SIGFOX SINGAPORE PTE LTD

RESPONSE TO TELECOM REGULATORY AUTHORITY OF INDIA CONSULTATION PAPER –

PRIVACY, SECURITY AND OWNERSHIP OF THE DATA IN THE TELECOM SECTOR

1. INTRODUCTION

1.1. Sigfox Singapore Pte Ltd ("Sigfox") refers to the Telecom Regulatory Authority of India ("TRAI") public consultation paper dated 09 August 2017 on the Privacy, Security and Ownership of the Data in the Telecom Sector ("Consultation Paper").

1.2. Sigfox is a company providing a worldwide connectivity solution for Internet of Things ("IoT") applications based on billions of devices connected to the Internet while consuming as little energy as possible and driving the total cost of ownership to a minimum in order to unlock the full potential of mass IoT. In-order to reach those objectives, Sigfox has developed an innovative technology based on an Ultra Narrow Band ("UNB") system operating in the unlicensed sub 1-GHz spectrum and transmitting IoT data via Internet to the Sigfox's cloud. Sigfox global network is comprised of base stations, software defined cognitive network nodes which are IP-connected through DSL, 3G or satellite to a centralised backend.

1.3. Sigfox welcomes the opportunity to make this submission on the Consultation Paper by TRAI. Sigfox has taken this opportunity to provide its comments based on its experiences as regards to the technical and social-economic aspects of security and data protection.

1.4. This submission is structured as follows:

Section 1 – Introduction
Section 2 – Executive Summary
Section 3 – Sigfox's Views and Comments on Issues for consultation

1.5. Sigfox would be pleased to clarify any of the views and comments expressed by the company in this document, as appropriate.

1.6. Sigfox contact person: Mary Lim at mary.lim@sigfox.com.

2. EXECUTIVE SUMMARY

2.1. An IoT business application is an end-to-end solution where devices and sensors generate data, interact and communicate over a network, sending data to information processing systems where meaningful information is generated to take business decisions. It is therefore essential that the end-to-end chain can be trusted in the sense that devices are genuine and authorised to communicate on the network.

2.2. Sigfox has gathered a team with lengthy experience in security industry that deals with all relevant aspects, from security by design to active operational measures. This addresses data protection in motion via measures built into the protocol, data protection at rest via cryptographic storage of data and credentials in devices, base stations and Sigfox core network. In an effort to support its ecosystem, Sigfox has developed partnerships with Internationally recognised security experts to facilitate the introduction of hardware security in devices and provide security assessment schemes for the IoT.

2.3. With regard to the questions raised in Consultation Paper, Sigfox identifies three main recommendations to foster the development of IoT technologies and its socio-economic benefits in India:

2.3.1. Foster multi-stakeholder collaboration on issues such as security and privacy implications of IoT, whereby different actors in the IoT chain can help each other and support government agencies in charge of law enforcement and hence protect consumers, operators, service providers, and the economy in general;

2.3.2. Develop bottom-up policies, where security issues can be addressed close to where they occur, instead of centralising responsibility amongst a few. Regulations enabling different levels of security should be implemented considering both, risk-based approaches that take into account the criticality and type of application, as well as cost of implementation to allow for ease of innovation; and

2.3.3. Encourage globally interoperable secure standards, both technical and regulatory, that facilitate trans-border data flows while protecting privacy. Develop international cooperation in the field of data protection by adopting Internet standards developed by well-established Standards Development Organisations (“SDOs”), such as the Internet Engineering Task Force (“IETF”), and by contributing to multilateral agreements within the World Trade Organisation and the specialised agencies of the United Nations.

3. SIGFOX'S VIEWS AND COMMENTS ON ISSUES FOR CONSULTATION

Q1 Are the data protection requirements currently applicable to all the players in the ecosystem 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?

3.1. Sigfox believes that the current data protection requirements are sufficient. Sigfox is of the view that the data protection requirement on "the license agreement also contains certain provisions relating to encryption of data" may not be applicable to all IoT applications. The regulation should allow end-service providers and end-customers to have the option whether to implement encryption or not, depending on the criticality of the application.

Q2 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?

3.2. With the development of the IoT, more and more data will be exchanged between machines, objects and individuals in numerous sectors of activity. Sigfox is of the view that beyond technology innovation, universal definition of personal data in non-obvious context (e.g. identifiers, names, etc.) will more often depend on specific cases and therefore require a flexible approach where all stakeholders and consumers are empowered to negotiate the right level of data control and liability between each other.

