CONSUMER PROTECTION ASSOCIATION
HIMMATNAGAR
DIST. : SABARKANTHA
GUJARAT

Comments on CONSULTATION PAPER on Privacy, Security and Ownership of the Data in the Telecom Sector

Introduction :

Questions of size, power, competition and choice have never been so important to our understanding of consumer protection and empowerment in the digital world. Consumers are feeling the direct impact that such large players have on their individual choices: from privacy tools disappearing from app stores, or WhatsApp users seeing the service bought out by Face book, followed by changes to the terms of data sharing , to the impenetrable terms and conditions which people must agree to in order to access digital services. These digital services that quickly link up friends, music, events and travel are convenient and can be great fun but can also feel a bit like a lobster pot - ***easy to get into but very tricky to get out of.***

Many multinational platforms and digital companies have become indispensable to contemporary life, offering high quality, convenient digital interactions. The data monetization model behind some, where people 'exchange' information about themselves for the ***service with no upfront financial cost, makes for a tantalizing offer. They are the default by which consumers experience and interact with digital - the gateway to the internet if you like: we don't search, we Google, we don't make video calls, we Skype.***

The dominance of a small number of firms is significant because people's choice over whether to engage or not in the digital world is becoming increasingly limited.

In the European Union, the prospects of keeping markets competitive and consumers protected are closely tied. It is suggested that competition itself can offer a protection of sorts by creating markets where companies compete for customers on the basis of value, quality and strong consumer credentials. In reality, without a range of options, and without an easy way to move between these options, it is difficult for consumers to sever ties if they are unsatisfied with a particular service. As a result, it becomes very hard to gauge whether people are happy or unhappy with services and the way companies operate. Classic ideas of competition and consumer protection are therefore stretched.

Looking ahead to the next phase of digital consumption; the internet of things, heavy reliance on a small number of large companies could become even more important. As well as raising

privacy and security issues, the internet of things marks a major change in how we think about consumption, purchase and ownership. This is mostly because of ***so-called 'hybrid' products, where physical products are owned by the customer, yet the presence of software means the device is subject to contract terms and conditions, which could put unexpected limitations on its use or make exiting a contract difficult.***

Large established players already marking out territory in the internet of things will have to gather and connect data to as many objects and people as possible to make their connected services thrive. The more data points connected, the more potentially valuable the insights, so drawing in and retaining as many customers as possible will be top of companies' agenda. Exercising choice could get harder for consumers, as they lean towards contracting with one company as an easy way of bringing together multiple services. In practice, switching provider by exiting contracts will be time consuming or inconvenient. Add to this the difficulties in transferring data between suppliers and lock in seems more and more inevitable.

These limitations on choosing between providers are really important for the digital age. If competition can no longer effectively deliver consumer protection through providing choice, then we need to approach things differently. In fact there is the real opportunity to forge a positive consumer agenda for the digital age that addresses areas of consumer concern and offers real choice over how to participate. A complex, integral and dominating set of relationships

should not put us off arguing for a fairer and more accountable digital system for consumers.

For example:

- *Data portability and system interoperability – to enable easy transfer between different services, keep different options open, and keep the value of data close to consumer control*
- *Smarter use of information, and more transparency on how decisions based on data are made, not just what data is collected.*
- *Innovations that aid consumer understanding and build consumer trust and confidence such as personal data intermediaries.*

Awareness is needed to save privacy :

In India, along with digitalization, there is a need to create strong laws for protection and privacy at the advanced level of data. At the same time, people should make adequate literally literate so that people can take full advantage of digitization facilities with full awareness.

Jurisdiction :

TRAI has issued several regulations touch on the subject of Privacy since from 2007. In unsolicited commercial communications regulations : The regulations require the TSPs to maintain confidentiality of all information submitted by the subscribers.

In India, the Information Technology Act clearly states that every business must have a privacy policy published on its website, whether or not you deal with sensitive personal data. The privacy policy needs to describe what data you collect, the purpose of the data, any third parties it might be disclosed to, and what security practices you use to protect the data. Certain sensitive data, including passwords or financial information, can't be collected or processed without the prior consent of the user.

ISPs are exchanges of data, and the security of data in transit should be looked at by the TRAI.

Issues for 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?

Comments :

No.

