Consultation No:09/2017

Telecom Regulatory Authority of India

CONSULTATION PAPER

on

Privacy, Security and Ownership of the Data in the Telecom Sector

New Delhi

09th August,2017

Telecom Regulatory Authority of India

Mahanagar Doorsanchar Bhawan,

Jawahar Lal Nehru Marg,

New Delhi-110002

www.trai.gov.in

Written comments on the consultation paper are invited from the stakeholders by 08 September 2017. Counter comments, if any, may be submitted by 22 September, 2017. Comments and counter comments will be posted on TRAI's website www.trai.gov.in. The comments/ counter-comments in electronic form may be sent by e-mail to arvind@trai.gov.in or bharatgupta.trai@gmail.com .For any clarification/ information, may be contacted at

Shri Arvind Kumar, Advisor (BB&PA)
Tel. No. +91-11-23220209; Fax: +91-11-23230056.

Contents

Chapter I

Introduction and Background

1.1 The rapid evolution of telecommunications services in India has aided the overall economic and social development of the country. It has enabled better connectivity among users, increasing use of information and communication technology (ICT) services and emergence of a variety of new business models. In parallel, we have also witnessed a quantum leap in the quantity and value of data that is being generated through the use of modern communication services. Each step of a user's interaction with ICT services, whether through traditional telecom services, Internet services, devices, applications or other forms of content, results in the generation of large amounts of data.

1.2 Reports indicate that 90 percent of the data in the world today has been created in the last two years alone with new data being added to this pool at the rate of approximately 2.5 quintillion bytes of data every day.[1] Data collection, storage and analytics have therefore become widely used tools that allow businesses to monetise their products and services and gain a competitive advantage over other providers. Data is collected by various businesses and agencies as a by-product of the user's interactions with them. This data is then retained by the business, and used to its advantage. At the same time, various Government agencies also benefit greatly from the generation of vast amount of data, which acts as an enabler for more efficient delivery of services and prevention and handling of crimes.

---

1 10 Key Marketing Trends for 2017 and Ideas for Exceeding Customer Expectations, IBM, https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=WRL12345USEN.

1.3 While recognizing the vast business and efficiency potential of data analytics it is also vital to assess whether the data protection rights of individuals are being adequately protected in this changing environment. Data protection in this context can be broadly understood to mean the ability of individuals to understand and control the manner in which information pertaining to them can be accessed and used by others. The focus therefore is on the issue of informational privacy, which forms a subset of the broader concept of 'privacy' that encompasses many other philosophical, psychological, sociological, economic and political perspectives.[2]

1.4 In the context of data protection, it is also important to establish the ownership of the data. For instance, if the data is recognized as belonging to the user to whom it pertains, then this data becomes available for use by them to better their own lives. This brings in the dimension of empowerment to the user.

1.5 The rationale for government intervention in this sphere arises on account of three key reasons to prevent harm to consumers. First, there is often an *information asymmetry* between the consumer and the data user on account of the under-estimation by consumers about the value of their personal data and ignorance about the scale and use of the data being collected and its use. The ability of data collectors to unilaterally change their privacy policies also contributes to this asymmetry. Second, is the problem of *bounded rationality*, which often leads consumers to underestimate the long term consequences of their actions while consenting to share their personal information in the course of availing specific products or services.[3] Third is the problem of a data monopoly. Since the service providers, through the provision of service generate

---

2 Roger Clarke, What's 'privacy'?, http://www.rogerclarke.com/DV/Privacy.html.

3 Vrinda Bhandari and Renuka Sane, Towards a privacy framework for India in the age of the internet, October, 2016, http://macrofinance.nipfp.org.in/PDF/BhandariSane2016_privacy.pdf.

and hold the data, it gives them an advantage, which they can use to get into adjacencies (and thus extending their monopoly). This results in harm to the market. The government or its authorized agency may take steps to make this data portable, under the control of the user, thus enabling the creation of newer services. The technical standards for this purpose may have to be defined in this case.