In this context, Sigfox supports the development of strong technology neutral regulation to ensure a high level of compliance complemented by effective enforcement practices. These regulations should focus on desired privacy outcomes, rather than specifying technological means to direct privacy practices.

With this regard, when mechanisms such as systematic anonymization or privacy-by-design principles are implemented to guarantee the right level of data privacy and appropriate information are provided to end-users, it should be made possible to avoid user's consent before sharing the data for valuation purposes.

Q3 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.

3.3. Over-regulating can create problems. A balanced mutli-stakeholder framework that allows the development of the IoT ecosystem while ensuring individual's rights to protect and control his/her Personal Data should involve designers, manufacturers, network operators, service and application providers, regulators and end users. This framework should be adapted to their interventions on and their roles in the overall digital ecosystem.

3.4. Therefore, the core criteria to define the Rights and Responsibilities of the Data Controller should be its effective control on the Personal Data and the effectiveness of its relationship with end-users. A clear identification of the Data Controller as the provider having the effective control over the Personal Data of the end-users as Data Subjects would allow assessing what should be its Rights and Responsibilities.

3.5. Accordingly, the Responsibilities of the Data Controller should encompass the definition of the purpose(s) of the processing of the Personal Data and the information of the end user on such purposes whereas the Responsibilities of other stakeholders in the digital ecosystem only acting on the instructions of the Data Controller, and therefore having no control over the Personal Data and frequently no relationship with the Data Subject, should be limited to the security measures taking on the processing of the Personal Data for the Data Controller and where needed, to the anonymization of such Personal Data.

3.6. As for the Rights of the Data Controller, it may not generally supersede the Rights of the Data Subjects on their Personal Data, however the Data Controller shall remain in capacity to provide the best service to the Data Subjects and thus be recognized to some extent a legitimate interest to process the data (see suggestions to Q11).

3.7. Privacy and data laws should enable inclusive approaches and, where necessary, create collaborative bodies in-order to involve all stakeholders in the way data controllers are regulated. More specifically, these bodies could oversee the development of ethical practices while ensuring users are able to negotiate on an equal footing with data collectors.

Q4 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 authorised authority to prevent harm? Can the industry create a sufficiently capable workforce of auditors who can take on these responsibilities?

3.8. Sigfox encourages the development of global and harmonized privacy standards, both technical and regulatory. Initiatives towards a self-audit based mechanism run by the industry can support privacy-enhancing solutions while providing visibility to authorities and users and prevent harmful incidents.

Q5 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?

3.9. Sigfox believes that the encouragement of new data based businesses is fundamental to develop the international data market. Sigfox is of the view that an overall framework of data protection should differentiate Personal Data, as the data identifying individuals and requiring a specific protection for end-users, and other non-personal data that would help growing such data market by offering new data based services to users and end-users. More particularly considering the IoT ecosystem, as non-personal data is likely to be the sole kind of data processed, a more flexible approach of the data protection could help encouraging the creation of new data based businesses.

3.10. Subject to this flexibility, although there is no universal privacy or data protection law that applies across the Internet, a number of international and national privacy frameworks have largely converged to form a set of core, baseline privacy principles. For example, the principles derived from the Organisation for Economic Cooperation and Development ("OECD") 2013 privacy guidelines.

Q6 Should government or its authorised authority setup a data sandbox, which allows the regulated companies to create anonymised data sets which can be used for the development of newer services?

Sigfox believes that there could be several economic, societal and business benefits derived from the collection and use of anonymized data. A data sandbox framework should consider data sets that can be managed by one or several regulated companies, providing hence for a more open-innovation environment that fosters technical-development.

Q7 How can the government or its authorised 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?

3.11. The government could foster multi-stakeholder collaboration and provide a platform for discussion on issues such as security and privacy implications of IoT, whereby different actors in the value chain can help each other and assist the government to monitor the ecosystem compliance and hence protect consumers, operators, service providers, and the economy in general.

3.12. Considering the wide range of applications and new use-cases offered by internet ecosystem, Sigfox is of the view that centralised and mandatory monitoring solution should be avoided as much as possible. Appropriate monitoring should rely on strong compliance principles enforced by efficient ex-post control policies.

Q8 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?

3.13. Sigfox agrees with the Internet Society opinion on security requirements for the IoT in that a bottom-up approach is needed, where security issues can be addressed close to where they occur, instead of centralizing responsibility amongst a few. Sigfox also strongly believes that different levels of security should be implemented considering both, risk-based approaches that take into account the criticality and type of application, as well as cost of implementation to allow for ease of innovation.

Q9 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?