Key principles of data protection like :

1. *Notice*
2. *Choice and consent*
3. *Collection limit*

4. *Purpose limitation*
5. *Access and correction*
6. *Discloser of Information*
7. *Security*
8. *Openness*
9. *Accountability* *etc.*

are not followed.

India's constitution provides protection for citizens' privacy rights. Also, Section 427 of Indian Telegraph Rules, 1951, inter alia provides that telephone should not be used to disturb or irritate any persons or to transmit any message for communication which may annoy a person. In 1997, the Supreme Court of India directed the Reserve Bank of India ("RBI") to institute measures to reduce unsolicited calls on the ground that the right to privacy is a fundamental right guaranteed under Articles 19 and 21 of the Constitution of India. (People's Union for Civil Liberties (PUCL) v. Union of India and Anr., AIR 1997 1 SCC 301.)

Other reasons :

1. *The transfer of personal information is a risk because of the open architecture of the Internet. According to MetaIntell, today more than 92% of such Internet/OTT apps use non-secure communication protocols.*
2. *Geo-location details, authentication, personal information, banking information etc. and data analytics can lead to a user's*

private information being harnessed for commercial gains, e.g. advertisement targeted to a user. This compromises the user's free will.

3. *User information is being extracted for carrying out marketing activities. "It is said that Big Data can even predict an individual's future actions'. Several concerns are being raised and most important is privacy of an individual.*
4. *Most of the time users believe that apps downloaded from an official app site can be trusted even though these stores do not guarantee trustworthiness of the products or items on sale or offer. These apps are hosted in such app markets without any risk assessment and can impact the device and a Service provider's internal network.*
5. *Internet apps bring "all manners of nuisance" including viruses, worms, malware, spyware or trojan horses etc. Hacking and theft are common occurrences. Recently even unreleased films from Sony were leaked by hackers.*
6. *Contact List : Data are sold to the Tele callers or Telemarketing companies. It may be used for black marketing.*
7. *Location : To track daily activities. Which is highly dangerous. Criminals can use it for kidnapping.*
8. *The 'always online' state of mobile phones exposes users to cybercrime. Most applications can trace the user's location for underlying processes (such as GPS apps finding the nearest restaurants etc). This information may be used to commit a crime, or the location itself may be the target of a crime. Such*

threats can impact the personal security, nation's security and financial health.

9. *Message : Messaging Apps can lick the data of users, which can be misused.*
10. *Photos : Can be misused for blackmailing.*
11. *According to the Antivirus company Simentek more than 36% of apps are having some kind of virus.*

Data Protection Policies in other countries :

1. ***Brazil*** *passed the Brazilian Internet Act in 2014 which deals with policies on the collection, maintenance, treatment and use of personal data on the Internet.*

   Any ***Brazilian*** *individual and legal entity must obtain someone's prior consent before collecting their personal data online, in any way. Consent can't be given by those under 16 years old, and from 16 to 18 years old they must have assistance from their legal guardian to give consent.*

   It also states that terms and conditions by service providers about how they collect, store, and use personal data need to be easily identifiable by the users, which means ***having a Transparent, accurate and easy to understand privacy policy.***

2. ***Canada's*** *Personal Information Protection and Electronic Data Act (PIPEDA) governs how service provider collect, store, and*

use information about users online in the course of commercial activity. ***According to the act, they must inform consumer about their privacy policies publicly available to customers.***

The privacy policy should be easy to find and to understand, and be as specific as possible about how they collect, handle, and use information.

3. *According to* ***Chile's*** *Act on the Protection of Personal Data, passed in 1998, personal data can only be collected when authorized by the user.* ***Service provider also need to inform users of any sharing of information with third parties.***

4. ***Colombia's*** *Regulatory Decree 1377 states that they must inform users of the purpose their data will be used for,* ***and they can't use the data for any other purpose without obtaining consent.***

Privacy policies must include a description of the purpose and methods for processing data, the users' rights over their data and the procedures for exercising those rights, and identification of who is responsible for handling the data.

5. ***Denmark*** *passed the Act on Processing of Personal Data in 2000. The Danish Data Protection Agency supervises and enforces the privacy laws.* ***If they discover violations of the***

law, they can issue a ban or enforcement notice, or even report the violation to the police.