1.6 The government should enable the industry to grow by way of creation of newer services. There is a global trend in the creation of new services on the basis of data. These services provide significant value to customers, and businesses. The country may be at risk of falling behind, if action is not taken to encourage the creation of such businesses. This could be done through enabling newer players to bring in innovative services, while also ensuring a level playing field. There are two equally critical steps to do so. The first is Data Portability, that is, the ability to extract all user data from a service, and share it with another. The second is to create anonymized, public data sets, which can be used as a test bed by newer service providers.

1.7 In light of the above, the aim of this consultation paper (CP) is to identify the key issues pertaining to data protection in relation to the delivery of digital services. This includes the provision of telecom and Internet services by telecom and Internet service providers (TSPs) as well the other devices, networks and applications that connect with users through the services offered by TSPs and collect and control user data in that process.

Chapter II

Data Protection

2.1 Data Protection may be broadly defined as the legal control over access to and use of data stored in the digital format. It may also be considered as a process of safeguarding digital information from corruption and or loss.

Key principles of data protection

2.2 In October 2012, a Group of Experts headed by (Retd.) Justice A. P. Shah, Former Chief Justice, Delhi High Court submitted a report to the Planning Commission on the subject of data privacy.[4] The report contained a number of recommendations towards the formulation of a sector and technology-neutral privacy bill for the country keeping in view the international landscape of privacy laws, global data flows and predominant privacy concerns with rapid technological advancements. Their recommendations *inter-alia* included a proposal for the adoption of the following National Level Privacy Principles:

(a) **Notice**: A data controller, which refers to any organization that determines the purposes and means of processing the personal information of users, shall give simple to understand notice of its information practices to all individuals, in clear and concise language, before any personal information is collected from them. Such notices should include disclosures on what personal information is being collected; purpose for collection and its use; whether it will be disclosed to third parties; notification in case of data breach, etc.

---

4 Report of the Group of Experts on Privacy, October, 2012, http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf.

(b) **Choice and consent**: A data controller shall give individuals choices (opt-in/opt-out) with regard to providing their personal information, and take individual consent only after providing notice of its information practices.

(c) **Collection limitation**: A data controller shall only collect personal information from data subjects as is necessary for the purposes identified for such collection.

(d) **Purpose limitation**: Personal data collected and processed by data controllers should be adequate and relevant to the purposes for which they are processed.

(e) **Access and correction**: Individuals shall have access to personal information about them held by a data controller and be able to seek correction, amendments, or deletion of such information, where it is inaccurate.

(f) **Disclosure of Information**: A data controller shall only disclose personal information to third parties after providing notice and seeking informed consent from the individual for such disclosure.

(g) **Security**: A data controller shall secure personal information using reasonable security safeguards against loss, unauthorised access or use and destruction.

(h) **Openness**: A data controller shall take all necessary steps to implement practices, procedures, policies and systems in a manner proportional to the scale, scope, and sensitivity to the data they collect, in order to ensure compliance with the privacy principles, information regarding which shall be made in an intelligible form, using clear and plain language, available to all individuals.

(i) **Accountability**: The data controller shall be accountable for complying with measures which give effect to the privacy principles.

Such measures should include mechanisms to implement privacy policies, including training and education, audits, etc.

2.3 The principles referred to above could be regarded as a starting point for examining the soundness of the current framework governing the protection of user data across various stakeholders in the digital ecosystem. At the same time it is also important to consider the additional challenges that arise in the context of "big data", which is commonly characterized by features such as the high variety, velocity, volume of the data under consideration. For instance, it has been argued that the very nature of big data may require us to rethink the concepts of 'notice' and 'choice' or 'consent' that have thus far been regarded as the key tools of data protection. Similarly, increasing use of big data also gives rise to other key issues such as accessibility, accuracy, reliability of data and harmonization of standards, many of which may fall outside the purview of a discussion that is specific to data protection.[5]

