perhaps a harder task than what older businesses had to achieve. For businesses to succeed online, security of the companies processes and primarily the customer has become paramount. In the last few years, online selling is including even the smallest retailers. The size of the market in itself is an indication of consumer trust in online transactions.

Introduction of a technology solution for monitoring the ecosystem, may create geo-fences for cross-border businesses. As mentioned above, business techniques are being

introduced cross-border. Unless innovative techniques can be excluded from non-compliance, such methods may greatly hamper growth of internet business.

Industry is best placed to comply with the privacy principles under a self-regulatory framework and putting users in control is critical.

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?

EBG Answer

The terms of the license agreement for ISPs permit use of encryption technologies only up to 40 bits with RSA algorithms or its equivalent without any prior approval from the DoT. While Indian ISPs are bound to 40-bit encryption keys, the rest of the internet is significantly more secure, with third-parties such as email service providers or OTT providers not prevented from using longer encryption keys.

In an era where the Government is pushing for Digital Payments through various online processes, The TRAI may look at allowing higher encryption norms to protect consumer transactions. It will give a huge fillip to online businesses as more consumers will opt for digital services knowing their connections are well-encrypted. Encryption can help align businesses with users who are increasingly conscientious about their security and privacy.

Encryption regulations should be harmonised to unanimously promote the use of strong encryption and the government should issue rules under the IT Act to compel the use of strong encryption.

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?

EBG Answer

Please note in Answer 3 we have raised the subject of distinction of Data Controllers and Data Processors as raised by UK's Data Protection Act from the Information Commissioners Office (ICO) who have suggested that it is considered essential for organisations involved in the processing of personal data to be able to determine whether they are acting as a data controller or as a data processor in respect of the processing. This is particularly important in situations such as a data breach where it will be necessary to determine which organisation has data protection responsibility.

EBG FEDERATION

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?

EBG Answer

Voice-based and messaging services for both TSP's and OTTs will both be delivered on data platforms as is currently experienced with the new player in India.

Communication service providers (OTTs) are subject to the SPDI Rules just as other TSPs. Therefore, from a data protection perspective, there already is parity between OTT providers and other TSPs.

Having a technology/platform neutral data protection law which applies horizontally across the ecosystem should be the path forward. The Ministry of IT is already working to draft a comprehensive data protection law that would cover all the sectors and bring uniformity. The Supreme Court has recognized this Committee's role in its recent ruling on privacy being a fundamental right.

Once the data protection law is enacted, TRAI should review the existing provisions in the Indian Telegraph Act and licensing conditions to recommend changes to the Department of Telecommunications (DoT) to align with the new requirements. DoT/TRAI could also issue advisory or guidelines for the telcos to comply with these new requirements.

Data protection, security and privacy norms should be treated equally on par for all stakeholders of the Digital ecosystem viz. content & application service providers, device manufacturers, browsers, Operating Systems, etc. Due to emergence of new applications like M2M, IoT, etc apprehensions are being cast regarding nature & extent of data being collected and stored over the Internet cloud, the purpose for which it can be used and security of these devices and the underlying networks including the storage locations etc. Though some of these issues are perhaps covered under the provisions of the IT Act, however a larger and more comprehensive privacy & data protection law is perhaps required. Such a move would need to specifically address issues of identifying categories of data that are sought to be protected, stakeholders that would be bound by requirements of data protection and obligations to be cast on them & mechanisms for enforcement of such obligations.

2nd Floor, Building No. 6, Okhla Industrial Estate, Phase 4, Okhla, New Delhi 110 020, INDIA
Ph.: 9811418874 E-mail : gm@ebgindia.com
Website: www.ebgindia.com

EBG FEDERATION

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?

EBG Answer

Encryption is a critical tool that the government has to promote national security and public safety with a competitive market edge.

Anonymized and de-identified data: Given that lot of economic value of data today is generated through processing of anonymized and de-identified data, the data protection law under consideration should incentivize the processing of such data over personal data where appropriate. While anonymized data should be kept out of scope of the law, for de-identified data, at a minimum, there should be reasonable exemptions.

Data processors: The data protection law should make distinction between a data controller (organization which determines means and purpose of data collection) and data processor (organization processing data on behalf of the data controller) roles. This is an important consideration given that legal liabilities and obligations would differ based on the role an organization is playing. The data controllers should primarily be responsible for complying with the law. If anything, data processors should be responsible to take the necessary technical and organizational measures to secure the data they process on behalf of the controller. The 'controller-processor' relationships are governed through contractual means and the law should not unreasonably intervene in these relationships. The rules issued under Section 43A of the Information Technology Act did not make a distinction between controller and processor and this led to lot of confusion and backlash. To address industry concerns, the government later issued a clarification which helped create the desired distinction and exempted processors from certain requirements. The new law should avoid such a situation.

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?

EBG Answer

India is looking at growth of the economy through growth in the digital ecosystem. Startups and Innovators will not prosper with the burden of cumbersome regulations.

cross-border flow of information is vital for the globalised data ecosystem.

Any disruption/hindrances to cross border data flows, introduced in the privacy law, would adversely impact innovation, economic competitiveness and availability of technology and services to users.

Cloud Computing, for instance, is affordable for small businesses and startups because it relies on massive economies of scale with globally distributed datacenters. A 2014 ECIPE study had estimated that 'if India were to introduce an economy-wide data localisation measure, the effect on GDP would be -0.8%. In addition, the domestic and foreign direct investments (FDI) that drive Indian exports and long-term growth, would drop by -1.9%. In terms of welfare loss, data localisation would cost the Indian worker almost 11 percent of one average month's salary.'

● Indian IT Industry and Cross border data flows Particularly for India, getting cross border data flows right is critical for growth of its Information Technology (IT)/outsourcing sector - India is the world's largest sourcing destination for the IT industry, accounting for approximately 67 per cent of the US$ 124-130 billion market. The industry employs about 10 million workforce. To increase market access for Indian IT companies in EU, the Indian government as part of the India-EU Free Trade Agreement (FTA) negotiations has demanded that the EU relaxes the restrictions on movement of data of European citizens to. Finally, India's flourishing global Information Technology Industry cannot be placed at a competitive disadvantage with others in the APAC region. A data transfer framework that prohibits data transfers except for very limited circumstances is bound to harm the domestic IT industry, who will not have the same level of choice of certain services due to those restrictions to foreign providers. In fact, India has the opportunity to look at international data transfers with fresh eyes, not restricted by very limiting legacy approaches that have proven to be insufficient to address the current demands and nature of the 21st century globalized economy and society.