According to the law, personal data can only be collected if the user gives explicit consent. ***Also, a company can't disclose personal information to third parties for the purpose of marketing without consent.***

6. ***The European Union Data Protection Directive of 1998*** *states that anyone processing personal data needs must do so in a* ***fair and lawful manner.*** *In order for the data collection to be considered* ***lawful, data can only be collected for specified, explicit and legitimate purposes, and users must give unambiguous and explicit consent after being informed that data collection and processing is taking place. They must also inform them if you're going to share their data with any third party.***

7. *The Data Protection Act (DPA) of 1978 (revised in 2004) is the main law protecting data privacy in* ***France****. The Postal and Electronics Communications Code also touches on the collection of personal data when it's used for sending electronic messages.*

The DPA applies to the collection of any information that can be used to identify a person, which is very broad in scope. The rules apply to anyone collecting data who is located in

France or who carries out its activities in an establishment in France ***(such as if your hosting server or other service provider related to collecting or processing data is located in France). This is why the French Data Protection Authority was able to fine Google for violating their privacy laws.***

Before automatically processing any kind of personal data, you must obtain the consent of the subject, and inform them of a number of things, including the purpose of the processing, the identity and address of the data controller, the time period the data will be kept, who can access the data, how the data is secured, etc.

8. *In* ***Germany****, the Federal Data Protection Act of 2001 states that any collection of any kind of personal data (****including computer IP addresses)*** *is prohibited unless you get the express consent of the subject.* ***You also have to get the data directly from the subject (it's illegal to buy email lists from third parties, for example).***

According to the act's Principle of Transparency section, the subject must be informed of the collection of the data and its purpose. Once the data is collected for a specific purpose, ***you can't use it for any other purpose without getting additional consent.***

These laws apply to any collection of data on German soil, and Federal Data Protection Agency and 16 separate state data protection agencies enforce them.

9. *In* ***Hong Kong****, If you're in violation of the Personal Data Ordinance, you could* ***face fines up to HK$50,000 and up to 2 years in prison, and you could be sued by your users as well.***

10. ***Italy's*** *Data Protection Code states has strict rules for any kind of electronic marketing. According to the code, you must obtain a user's consent before* ***tracking them or using data for advertising or marketing communications. You must provide the users with specific information before collecting or processing their data, including the purpose and methods for processing the data and their individual rights under the law.***

The Italian Data Protection Authority protects the rights of individuals regarding the privacy of their personal data. ***They can impose fines, such as the million-euro fine they threatened Google with for violating Italian privacy regulations.***

11. ***In United Kingdom*** *The Data Protection Act requires fair processing of personal data, which means that* ***you must be transparent about why you're collecting personal data and how you're going to use it. The law also states that***

if you use browser cookies, you need to clearly explain what they do and why you're using them, and gain the informed consent of your users.

Additional measures should be taken as early as possible to prevent consumer right on Privacy which are discussed in this consultation paper.

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?

Comments :

Definition of Personal Data :

'Personal data' means any 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.

Should the User's consent be taken before sharing his/her personal data for commercial purposes?

Yes.

Consumers should have meaningful control over how their personal information is shared with third parties.

Explicit Consent should be needed if the personal data collected is ordinary of non-sensitive or sensitive personal data.

Sensitive personal data :

Relates to specific categories of data which are defined as data relating to a person's racial origin; political opinions or religious or other beliefs; physical or mental health; sexual life; criminal convictions or the alleged commission of an offence; trade union membership.

Any Consent " Should be given by a clear affirmative act such as by a written statement, including by electronic means or an oral statement.

If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which should be :

1. *Clearly distinguishable from the other matters,*
2. *In an intelligible and easily accessible form,*
3. *Using clear and plain language.*

* *Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.*

* *The data subject should have the right to withdraw his or her consent at any time.*

* *The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.*

* *It shall be as easy to withdraw as to give consent.*

When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

In relation to the Child's consent :

The processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorized by the holder of parental responsibility over the child.

Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning

health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

What are the measures that should be considered in order to empower users to own and take control of his/her personal data?

Direct Representation by Consumer organizations :

Consumer Organizations should be empowered. *Consumers across the European Union have now the right to ask a competent NGO to complaint and bring claims against data processors on their behalf. TRAI should give " The right to take collective action " to registered organizations.*

Consumer can complaint to the Registered consumer organizations about the handling of their personal information by the service providers.