Telecommunications and data protection

2.4 In the course of delivering their services, telecom and Internet service providers have the ability to gain access to a lot of information and data pertaining to their subscribers. This includes call detail records, calling patterns, location data, data usage information, etc. Though the above mentioned data is the personal data of the individual but the ownership rights, authority to use, transact and delete this data are presently ambiguous. In order to protect the privacy of users of telecom services it is important that ownership rights, authority to use, transact and delete personal data are ascertained, and to ensure that all the players in the chain are bound to follow certain safeguards while collecting, storing and

5 Kuner et al., The challenge of 'big data' for data protection, International Data Privacy Law (2012) 2 (2): 47-49, https://academic.oup.com/idpl/article/2/2/47/755343/The-challenge-of-big-data-for-data-protection.

using the data pertaining to their subscribers. Similarly, the role and responsibilities of data controllers should also be defined.

2.5 The 2012 report of the Group of Experts, referred to above, carried out a review of the manner in which the telecom regulatory framework, which includes the Indian Telegraph Act, 1885, the rules made under it and licensing terms and conditions, uphold the suggested privacy principles referred to above. The report noted that the existing framework contained some elements relating to the principles of accountability, collection and use limitation, security and third party disclosures while missing others such as notice, choice and consent and access and correction.[6] The following sections provide an overview of the current framework in this regard.

Telecom sector-specific requirements

2.6 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 as well as general provisions contained in the Information Technology Act, 2000 (IT Act).

(a) Indian Telegraph Act, 1885

The Indian Telegraph Act, 1885 (Telegraph Act) puts a general obligation on service providers to prevent unauthorized interception of messages and to maintain secrecy. In particular, the Telegraph Act contains the following provisions that are relevant in this regard:

- Restriction on any 'telegraph officer', which includes any person employed by a license holder, from altering, intercepting or divulging the contents of any message, except as required by law (S. 26).

6 Annex 2, Report of the Group of Experts on Privacy.

- It is also an offence to intrude into a telegraph office with the intention of unlawfully learning the contents of any message (S.24); damage or tamper with a telegraph to intercept its message or prevent its transmission (S.25); and fraudulently retain or detain a message (S. 30).

- Designated public officials have the right to intercept telephonic communications under identified circumstances, namely, situations of public emergencies or interests of public safety where such interception is required in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign states, public order or the prevention of incitement of offences.

- Further details regarding the process of interception have been laid down under the Indian Telegraph Rules, 1951. The rules *inter alia* require the service providers to put in place adequate and effective checks to ensure that unauthorized interception of message does not take place and utmost care is taken in the interception of messages as it affects the privacy of citizens.

(b) Requirements under the license agreement

The Unified License agreement contains further requirements relating to the protection of user data, which include:

- 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).

- 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. The

exceptions to these conditions apply when the party has consented in writing, or when the information is already open to the public.

- The license agreement also contains certain provisions relating to encryption of data. It restricts the licensee from employing bulk encryption equipment in its network and provides that use of encryption by the subscriber shall be governed by the Government policy/rules made under the IT Act, which authorises the Central Government to set encryption standards.

- Requirement to maintain suitable monitoring equipment as per the requirements of the licensor or designated security agencies (Clause 39.12). This includes the requirement to adopt necessary hardware and software for doing the lawful interception and monitoring from a centralized location. Further, the licensee is also required to maintain all commercial records/ Call Detail Record (CDR)/ Exchange Detail Record (EDR)/ IP Detail Record (IPDR) with regard to the communications exchanged on the network for at least one year.

- The license terms were amended in October, 2013 in line with the Government's decision to set up a Centralized Monitoring System (CMS) to facilitate lawful interceptions. Accordingly, the license agreement was modified to require licensees to provide connectivity upto the nearest point of presence of Multi Packet Label Switching network of the CMS at their own cost.[7]

(c) Initiatives taken by TRAI

In February, 2010, TRAI issued a directive to all TSPs requiring them to ensure compliance of the terms and conditions of the licence regarding confidentiality of information of subscribers and privacy of

7 Amendment to the Unified License Agreement regarding Central Monitoring System, 11 October, 2013, http://www.dot.gov.in/sites/default/files/DOC231013.pdf?download=1.

