GSM Association
Level 1, Red Fort Capital
Parsvnath Tower,
Bhai Veer Singh Marg, Gole Market
New Delhi-110001, India
Tel: +91 (011) 66782420
Fax: +91 (011) 66782403
Web: www.gsma.com

6 November 2017

Mr Arvind Kumar,
Advisor (BB&PA)
Telecom Regulatory Authority of India
Mahanagar Doorsanchar Bhawan
JLN Marg, New Delhi – 110002

Dear Mr Kumar

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

The GSMA would like to thank the TRAI for the opportunity to submit its feedback and comments related to the above consultation and for agreeing to an extension to the original deadline.

The GSMA looks forward to further working with all stakeholders in India, to develop a data protection policy that protects the private data of citizens; is non-discriminatory across sectors and does not impact negatively the incentives for investment and innovation. Balancing the interests of citizens to the protection of personal data, without impairing the development of emerging business models and technologies which have the potential to benefit citizens and consumers greatly, is the challenge.

Please do not hesitate to contact us if you have any questions regarding this submission or any other matter in which we might be of help to the TRAI and other stakeholders in India:

Mr Boris Wojtan, Director – Privacy, GSMA; bwojtan@gsma.com
Mr Saurabh Malhotra, Policy Manager, GSMA; smalhotra@gsma.com

Yours sincerely,

Emanuela Lecchi
Head of Public Policy, APAC
elecchi@gsma.com

Copy to: Sh. Bharat Gupta, Joint Advisor (TRAI)

GSMA response to the TRAI Consultation on:

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

06 November 2017

New Delhi

The GSMA represents the interests of mobile operators worldwide, uniting nearly 800 operators with more than 250 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and Internet companies, as well as organisations in adjacent industry sectors. The GSMA also produces industry-leading events such as Mobile World Congress, Mobile World Congress Shanghai and the Mobile 360 Series conferences.

For more information, please visit the GSMA corporate website at www.gsma.com

Introduction

The growth of mobile services in Asia Pacific has been exponential in recent times. As of the end of 2016, there were 2.7 billion unique mobile subscribers and by 2020 it is projected that there will be 3.1 billion mobile subscribers, three quarters of the population[1]. Fuelled by growing access to mobile data services, the mobile ecosystem is flourishing, providing a platform for innovation that is generating employment opportunities and spurring the creation of new services.

The Internet and the wider digital ecosystem around it has also changed. Where once you might see clearly defined segments in a value chain, you now see content providers, hosting providers, advertisers, access providers, online service providers, software and operating system developers all competing in each other's space. In such a converging world it is reasonable to ask what the rules should be, whom they should apply to and who should enforce them.

These questions are challenging for policymakers around the world. In the European Union, proposed rules for 'ePrivacy' recognise that confidentiality of communication should be assured not just by traditional telecoms companies but by any organisation that offers electronic communications. How far such rules should go given that the EU has recently passed its General Data Protection Regulation (2016/679) ('GDPR') which applies horizontally to any processing of personal data and which agency should supervise the rules is still the subject of heated debate. In the United States, the Federal Trade Commission and the Federal Communications Commission have both sought to supervise data privacy in relation to common carriers. In Sweden, the national regulatory authority for telecom has apparently pooled resources with the data protection authority. In Thailand, data privacy will soon be dealt with in a generally applicable law rather than just in relation to telecom companies.

In India, telecom companies are currently subject to stricter requirements than the internet companies that provide similar services over the telecom infrastructure. There will be an opportunity to reassess this imbalance in the near future as the government considers the adoption of new general data protection rules. Following on from the Report of the Group of Experts on Privacy from October 2012 led by Justice A.P. Shah (the "Group of Experts" report), the government has set up a new committee under the leadership of Justice B.N. Srikrishna to identify key data protection issues in India and to recommend methods of addressing them. Moves towards a new comprehensive data protection law have been given further impetus by the recent 9-judge Supreme Court judgement which clarified that the constitution did protect privacy as a fundamental right.

One thing seems certain. It no longer makes sense to compartmentalise digital and related services. Instead, there needs to be a horizontal law that applies to all

[1] The Mobile Economy, Asia Pacific 2017, GSMA

processing of all personal information as a starting point and any additional requirements to address specificities should be kept to a minimum.