Important information about the complaints process:

- *They do not need a lawyer. However if they do decide to hire a lawyer, They must pay for the lawyer yourself.*
- *The registered organization investigates privacy complaints from individuals.*
- *The registered organization aims to resolve complaints as quickly as possible.*
- *Complaints are generally resolved through conciliation.*
- *Consumer can choose to withdraw their complaint at any time.*

What are the new capabilities that must be granted to consumers over the use of their Personal data?

The individual should have following rights under the directive :

1. *Pertaining to the enforcement of the Act, if the supervisory authority does not respond to the individual within one month on the progress of a complaint, the individual should have the right to judicial remedy.*
2. *The individual also should have the right to a judicial remedy if they consider that their rights have been infringed upon in non-compliance with these provisions.*
3. *The individual should have the right to receive compensation from the controller or the processor for the damage suffered.*
4. *The individual should have the right to request from the supervisory authority that the processing is lawful.*
5. *Remedies: The individual should have the right to a judicial remedy against a controller/processor, or supervisory authority, specifically the individual has the right to bring a court action for obliging the supervisory authority to act on a complaint.*
6. *Penalties: Penalties should be imposed on any natural or legal person, and should be implemented by the authority.*
7. *Compensation: Damage suffered by an individual should be compensated by the controller or processor.*
8. ***Complaints:*** *Any individual or body, organization, or association which aims to protect the rights and interests of data subjects in relation to the protection of their data may*

file independently or on behalf of a data subject and complaint with the supervisory authority.

9. *According to Argentina's laws concerning privacy, it's only legal to handle or process personal data if the subject has given prior informed consent.* ***Informed consent means you must tell them the purpose for gathering the data, consequences of refusing to provide the data or providing inaccurate information, and their right to access, correct, and delete the data. Also, any individual can request deletion of their data at any time.***

Consumer should have the following rights vis à vis data controllers:

- *Data controllers are required to inform when they collect personal data about the consumer;*
- *Consumer should have the right to know the name of the controller, what the processing is going to be used for, to whom their data may be transferred;*
- *Consumer should have the right to receive this information whether the data was obtained directly or indirectly, unless this information proves impossible or too difficult to obtain, or is legally protected;*
- *Consumers should be entitled to ask the data controller if he or she is processing personal data about you;*
- *Consumers should have the right to receive a copy of this data in intelligible form; free of cost.*

- *Consumer should have the right to ask for the deletion, blocking or erasing of the data.*

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.

Comments :

The Data Controller should be under the direct supervision of TRAI.

The Rights and Responsibilities of Data Controller :

Data controller must follow following Data protection principles :

1. *Personal information must be fairly and lawfully processed.*
2. *Personal information must be processed for limited purpose.*
3. *Personal information must be adequate, relevant and not excessive.*
4. *Personal information must be accurate and up to date.*
5. *Personal information must not kept for longer than is necessary.*
6. *Personal information must be processed in line with the data subject's rights.*
7. *Personal information must be secure.*
8. *Personal information must not be transferred to other countries without consent and adequate protection.*

The data controller determines the purposes for which and the manner in which any personal data are, or are to be processed,

The controller should have following responsibilities :

- *Registering with the TRAI before processing any personal data.* ***Failure to register should considered to be an offence.***
- *Issuing notification to the TRAI of possible breaches in processing of data.*
- *Appointing data protection supervisors.*
- *Putting in place adequate technical and organizational measures to safeguard personal data, which they are processing from destruction, adequate loss, unauthorized access or disclosure.*
- *The controller of the collected data also needs to create a description of the data file, including their name and address and the purpose for collecting the data. This description needs to be made available.*
- *Implementing appropriate technical and organizational measures to ensure that processing of personal data is in compliance with the provisions.*
- *Consulting with the supervisory authority before processing specific types and categories of data.*
- *Documenting all processing systems under their responsibility and providing all information to the supervisory authority so that it can perform its duties.*

Can the Rights of Data Controller supersede the Rights of an Individual over his/her Personal Data?

No.

Mentioned above.

Mechanism for regulating and governing the Data Controllers:

TRAI should regulate and govern the Data Controllers. The TRAI's role is to ensure that those who keep personal data comply with the provisions of the Act. TRAI should :

- *Monitor and ensure application of the directive*
- *Hear and investigate complaints lodged by data subject or based on own initiative*
- *Check the lawfulness of data processing*
- *Provide assistance to other supervisory authorities to ensure consistent application of provisions*
- *Monitor the development of information and communication technologies and how they impact the protection of personal data*
- *Consult with CAGs, institutions and bodies on legislative and administrative measures relating to the protection of individual's rights and freedoms*
- *Is consulted on processing operations*
- *Promotes awareness of privacy standards, etc*
- *Advises or request data subjects in exercising the rights laid down in provisions.*

They should have a wide range of enforcement powers to ensure that the principles of data protection are being implemented.