communications. This directive was issued in light of the concerns raised by consumers and consumer groups that service providers had not taken adequate steps to ensure such confidentiality and privacy. Accordingly, the Authority directed the service providers to put in place appropriate mechanisms to prevent the breach of confidentiality of information of subscribers and furnish the details of the steps taken in this regard to the Authority.[8] Unsolicited calls and bulk SMSs also pose a threat to consumer privacy by interfering with individual peace of mind and private life. These can also be used as a tool for phishing attacks. Accordingly, the National Customer Preference Register (NCPR) has been created in order to protect the privacy of telecom subscribers. The NCPR is a national database containing a list of the telephone numbers of all subscribers who have registered their preferences regarding receipt of commercial communications. As per TRAI guidelines, companies are prohibited from making unsolicited commercial communication with subscribers who have registered themselves in the NCPR.

(d) Information Technology Act, 2000

The IT Act also contains provisions relating to the protection of data and the interception of information by authorised agencies. These provisions are applicable to TSPs as well as to other intermediaries such as web-hosting service providers, search engines, online payment sites, online auction sites, online market places and cyber cafe.

- 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. It will be liable to pay compensation to the affected person in case of any

8 http://www.trai.gov.in/sites/default/files/Directions-26-Feb-10.pdf.

negligence in implementing such measures resulting in a wrongful loss or wrongful gain to any person.

- Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 (IT 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.

- Section 72A provides for the punishment for intentionally or knowingly disclosing personal information relating to a person that was acquired for providing services under a lawful contract, without the consent of the person concerned or in breach of a lawful contract. Therefore, Section 43A provides for compensation for failure to implement reasonable security measures while Section 72A imposes criminal liability on the person who discloses personal information without consent or in breach of a contract.

The IT Act also allows the Government to call for the interception, monitoring or decryption of any information on a computer resource. The grounds of interception under the IT Act are however different from those given under the Telegraph Act. The IT Act gives relatively wider scope for interception by removing the conditions of public emergency, public safety and public interest, and allowing interception "for the investigation of any offence".

Security of the telecommunications network

2.7 Preserving data confidentiality is a fundamental motivator for ensuring the security of telecom infrastructure.[9] However, the need for maintaining the security of telecommunications systems also stems, more broadly, from the role of this sector as one of the key pillars of critical national infrastructure. Vulnerabilities in the telecommunication infrastructure can lead to disruption of basic services with a severe impact on citizens, businesses and the delivery of public services. It is therefore essential to ensure that each layer of telecom infrastructure and the ecosystem as a whole is protected through adequate security measures in order to safeguard the system from any potential vulnerabilities. Accordingly, the requirement of network security framework in this sector can be attributed to the following sources:[10]

- Customers/subscribers need confidence in the network and the services offered, including availability of services (especially emergency services) in case of major catastrophes.

- Public authorities demand security by directives and legislation, in order to ensure availability of services, fair competition and privacy protection.

- Network operators and service providers themselves need security to safeguard their operation and business interests, and to meet their obligations to the customers and the public.

2.8 Section 70 of the IT Act provides for the declaration of certain areas as critical information infrastructure (CII) and the need for introducing appropriate measures for the security of these systems. CII refers to

---

9 ITU, Security in Telecommunications and Information Technology, 2003, http://www.itu.int/itudoc/itu-t/85097.pdf.

10 Id.

protected systems or functions whose incapacity or destruction would cause a debilitating impact on national security, governance, economy and social well being of the nation. Keeping in view the critical rule of the telecommunications sector, the National Critical Information Infrastructure Protection Centre (NCIIPC), the agency mandated to facilitate the protection of critical infrastructure, has designated this to be one of the CIIs.

Chapter III

Stakeholders: Digital Eco System

3.1 While the aforementioned conditions of privacy, confidentiality and security discussed in Chapter II remain extremely relevant to services provided by TSPs, it is well recognised that privacy concerns also emanate from the activities of a variety of other stakeholders that process and control the personal data of users. This includes stakeholders like content and application service providers, device manufacturers, browsers, operating systems, etc. The following are some of the ways in which data pertaining to users can be accessed or controlled by these different players.