Regulatory principles for the digital ecosystem should not single out Telecom Service Providers (TSPs) by applying stricter requirements and should be based on applying the same principles for the same service, ensuring a single, consistently applied framework is in place covering all competitors/ecosystem players in the digital value chain regardless of technology or the type of provider.

In this way, broadband penetration can continue to expand with positive benefits for digital inclusion and innovation.

Keeping the above backdrop in mind, in the subsequent section, we respond to the specific questions raised by TRAI in its 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?

Response: In order to keep up with changes in technology and business models, protection for telecom subscribers should be rooted first and foremost in principles-based rules that apply to **any body corporate** that collects and processes personal data. To the extent that further rules are considered necessary to protect the confidentiality of communications, or to address issues arising out of big data analytics, these should be kept to a minimum and should apply to all providers of communications services.

The data privacy and telecom regulatory requirements applicable to **all** the players in the eco-system in India, (including the Information Technology Act 2000 and the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules 2011 (the 'Reasonable Security Practices Rules') issued under the IT Act (the "**Horizontal Rules**')) are less stringent than the requirements to which our members are subject. It is our view that, in light of the changes to the ecosystem mentioned above, and the fact that the IT Act is equally applicable to the Telecom operators, any requirements over and above horizontally applicable rules (e.g. additional requirements in licences) need to be carefully scrutinised and justified. If there is no reason to subject an internet player to a particular rule, then there is no reason to subject a telco that offers a functionally equivalent service, to that same rule, thereby avoiding conflicting provisions/positions and an uneven playing field amongst competitors.

Having said that, the current Horizontal Rules in India do not reflect fully internationally recognised data privacy principles such as notice, choice and consent; and access and correction (on consent, see also answer to question 2). These principles should be assessed for their relevance in the Indian context by the government through the newly appointed committee mentioned above (the committee set up under the leadership of Justice B.N. Srikrishna to identify key data protection issues in India and to recommend methods of addressing them). If the principles need to be included in the Indian system, then the Indian IT Act should either be amended to align more with internationally recognised data privacy principles or it should be replaced by a comprehensive horizontal data privacy law i.e. applicable to the entire value chain in a digital economy.

The GSMA agrees with the TRAI recommendation to implement certain National Level Privacy Principles that could act as a starting point "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." (See paragraph 2.2 of the Consultation Paper)

In the GSMA's view, any system of data protection implemented in India needs to be applicable to all sectors, by way of Horizontal Rules. These should be aligned with internationally recognised, principles-based data privacy legislation around the world. The GSMA believes that a principles-based approach to privacy helps protect the interests of citizens generally and, because principles are by their nature flexible, they can adapt to new technologies and capabilities such as big data analytics as they arise and apply to the specificities of different sectors, including the telecom sector. In particular, the Horizontal Rules would benefit from concepts such as privacy-by-design and a risk–based approach which obliges organisations proactively to assess and mitigate risks of harm to individuals. The review of the current system would also be an opportunity to clarify that personal data, including telecom data, can be transferred out of the country provided that the data remains subject to an equivalent standard of protection and individuals' rights are not prejudiced.

Any additional law or licence requirements imposed on a particular sector or technology should be kept to a minimum and be subject to rigorous scrutiny as to the reasons why that particular sector or technology needs special rules. Specific conditions in a telecoms license pertaining to privacy, security and ownership of data should be removed or reduced to what is absolutely necessary after a proper review; the new framework should ensure that the same rules should made applicable to all providers of communications or equivalent services.

However, for matters where the general principles may require to be adapted to sectoral specificities or new technologies, for example in relation to placing of cookies, adapting the principles should be a matter for good practice guidance. This could be issued by regulators but, preferably, should be applied and administered by the industries or bodies concerned. The GSMA, for example, has developed a set of ***Mobile Privacy Principles***, which describe the way in which mobile consumers' privacy should be respected and protected when they use mobile applications and services that access, use or collect their personal data. The GSMA principles do not replace or supersede applicable law, but are based on recognised and internationally accepted principles on privacy and data protection. These principles seek to strike a balance between protecting an individual's privacy and ensuring that individuals are treated fairly while enabling organisations to achieve commercial, public policy and societal goals.