1. *The power should be include the serving of legal notices compelling data controller to provide information needed to assist his inquiries and compelling a data controller to implement one or more provisions of the acts in a particular prescribed manner.*
2. *They may investigate complaints made by the consumer or carry out investigations proactively.*
3. *They may authorize officers to enter premises and to in inspect the type of personal information kept, how it is processed and the security measures.*
4. *Data controller should require to co-operate fully with their staff with such officers.*
5. *If data controller found guilty of an offence under the act can be ordered to delete all or part of database, penalize and on conviction, Civil and criminal penalties (Imprisonment).*
6. *They should publish an annual report which names, in certain cases, those data controllers that were the subject of investigation or action by their Office.*

The in charge officer should be independent that has the ability to :

- *Serve information notices requiring organizations to provide specified information within a certain time period for the purpose of determining whether or not they are complying with data protection principles.*

- *Serve enforcement notices requiring organizations to take (or refrain from taking) specified steps in order to ensure they comply with the law.*
- *Serve assessment notices to public or specified organizations and bodies. An assessment notice requires that the data controller allows the officer to enter into specified premises, direct the controller to documents, provides assistance to copies of documents to the officer , allows the officer to inspect documents and equipments, etc., allows the officer to observe the processing of any personal data that takes place on the premises.*
- *Serve assessment notices to conduct compulsory audits to assess whether organizations processing of personal data follow good practice.*
- *If personal data is not being processed for the special purposes the officer may make a determination that will be issued to the data controller.*
- *Submitting proposals for the notification of regulations to the authority.*
- *Prepare a code of practice for the sharing of personal data.*
- *Assist in cases involving processing for special purposes.*
- *Inspect personal data recorded in specified international information systems.*
- *Serve monetary penalty notices to the data controller. Before the officer can serve the monetary penalty notice, he must first indicate his intent to do so to the organization. The officer is*

responsible for determining and publishing a guide as to when monetary penalties will be served.

- *Inspect and enter a premise if granted a warrant by a judiciary system.*

Data Transfer outside India :

The Data Protection Directive should applies to India Only. Special precautions need to be taken when personal data is transferred to countries outside the India. Without such precautions, the high standards of data protection established by the Data Protection Directive would quickly be undermined, given the ease with which data can be moved around in international networks. Personal data can only be transferred to countries outside the India when an adequate level of protection is guaranteed, adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights. Data transfers should not be made to countries that do not ensure adequate levels of protection.

Handling Complaints :

Data controllers must respond to any complaints received regarding misuse of data under their control.

If a data subject believes that his/her rights have been breached or that his/her data has been compromised, he/she has the right to request the data controller to remedy the situation. If the complainant does not receive an adequate answer from the data controller, he/she can file a complaint to the higher authority.

The data controller should cooperate with the supervisory body and the data subject by investigating complaints and redressing any legitimate grievances.

If the data concerned is found to be inaccurate or to have been unlawfully obtained, the data subject has the right to demand that it be corrected, blocked or erased and compensation.

Redressal :

Complaint redressal system must be developed.

The redressal mechanism should make provision for :

- *Securing the production of material used for the processing of personal data*
- *Inspecting, examining, operating, and testing equipment or material used in connection to the processing of personal data*

Compensation:

An individual should be entitled to compensation from a data controller for damages caused from non-compliance by the controller.

Offences:

A person who fails to comply with an enforcement notice, information notice, or special information notice should be held criminally liable for the offence.

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?

Comments :

Yes,

It is advisable to create a technology enabled architecture to audit the use of personal data, and associated consent with the capability adoption of advance technology in future.

An audit based mechanism will provide sufficient visibility for the government or its authorized authority to prevent harm under the regulatory control.

Industry can definitely create a sufficiently workforce of auditors who can take on these responsibilities.

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?