3.14. In the context of the IoT, high and undifferentiated security or data protection requirements for all applications can create negative effects for innovative use-cases based on the transmission of low sensitivity data.

3.15. The government should promote privacy-by-design and security-by-design principles throughout the development, implementation and deployment cycle.

Piracy-by-design principles should also be applied to the development of standards, applications, services, and business processes.

For example, the adoption of open Internet standards developed by well-established SDOs, such as the IETF and the suit of IoT-specific communication protocols, can enable interoperability and security of IoT applications and services.

3.16. Another key issue of data protection pertaining to the collection and use of data by various other stakeholders in the digital ecosystem is the need for the adaptation of the protection mechanisms to (i) the kind of data protected, i.e. Personal Data or non-personal data together with; (ii) the context of the processing, like the provision of a subscribed electronic communication service; and (iii) the effective control of the stakeholder on such data.

Q10 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?

Sigfox is of the opinion that level of data protection should depend on the applications, the technologies and the roles played by the different stakeholders involved in the value chain. Business models, Market definition, competition and regulatory framework still make relevant the distinction between TSPs and added value or Over-The-Top ("OTT") services providers as the nature of the services differ significantly, although some technical commonalities exist.

Q11 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?

3.17. Considering the pace of innovation and the increasing range of applications enabled by the Internet and the IoT, the definition of all possible exceptions appears as a difficult task. Sigfox believes that graded regulations stating strong principles and giving authorised authorities the flexibility to develop progressive and tailored decision or guidance based on clear criterion such as data and applications' sensitivity, scope of the services and market maturity are appropriate tools to foster economic developments and to allow for ease of innovation.

3.18. Sigfox believes that some legitimate exceptions could consist in the legitimate interest of the Data Controller of Personal Data, and where applicable of other stakeholders in the digital ecosystem processing personal and non-personal data, to process such data. This legitimate interest could be for example the need to provide the service subscribed by the Data Subjects or the need for technical intervention on the network to ensure the quality of the service provided to Data Subjects.

3.19. More particularly, the checks and balances to be considered pertaining to law surveillance and enforcement contexts should focus on the proportionality made between the necessary protection of public order and the fundamental protection of individuals' privacy. The relevant legal requirements should also ensure not placing an excessive burden on the stakeholders of the digital ecosystem so that cooperation with public authorities remain cooperation rather than co-investigation, especially considering M2M communications which may have relative relevance for national authorities when compared to person-to-person communications. Lastly however, the burden of the costs incurred by the stakeholders to face and respond to law surveillance or enforcement requests should be considered by the regulator.

Q12 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?

3.20. The report on "Cross-Border Data Flows: Where Are the Barriers, and What Do They cost?" from Information Technology & Innovation Foundation ("ITIF") analyses the privacy and security "justifications" that nations offer for enacting barriers to data flows. The report indicates that in most instances, data localisation mandates do not increase commercial privacy nor data security. What is important is that the company involved is dedicated to implementing the most advanced methods to prevent such cyber-attack.

3.21. A growing body of research has examined not only the relationship between cross-border data flows and economic growth but the economic costs engendered by limiting cross-border data flows. For example, the International Trade Commission ("ITC") study estimated that removing foreign digital trade barriers would increase U.S. gross domestic product ("GDP") by $16.7 to $41.4 billion (0.1 to 0.3 percent) and wages by 0.7 to 1.4 percent in the seven digitally intensive sectors[1].

[1] Reference to United States International Trade Commission published "Digital Trade in the U.S. and Global Economies, Part 2".

3.22. The study shows that data localisation will increase the operational cost of the company. For example, if Brazil had enacted data localisation as part of its "Internet Bill of Rights" in 2014, companies would have had to pay an average of 54% more to use cloud services (of all categories) from local cloud providers compared with the lowest worldwide price.

3.23. For example, the European Commission recently proposed a Regulation which aims at implementing a free-flow of data principle between all European Member States and prohibiting unjustified national data localisation obligations for European economic operators. This kind of initiative represents a real opportunity to develop data market geographically while remote access of national authorities for public order protection will remain possible through an international harmonised cooperation procedure. In this Proposed regulation for example, the national industries would be solicited to soft regulate this international free flow of data from a security point of view through industry "Codes of Conduct".

3.24. On the other hand, countries like India with striving innovation and technology growth could offer data-based services to multiple other countries, provided there is an open framework that provides good data-privacy guarantees. For instance, data hosting and data mining services could be offered from India to service providers abroad, similarly to what the software development and customer services worldwide industries are implementing by off-shoring these services.