(a) Cookies and fingerprinting: A cookie is a small file, typically consisting of letters and numbers, which allows a website to identify a user's device. Cookies can be of many types such as session cookies that expire after a particular browser session; persistent cookies that can be used for monitoring a user's actions over a continuing period; first party cookies that are set by the domain being visited by the user; and third party cookies that are set by a domain other than the one being visited by the user. Research has shown that in general users have a low level of awareness about the meaning and use of cookies and the beneficial and harmful objectives for which they can be deployed.[11] These objectives may include actions like saving the login details of the user for future support or closely tracking the browsing history of users, very often for advertising purposes.

---

11 Information Commissioner's Office, Guidance on the rules on use of cookies and similar technologies, May, 2012, https://ico.org.uk/media/for-organisations/documents/1545/cookies_guidance.pdf.

(b) Many other tracking techniques are also in use. For instance, "device fingerprinting" is a method that uses the various information elements transmitted by a device in order to identify it. Different software, platforms and APIs each offer access to different information elements stored in the device. The web browser JavaScript API, for example, can provide information relating to the screen size, colour depth and available system fonts. Other APIs may request access to information elements stored in the firmware (e.g. the CPU type), operating system (e.g. the OS type) or graphics card model. However, a number of information elements can be combined to provide a set which is sufficiently unique (especially when combined with other identifiers such as the originating IP address) to act as a unique fingerprint for the device or application instance. Such a fingerprint provides the ability to distinguish one device from another and can be used as a covert alternative for cookies to track Internet behaviour over time.[12]

(c) Permissions taken by applications: The digital ecosystem is full of a large number of software applications (apps) that designed for specific purposes like entertainment, email and communications, shopping, banking and payments, etc. Studies have indicated that the growth of app usage in India in the last year was four times that of the global growth (India - 43%, ; global – 11%).[13] While the increasing usage of these apps continues to offer many efficiencies and benefits to both users and developers, they also pose several concerns from a data protection perspective by allowing the app owner to collect vast amounts of data about the user. Besides app

12 Working Party under Article 29 of Directive 95/46/EC, Opinion 9/2014 on the application of Directive 2002/58/EC to device fingerprinting, 25 November 2014, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp224_en.pdf.

13 Manishree Bhattacharya, India - the lucrative App market, 24 March 2017, https://community.nasscom.in/community/discuss/product/blog/2017/03/24/india-the-lucrative-app-market.

owners and developers there are a number of other players in the app ecosystem, such as app stores, operating systems, device manufacturers, and other third parties like analytics and advertising providers who play a role in in the collection and processing of personal data through apps.[14]

(d) Apps may also collect information about other people (who are not their customers) through a consenting customer. For example, global directories of phone numbers crowd-sourced through customers. The person whose personal information is being shared may not be aware of this sharing.

(e) Notably, apps are able to collect large quantities data from a user's device and process the same for various business purposes. This includes collection of information which is necessary for providing the relevant service to the user (such as access to stored photographs for a photo editing app) as well as several other categories of information, such as the user's contact list, messages, camera, location, etc., which may not have any direct co-relation with the underlying service being offered by the app. The permissions granted by the user allowing access to these various categories of information is often given under circumstances where the user does not fully understand the implication of granting the consent. Moreover, the one-sided nature of these arrangements with an uneven bargaining power between the provider and the user implies that the user often does not have an effective choice in the matter -- the app may not available for use without authorising those permissions.

---

14 Working Party under Article 29 of Directive 95/46/EC, Opinion 02/2013 on apps on smart devices, Adopted on 27 February 2013, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf.

(f) The lack of adequate security mechanisms in some apps also poses a major concern. Malware attacks on vulnerable apps can expose the private information of their users, such as passwords, photographs, financial data etc, to third parties potentially causing severe losses to users.