Comments :

India is fast catching up with the global trend as data center solution are concerned, certified according to the terms set up by ISO 27001, ISO – 9001 : 2008 and ISO 20000 – 1. Data centers store

and process outsourced data from different companies, allowing companies to focus on their core functions and objectives. Many of the data centres followed (ISO) standards and certifications as well as TIA/ANSI-942 and Tier certifications. For example, Reliance Communications operates nine data centers across India. Each data centre provides hosting, network, application, and consulting services to the customer, and offers space, power, cooling, and other needed facilities for companies to come and install and operate equipment. Reliance also offers companies the option of storing their data on the cloud, and offers central computing plus data storage and IT infrastructure hosting.

Nationally recognized e-commerce websites have shifted their data centers to India because of latency issues that were costing them a lot of paying customers.

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?

Comments :

Every country has a currency, and for a Smart Nation, Data is Cash, *acknowledging this data analytics is indispensable to the success of failure of our Smart Nation Initiative.*

* *This will be useful to start ups. If start ups worry less about stepping on regulatory toes, they can get off the ground and begin to focus on compliance later when they are more stable or have generated a revenue stream.*
* *Interested, qualified parties can come on board to solve new challenges.*
* *This will find new ways in which data can be resourced, which the government can then use to create smarter policies.*
* *The biggest challenges in a disruptive world is the technology usually crosses various domains. To combat this challenge, different regulators should work together.*
* ***It should comply with Legal and Regulatory requirements.***

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?

Comments :

Mentioned above.

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?

Comments :

A successful cyber attack on a telecommunications operator could disrupt service for thousands of phone customers, sever Internet service for millions of consumers, cripple businesses, and shut down government operations.

Today's cyber adversaries are constantly sharpening and evolving their capabilities to exploit new vulnerabilities. Addressing these threats will require that telecoms operators approach activities and investments with comprehensive, up-to-the-minute knowledge about information assets, ecosystem threats, and vulnerabilities.

- *To develop a plan for the protection of critical information infrastructure and its integration with business plan at the entity level and implementation of such plan. The plan should include establishing mechanism for secure information flow, guidelines and standards, crises management plan, proactive security posture assessment and forensically enables information infrastructure.*
- *To mandate implementation of global best security practices.*
- *To mandate secure application/software development process based on global best practices.*

- *To undertake and encourage Research and Development programs.*
- *To create and maintain testing infrastructure and facilities as per global standards and practices.*
- *To build trusted relationships with vendors and service providers for improving end-to-end supply chain security visibility.*
- *One in which security incidents are seen as a critical business risk that may not always be preventable, but can be managed to acceptable levels. We call this model Awareness to Action. To create awareness of the threats, vulnerabilities and consequences of breach of security among entities.*
- To foster education and training programs *for concerned entities including Consumer Advocacy groups.*
- *Collaboration with others : Sharing information with others to improve security and gain intelligence on current threats.*
- *Core practices like employee awareness and training , policies and tools to reduce insider risks, and protection of data- including intellectual property – will need to be updated.*
- *The confluence of mobility, cloud, and social networking have multiplied risks, one should address these threats and deploy technologies that monitor user and network activity to provide insight into ecosystem vulnerabilities and threats.*
- *Foreign Handset makers are having more than half of India's $ 10 Billion Smart Phone market, with most of these companies having services outside India. This will prevent any crippling*

cyber attacks that could be launched on the country's Telecomm and Power transmission sectors.

- *The foreign handset makers should setup servers in India to ensure protection of data, following concerns about security breaches, as smart phone vendors have servers in their home country.*

Government has taken such steps before, in 2008 told Black Berry to shift some server to India to address security concerns. The company eventually setup a server in Mumbai in 2012 to facilitate this.

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?

Comments :

The dangers of tracking headers :

Following issues with tracking headers:

- *Users cannot block tracking headers, because they are injected by carriers out of reach at the network level*
- *"Do not track" tools in web browsers do not block the tracking headers*
- *Tracking headers can attach to the user even when roaming*

across international borders

- *Even if tracking headers are not used by the carrier itself to sell advertising, other firms can independently identify and use the tracking headers for advertising purposes*
- *Certain tracking headers leak important private information about the user in clear text, including phone numbers*
- *Rich data profiles about users that tracking headers create make them prime targets for government legal requests or surveillance.*
- *Using tracking headers also raises concerns related to data retention. When "honey pots" of sensitive information, such as data on browsing, location, and phone numbers, are collected and stored, they attract malicious hacking and government surveillance. This kind of collection and retention of user data is unsustainable and unwise, and creates unmanageable risks for businesses and customers alike.*

It's important to note that tracking headers do not work when users visit websites that encrypt connections using websites with HTTPS.