There is an important point of difference between what constitutes "personal data", which arguably merits a high level of protection (especially for sensitive personal data, such as medical records) and the treatment of "metadata", or data processed through an algorithm. The latter have the potential to realise important social and economic benefits that need to be recognised. The GSMA's guidance on big data analytics takes into account these considerations in big data analytics, to ensure that guidance is compatible with recognised privacy principles. Some of the guidance provided relates to the way that transparency and control are provided to users, and how to describe the purpose of processing to users, to encourage good data privacy practices in the context of big data analytics.

Big data analytics and IoT depend both on the availability of data and on consumer trust. The mobile industry is determined to help realise the economic and societal benefits of big data analytics through good digital responsibility practices, so that society can unlock the huge potential of big data analytics in a way that respects well established privacy principles for personal data and fosters an environment of trust.

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?

Response: The definition of 'Personal Information' in the Reasonable Security Practices Rules is already quite broad and does not require any changes:

> "Personal information" means any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person.

This wide definition is necessary to ensure that the rules do not become outdated or perceived as applying to particular sectors or types of company. In addition, having a broad definition allows organisations to determine when something complies with the appropriate level of safeguards, depending on the likelihood of harm. For example, if key-coded or pseudonymised data is given to a service provider for storage or processing without the key, then the controller may be content with the service provider's security protocols without feeling the need to impose additional security measure.

The Reasonable Security Practices Rules go on to define 'Sensitive personal data or information' but several points need to be highlighted and understood in this regard.

First, some personal data is of a more sensitive nature (Sensitive Personal Data). Typically, Sensitive Personal Data include not only information about physical or mental health but also information about racial or ethnic origin, political opinions, religious beliefs, trade union activities, sexual life, or details of criminal offences.

Second, the Reasonable Security Practices Rules apply mainly to the processing of Sensitive personal data or information. The level of protection required for Sensitive Personal Data is higher than the level of protection afforded to less sensitive data. The rules should therefore make a clearer distinction between the principles that apply to processing of all personal information and those additional protections that apply only to processing of Sensitive personal data or information.

Third, under the Reasonable Security Practices Rules Sensitive personal data or information may be transferred to a body corporate or person located in another country[2] if necessary for the performance of a contract. It should be made clear that international transfers of any personal information should be permitted if the destination country has an adequate level of protection, or if the body corporate responsible for the data has ensured sufficient safeguards. In specific cases, international transfer of data may have an impact on national security and this should be assessed on a case by case basis. Further, a number of tools have been developed in other jurisdictions to help organisations manage data flows, such as the APEC cross-border privacy rules, the EU Standard Contractual Clauses. Entities who transfer personal data (either sensitive or less sensitive data) to other countries should be subjected to the privacy and data protection laws of the country where the services are being provided to the customer.

Fourth, it will become increasingly important in an age of big data analytics and IoT to have explicit recognition that anonymous data **is not** personal data and that pseudonymisation can provide genuine safeguards **without the need for consent**.

While consent may be considered as a tool for empowering the consumers, it also poses certain difficulties and, some would argue, does not even protect the individual very well as consumers notoriously click their consent to all kinds of agreements and eventually become fatigued by constant requests. There are logistical difficulties in collecting and tracking consents for different groups of consumers as they have come on board (e.g. through acquisition) not to mention going back to all of them for any new processing.

In order to maximise the chances for innovation and economic growth, companies need to have flexible grounds for processing such as processing for purposes that are compatible with the original purposes, or processing where it is in their legitimate interests to do so and the interests of the individual do not outweigh those of the company. These kind of grounds for processing encourage companies to think genuinely about the risk of harm to individuals and how to mitigate the risk. We believe that reliance on consent can lead to a tick-box mind-set.