(g) Platforms and operating systems: Operating systems such as Google's Android, Apple's iOS and Microsoft's Windows and the app stores run by them act as an intermediary between app providers and end users. This gives them the ability to set the rules of the game in terms of the permissions that may be sought by apps and providing disclosures and transparent to users regarding their privacy controls. Some measures that have been suggested in other jurisdictions in this regard include a requirement of providing just-in-time disclosure to customers before allowing an app to access sensitive content; dashboard facility to allow users to view all privacy permissions given by them; formulating best practices for app developers and considering the offering of a Do Not Track mechanism that would allow users to prevent tracking by ad networks or other third parties.[15]

(h) Further, the use of proprietary codes and systems also contributes to an increase in the vulnerabilities of certain types of systems. This calls for a need to consider appropriate mechanisms for the timely detection and reporting of any threats.

(i) Control by devices: The devices and equipment used by individuals to connect to various networks also have the ability to gather large volumes of data about the user's behaviour. Incidents have come to light where device manufacturers have distributed pre-installed

15 FTC Staff Report, Mobile Privacy Disclosures - Building Trust Through Transparency, February, 2013, https://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf.

software that allowed them to monitor the location, call and messaging activities of the device owners.[16] In other cases, the device manufacture may exercise strict control over the manner and extent to which third parties can gain access to user data on the device, even with the consent of the user, while utilising this information for its own purposes.

(j) The growth in the adoption of Internet of Things (IoT) devices also raises concerns about the nature and extent of data being collected by these devices, the purpose for which it can be used and the security of these devices.

3.2 The issues above may be covered to some extent by the provisions of the IT Act but we are yet to formulate a more comprehensive privacy and data protection law for the country. Any move in this direction will need to specifically address the issues of identifying the categories of data that are sought to be protected; the stakeholders that would be bound by the requirements of data protection and the obligations to be cast on them; and mechanisms for the proper enforcement of such obligations.

3.3 In this context it is relevant to note that traditionally the scope of data protection regulation world over has been limited to personal data. This is because personal data, or data attributable to a particular individual has the ability to generate various harms including identity theft, financial loss, loss to reputation and dignity, disturbance of mental peace, threat to physical safety and increasingly, discrimination. Accordingly, a standard distinction that is made in digital communications is that between content and metadata. This traditional distinction is getting blurred with the emergence of sophisticated tools that enable cookies, location and traffic tracking from multiple sources that may be aggregated over time for

16 Matt Apuzo and Michael S. Schmidt, Secret Back Door in Some U.S. Phones Sent Data to China, Analysts Say, 15 Novermber, 2016, https://www.nytimes.com/2016/11/16/us/politics/china-phones-software-security.html.

identifying specific users. Therefore, it might be important to broaden the scope of what can be considered personal data, keeping in mind changes in technology and methods of aggregation.

3.4 Since the use of data is growing, it is important that any regulations concerning the use of data be able to cope with the volume, and diversity of usage. It would be useful to build a technology framework, which can monitor the uses of data, and compliance with various regulations. This will enable the regulator to pro-actively monitor the system, as well as bring in advanced techniques for fraud detection, etc. The Digital Locker Authority has recently published a Electronic Consent Framework[17] which appears to be extensible, and suitable for this purpose.

3.5 The techniques used by the TRAI to regulate the flow of information, and protect consumers within its jurisdiction are also applicable to other uses of data, for instance, in the fields of health and finance.

3.6 The need for appropriate safety and security mechanisms to preserve the infrastructure and systems of various providers is another important element of a sound data protection framework. Besides exposing the personal information of individual users, data breaches also result in financial and reputational consequences for the organisation. It is reported that there were 4,149 breaches reported during 2016 exposing over 4.2 billion records. The types of data exposed through these incidents include email addresses (42.6 percent); passwords (38.1 percent); names and usernames (35.1 and 21.6 percent, respectively); and addresses (20.4 percent).[18] While recognising the severity of this problem we also need to consider the steps that may need to be taken by various stakeholders to improve the awareness and understanding of consumers regarding the

---

17 http://dla.gov.in/sites/default/files/pdf/DigitalLockerTechnologyFramework%20v1.1.pdf

18 Data Breach QuickView Report, January, 2017, https://pages.riskbasedsecurity.com/hubfs/Reports/2017%20Q1%20Data%20Breach%20Quick%20View%20Report.pdf.

use and protection of their data and the likely effectiveness of such measures.