- *The Data being collected from users after their consent through apps is disproportional to what is needed to enable such functions.*
- *Some entities are getting far more data, which is being used for commercial monetization purposes, which is wrong and needs to be solved.*

- *Some data is gathered without authorization and used outside the country.*
- *Indian Government has rules for Banking, Financial services and even Telecom where user data has to be stay in the country.*

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?

Comments :

Yes.

Mentioned above.

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?

Comments :

- *National security and defense;*
- *The prevention, investigation, detection and prosecution of criminal offences;*

- *The assessment or collection of taxes*
- *The protection of data subjects and the rights and freedom of others.*
- *Processing by an individual only for the purposes of that indiviual's personal, family or household affairs.*

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?

Comments :

Twenty-first century digital realities challenge traditional modes of international legal cooperation, revealing an institutional gap in Internet governance that may be solved by drawing lessons from the technical governance of the Internet. Preserving the global character of the Internet, fighting illicit online behavior, and establishing procedural interoperability and due process across borders demand innovative cooperation mechanisms that are as transnational as the Internet itself.

In order to properly address jurisdictional tensions such as cross-border access to user data, content takedowns, or domain seizures, we recommends the creation of issue-based multi stakeholder policy networks to develop scalable solutions.

1. *Unilateral actions to solve the complex jurisdictional conundrum on their own create a legal competition that makes the problem harder, rather than easier, to solve.* Economic and technological interdependencies have created a range of problems that exceed the scope of national sovereignty and can therefore no longer be sufficiently resolved by the unilateral action of national governments."
2. ***National actions upon operators with global reach have impacts on other jurisdictions.*** *Internet platforms or technical operators incorporated India can be impose our National laws and regulations on these private service providers, with direct trans boundary impacts on all foreign users of these services.*
3. *Draft legislations should include clauses establishing extraterritorial reach.*
4. *Litigation also plays a prominent role in setting new global standards, with impacts far beyond the respective jurisdictions. Face book, for instance, changed its global terms of service after a US court decision on its "sponsored stories" feature. Courts increasingly affirm competence regarding services incorporated in other countries merely because they are accessible in their territory, as illustrated by the recent Yahoo case in Belgium.*
5. *Local court decisions can also trigger new international norms for the interaction between states and Internet companies. For instance, the right to be de-indexed, initially established by*

Europe for Google, is now implemented by other search engines such as Microsoft Bing or Yahoo Search and has produced ripple effects in Asia and Latin America.

6. *The data of national citizens processed by foreign companies needs to be stored within the national jurisdiction like Russia.*
7. *Other digital sovereignty measures can range from strong national intermediary liability regimes, requirements to open local offices, demanding backdoors to encryption technologies, or the imposition of full-fledged licensing regimes.*
8. *Necessary data centres could be, established in the countries, which are stored in the reach of national authorities, while still allowing global processing and cross-border interactions.*
9. *Any national policy measure that would be detrimental if generalized around the world should not be adopted in the first place. International norms of cooperation are needed to prevent this legal arms race.*
10. *Based on the lessons of the Internet & Jurisdiction Project, some key factors for the success of such issue-based policy networks are:*
    - *Framing the problem as an issue of common concern for all service providers.*
    - *Ensuring the neutrality of the convener and facilitation team/ secretariat;*
    - *Involving all stakeholder groups: Internet platforms, technical operators, academia, Consumer Advocacy Groups, and international organizations .*

- *Engaging a critical mass with sufficient diversity to be representative of the various perspectives and to implement potential solutions;*
- *Constructing and expanding a global network of key actors;*
- *Creating trust among heterogeneous actors and adopting a shared vernacular;*
- *Combining smaller working groups and reporting on progress to make the process manageable and transparent;*
- *Informing stakeholders about relevant trends around the world to foster evidence-based policy innovation; and*
- *Providing sufficient geographic diversity from the onset to allow the scalability of adoption of any emerging policy solution. Addressing jurisdictional issues on the Internet and preempting the current legal arms race requires enhanced efforts to catalyze multi stakeholder cooperation on the specific topics of cross-border requests for domain seizures, content takedowns, and access to user data.*

Such innovative multi stakeholder networks can produce scalable and adaptive policy standards that guarantee procedural interoperability and transnational due process in relations between public and private actors.