Controllers can give consumers an element of control over personal data that relates to them without necessarily obtaining a consent, for example, through greater transparency, dashboards or tools to “opt in” or “opt out” of certain processing and by providing easy access to the data and their previous consents. The controllers or entities handling customer personal (and especially Sensitive Personal) data should

[2] “7. Transfer of information.-A body corporate or any person on its behalf may transfer sensitive personal data or information including any information, to any other body corporate or a person in India, or located in any other country, that ensures the same level of data protection that is adhered to by the body corporate as provided for under these Rules. The transfer may be allowed only if it is necessary for the performance of the lawful contract between the body corporate or any person on its behalf and provider of information or where such person has consented to data transfer” *[Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011]*

adhere to the customers' right to be forgotten and should consider any customers' request to delete his/her personal data at termination of the services (except for the data that is required to be store under law for certain duration), bearing in mind that anonymous data is not 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.

Response: The GSMA believes that the best mechanism to regulate data controllers is to set out the principles which controllers are expected to uphold (such as the National Level Privacy Principles proposed in the Report of the Group of Experts on Privacy) and to encourage them to adopt comprehensive internal compliance programmes. These should help them not only to comply, but also to be able to demonstrate to consumers and regulators how they comply. This allows companies a measure of flexibility to comply in a way that makes sense in the context of their business and allows regulators to supervise where it matters rather than being inundated with prior authorisation requests.

Data controllers can use GSMA tools like *Privacy by Design Guidelines for Mobile Apps* and related *Accountability Framework* to guide their practices and provide reassurance to consumers and regulators. Similar to the entities operating in the Internet ecosystem, the data controllers cannot be allowed to have rights that supersede the rights of an individual to privacy of their personal data, and a compliance programme should allow companies to reassure the public about this.

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?

And

Q. 7 How can the government or its authorized authority set-up 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?

Note: this response relates to both Q4 and Q7

Response: It would be important to educate the public to the difference between personal data, Sensitive Personal Data and metadata. Fears relating to abuse of personal data and specifically Sensitive Personal Data should be countered by

encouraging good practice and transparency. Adherence to rules (in law or from internal policies) can be checked by the companies themselves or by third parties such as accredited standards bodies like ISO for security; or by auditing firms that have the requisite expertise and capability. Regulators can fulfil their legal duties to supervise companies efficiently by relying for reports in most cases and reserving their own audit resources for high profile cases or cases where there is a significant risk of harm.

Technological controls can be put in place by companies to regulate some processes. However, in many cases human intervention is still needed. For example, a "fair processing notice" is expressed in a myriad of different ways and contexts, so it is hard for a computer to understand whether the notice is sufficient. In such cases, best practice is for the companies to document their policies and processes and adopt principles that increase accountability. For example, in some jurisdictions, industry-led trust marks, self-certification schemes, and Codes of Conduct have integrated auditing to facilitate accountability. While these initiatives may benefit from government support, they are (and, in a dynamic context, such as the digital economy, should be) industry-driven solutions.

In the context of cross border data transfers, the APEC Cross Border Privacy Rules system includes "accountability agents" to certify that the privacy policies and practices of participating companies are compliant with the CBPR system program requirements, including adherence to the APEC Privacy Principles, which are based on globally accepted privacy principles.

Through the APEC CBPR system, Accountability Agents work collaboratively with companies, consumers and governments to ensure that cross border personal data transfers meet the standards required by the APEC Privacy Framework.

Stronger economic cooperation, through alignment of approaches and progressive policies and regulations should be adopted to facilitate the growth of the digital economy as a whole and specifically in those sectors that underpin the digital economy, such as Telecommunications, E-Commerce and digital services. Such approaches would include elimination of restrictions to digital trade such as barriers to cross-border data flows and requirements to localise data.

Further, regulators have this flexibility, based on evidence and analysis, come out with instruments to monitor or regulate in an ex-post approach than creating an ex-ante compliance framework for want of any evident market failure or where industry players cannot be said to take care of the same themselves.

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?

Response: Data is a critical asset for competing in the economy. User trust is also critical, and protecting privacy is important to build trust. Governments can encourage the creation of new data based businesses by encouraging the adoption of privacy principles, building regulatory certainty, and permitting businesses to engage in commercial contracts to share data (within a privacy protective framework).

To ensure that the existing mechanisms work well, it is important that markets are monitored and that a sufficient level of transparency is available to do so effectively.