3.7 Finally, issues of cross-border transfer of data and exercise of jurisdiction over service providers that do not have a direct presence in the country are becoming increasingly relevant in the context of digital data. Any effective solution on data protection would necessarily have to address these issue in the manner that balances the requirements of business innovation, efficiency and security.

Chapter IV

Data Protection Framework in other countries

4.1 In the European Union (EU) the Directive on Privacy and Electronic Communications, known as the ePrivacy Directive, sets out rules on how providers of electronic communication services, such as telecom companies and Internet Service Providers, should manage their subscribers' data.[19] It lays down directives relating to confidentiality of electronic communications and related traffic data; security obligations; confidentiality of terminal equipment; processing of traffic data and location data; and sending of unsolicited communications.

4.2 As noted above, the scope of the current e-Privacy directive is mostly limited to traditional electronic communication services but the European Commission has recently proposed a Regulation on Privacy and Electronic Communications to update current rules to adapt to technical developments and the new General Data Protection Regulation (GDPR) framework that had been adopted by the EU.[20] The new proposal seeks to ensure the confidentiality of electronic communications regardless of the technology used, i.e. the proposed rules will also apply to Internet-based voice and messaging services. Further, privacy is sought to be guaranteed for both the content of the communications as well as metadata (e.g. time of a call and location), which need to be anonymised or deleted if users do not give their consent.

4.3 In addition to the e-Privacy directive, communication service providers are also bound by the provisions of EU's Data Protection Directive (95/46/EC), which will be replaced by the GDPR with effect from May, 2018. The

---

19 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, OJ L 201, 31 July 2002, which was amended in 2009 and 2013.

20 European Commission, Press release, 10 January 2017, http://europa.eu/rapid/press-release_IP-17-16_en.htm.

GDPR covers the protection of personal data of individuals and applies to all sectors. The key requirements of the GDPR include requiring the consent of the data subject, providing data breach notifications, requirement of privacy by design, conditions applicable to the transfer of data across borders, etc. The GDPR however does not cover business-to-business communication or communication between individuals, which does not include personal data. The proposed e-privacy regulation in Europe will therefore complement the GDPR by giving citizens and companies specific rights and protections in the context of electronic communications.[21]

4.4 In the United States, there are a number of laws, regulations and guidelines relating to the protection of data, which are implemented by different agencies. The Federal Trade Commission implements the federal consumer protection law that prohibits unfair or deceptive practices and applies to both offline and online privacy and data security policies. In addition to this there a a number of specific requirements that are applicable to particular categories of information such as health data, financial data, credit information, etc.

4.5 In 2016, the Federal Communications Commission enacted broadband privacy rules that were aimed at securing greater choice, transparency and security protections for the personal information held by broadband providers. In particular it included requirements that Broadband ISPs would be required to obtain affirmative "opt-in" consent from consumers to use and share sensitive information. This would include precise geo-location, financial information, health information, children's information, social security numbers, web browsing history, app usage history and the content of communications; Broadband ISPs would be allowed to use and share non-sensitive information - for example, email address or service

21 European Commission - Fact Sheet, 10 January, 2017, http://europa.eu/rapid/press-release_MEMO-17-17_en.htm.

tier information - unless a customer "opts-out"; and Customer consent would be inferred for certain purposes specified in the statute, including the provision of broadband service or billing and collection.

4.6 Although the United States Senate has recently voted to repeal these rules, their content may instructive in terms of the choice and transparency based approach adopted in the context of communication services.

4.7 With this background, the following questions are being posed to stakeholders in order to obtain their views on the next steps towards a more comprehensive consultation on data protection in telecom sector and other areas of the digital ecosystem.

Chapter V

Issues for consultation

It may please be noted that answers/ comments to the issues given below should be supported with justification. The stakeholders may also comment on any other issues related to Data Privacy and Security in Telecom Sector along with all necessary details.

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?

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?

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.

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?

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?

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?

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?

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?

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?

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?

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?

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?