For example, when considering the application of competition law to data it is necessary to strike a delicate balance between stimulating competition (recognising that data can be the key input in the business model of the digital economy), protecting consumers' privacy and providing incentives to invest and innovate.

Different authorities have been looking at the implications for competition law of companies holding, storing and processing large amount of data. In the context of a competition law case, where typically there has been a complaint or in other ways a specific situation has been highlighted to require intervention, the case law in competition law points out to the importance of data for competition, and stresses the importance of taking a case by case approach to appropriately balance the benefits and costs of intervention in each case and to take into full account the specificities of the markets under consideration.

It is important to distinguish a situation where cases are considered on a case-by-case approach under competition law (ex post, after something has been alleged to have a negative impact on competition and consumers) from a situation where some authority is given the right to regulate ex ante (in the absence of any specifically alleged consumer harm). As seen above, regulation of data protection that results in an authority having to approve data protection schemes would likely result in a bottleneck of requests not dealt with properly.

The GSMA believes that a system of internal policies, with external certified compliance is the right approach in regulation. Competition law will be available to ensure that the abuse of data is considered on a case-by-case basis, when consumer harm is alleged specifically (ex post). This is the right approach, given the varied nature of data and its markets. In doing so, competition authorities have to fully consider certain specific issues which relate to the way the data is collected, stored and processed and the complexity of business models based on the usage of data assets (the so-called "platform economy"), the ease of replicability, whether the scale/scope of data collection matters and how all the relevant competitive features in data-driven markets interplay pursuing a holistic approach taking both demand side and supply side effects into account.

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?

Response: A requirement to provide data to a government-mandated data sandbox may choke off investment and innovation incentives and thereby harm consumers; particularly in light of the emerging and dynamic nature of the business models and technologies related to anonymised data. Governmental or regulatory bodies should rather act as catalysts and facilitators to help market and negotiation-based solutions to take off. In the absence of any market failure, a general right to data portability should be governed by private negotiations and free competition, both being based on voluntariness.

This will generally result in more efficient operations preserving investment and innovation incentives to the benefit of users and the entire economy. Sharing data has the ability to enhance the digital economy. For example, there are benefits presented by collaboration, with data as a catalyst for innovation and economic activity. However, we have concerns about the prospect of a requirement to share anonymized data sets via a government-mandated sandbox.

While requiring portability of anonymised data generated by industry could impact intellectual property and trade secrets, there is potential in continued commitment to open government data for use by industry. Sharing anonymised data generated by government systems may help businesses develop new business models and innovation without creating intellectual property and trade secret issues.

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?

(See combined response to questions 4 and 7 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?

Response: Obligations in law to implement security measures that apply horizontally to all players should be expressed as a general standard so that the security is appropriate given the type of data, the state of the art and any other circumstances. Not only this forces organisations to think very carefully about risks of harm, but it also provides a flexible standard that can adjust to new technologies and threats without having to revisit the statue book each time.

Sector-specific rules should only be mandated only if considered absolutely necessary and if justified on the basis of evidence of a particular threat after a robust review.

While no security technology is guaranteed to be unbreakable, attacks on GSM-based networks and services are uncommon, as many would require considerable resources, including specialised equipment, computer processing power and technical expertise beyond the capability of most people or organisations. We are not aware of any data breach that has taken place in the Indian GSM based networks. This in itself should also provide confidence in the ability of the Telcos to safeguard the data of their consumers.

This indeed is a testimony to the robust IT and network security governance model and policies followed by the Telecom operators.

The barriers to compromising mobile security have been very high, and the GSMA considers that research describing possible vulnerabilities has generally been of an academic nature. However, the changing technology landscape and the emergence of new threats and sources of attack requires industry to take an even more proactive approach to protecting networks in future:

- It is important that the mobile industry ensures adequate mechanisms, tools and opportunities are in place to facilitate the sharing of threat and attack information and to ensure the dissemination of information can be done promptly in response to incidents. Such an initiative could include regulators or other government authorities such as national Computer Emergency Response Teams (CERTs). We understand that such a system is already in place in India.

- Securing mobile networks and services is complex, with multiple decisions to be taken by mobile network operators and their suppliers to implement the security standards properly and to deploy and configure a range of features. GSMA offers advice and guidance to its members on how to achieve optimal security levels and continues to work on defining baseline security requirements to be committed to by all mobile network operators

Regulations, where necessary, should be applied consistently across all providers within the value-chain in a service- and technology-neutral manner, while preserving the multi-stakeholder model for internet governance and allowing it to evolve.

Good security practice and policy by industry suppliers is essential. Programmes such as the *GSMA Security Accreditation Scheme*, which provides certification of suppliers, ensures that a commitment to security levels is encouraged and can be evidenced. Security assurance of suppliers and their products has been performed by the GSMA for some time with the Security Accreditation Scheme for SIM suppliers and the current development of a programme for infrastructure OEMs.

The GSMA supports global security standards for emerging services and acknowledges the role that SIM-based secure elements can play, as an alternative to embedding the security into the mobile device or an external digital card (microSD), because the SIM card has proven itself to be resilient to attack.

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?

Response: The fact that non-telecom companies are providing many services that are equivalent to communications services traditionally provided by licensed telecom companies and that many telecom companies have entered other markets such as content provision in the ever-converging internet value chain, demonstrates clearly that horizontal, principles-based rules are needed for all stakeholders operating in the Internet ecosystem.

These should relate generally to the collection and use of personal data and apply to any organisation processing personal data. To the extent that activities include communications, users have an expectation that their communications will be kept confidential. It may therefore be necessary to impose a duty on all providers of communications or equivalent services to keep the content of communications confidential. In some countries such a duty is subject to certain lawful business exemptions (for example checking hyperlinks and attachments for malware). Location data and traffic data that are associated with communications should be treated in the same way as ordinary personal information. It would be up to the company to understand the risk of harm to individuals in each case.

The GSMA and its members believe that privacy and security are fundamental to building consumer trust in mobile services, and are committed to working with stakeholders from across the mobile industry to develop a consistent approach to privacy protection and promote trust in mobile services. For services that they provide themselves to their consumers, mobile network operators will endeavour to protect digital identities, secure communications and personal data.

The wide range of third party services available through mobile devices offers varying degrees of privacy protection. Therefore:

- To give customers the confidence that their personal data is being properly protected, irrespective of service or device, a consistent level of protection must be provided
- The necessary safeguards should be derived from a combination of internationally agreed approaches, national legislation and industry action

From the perspective of being transparent and informing consumers industry, data protection authorities and other regulators should:

- Be clear with consumers about what they do protect, and what consumers should expect in terms of privacy
- Make clear what they have no control over, such as third party applications and services. For sophisticated consumers, this may be known, but for many segments of consumers it is not

When legislation and regulations are being formulated or revised:

- Governments should ensure legislation is service and technology-neutral, so that its rules are applied consistently to all entities that collect, process and store personal data

- **Because of the high level of innovation in mobile services, legislation should focus on the overall risk to an individual's privacy, rather than attempting to legislate for specific types of data.** For example, the same data element can be used to derive value that can be commercial (e.g., sold to third party organisations), operational (e.g., inform internal decision-making and resource allocation) or public (e.g., inform disaster recovery efforts)

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?

Response: Privacy protections should be applied across sectors to provide certainty for consumers and should involve all stakeholders operating in the Internet ecosystem irrespective of the technology and service. A principle based horizontal rules that applies to all entities who deals with customer data, should be considered: operators should have the same flexibility as other players in the broader Internet ecosystem.

The GSMA notes that the ability to collect, store, transmit and use data is an important component of economic and social value created in the digital ecosystem. This raises policy questions in relation to consumer privacy, data protection and national security as identified in the consultation paper.

A new framework should not only ensure equal obligations on all competitors, but also provides consumers with an acceptable baseline level of protection that is proportionate and fit-for-purpose.

It follows that the GSMA believes that there is a need to "bring about greater parity" in the treatment of TSPs and their competitors and this parity should be achieved through

a comprehensive review of the data protection framework across all sectors. If there is a risk of harm to consumers, then arguably they should be applicable across the board.

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?

Response: Governments should ensure they have a proportionate legal framework that clearly specifies the surveillance powers available to national law enforcement and security agencies.

Any interference with the right to privacy of telecommunications customers must be in accordance with the law. The retention and disclosure of data and the interception of communications for law enforcement or security purposes should take place only under a clear legal framework and using the proper process and authorisation specified by that framework. To that extent, in India, there are already defined legal and licensing methods to deal with such LEA requests, hence we do not believe that there is any new obligation/requirement that should be considered for this purpose.

However, the same obligations are not currently applicable on OTT Communication Service Providers who are also providing similar telecommunication services. Therefore, it is important to carry out an analysis of the existing regime. To the extent that any obligations currently imposed on the telecommunications operators are to be retained because otherwise there would be harm to consumers, then all communications service providers should also be subjected to the same rules (e.g. about lawful surveillance and law enforcement) as those applied on telecom service providers under the principles of 'same service, same rules'.

There should be a legal process available to telecommunications providers to challenge requests which they believe to be outside the scope of the relevant laws.
The framework should be transparent, proportionate, justified and compatible with human rights principles, including obligations under applicable international human rights conventions, such as the International Convention on Civil and Political Rights.
Given the expanding range of communications services, the legal framework should be technology neutral.

Governments should provide appropriate limitations of liability or indemnify telecommunications providers against legal claims brought in respect of compliance with requests and obligations for the retention, disclosure and interception of communications and data.

The costs of complying with all laws covering the interception of communications and the retention and disclosure of data should be borne by governments. Such costs and the basis for their calculation should be agreed in advance.

The GSMA and its members are supportive of initiatives that seek to increase government transparency and the publication by government of statistics related to requests for access to customer data.

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?

Response: The international flow of data plays an important role in innovation, competition and economic and social development.

Stronger economic cooperation, through alignment of approaches to ensure that progressive policies and regulations are adopted to facilitate the growth of the digital economy as a whole and specifically in those sectors that underpin the digital economy, such as Telecommunications, E-Commerce and digital services, is desirable. Such approaches would include elimination of restrictions to digital trade such as barriers to cross-border data flows and requirements to localise data.

The governments should recognise that the opportunities for partnerships between international and domestic players, and for the development and growth of local players, are greatest in markets where the regulatory environment supports investment by both international and domestic players.

Therefore:

• Restrictions and conditions on international data flows should be kept to a minimum and applied in exceptional circumstances only (such as threats to clearly defined national security issues, to be assessed on a case-by-case basis).

• Cross-border data transfer rules should be risk-based and support measures to ensure data is handled with appropriate and proportionate safeguards while helping realise potential social and economic benefits

• Also, to the extent that governments need to scrutinise data for official purposes, they should achieve this through existing lawful means and appropriate intergovernmental mechanisms.

A key concern is that cross-border data transfers are currently regulated by a patchwork of international, regional and national instruments and laws that can be both confusing as well as conflicting. Further, they do not create an interoperable regulatory framework that reflects the realities, challenges and potential of a globally connected world. Data protection rules should be made interoperable across countries and regions to the greatest extent possible. Interoperability creates greater legal certainty

and predictability that allows a company to build a scalable and accountable data protection and privacy framework.

Interoperable data protection frameworks would help strengthen and foster appropriate and effective mechanisms to ensure data is managed in ways that safeguard the rights and interests of consumers and citizens. Interoperable data protection frameworks incorporating effective accountability mechanisms can help strengthen and protect important rights that help individuals and economies flourish.

For example, efforts to make the APEC CBPR system and EU Binding Corporate Rules interoperable have the potential to benefit industry, digital trade and consumer interests and rights. The GSMA and its members remain committed to working with stakeholders to ensure that cross-border data flows are managed in ways that safeguard the personal data and privacy of individuals. The GSMA and its members also recognise the importance of addressing challenging issues arising from cross border data flows, including jurisdictional issues.

The APEC's Cross-Border Privacy Rules are a good example of international cooperation that aims to facilitate rather than frustrate flows of data across borders while at the same time seeking to achieve genuine, consistent standards of privacy protection throughout the region.

The phenomenal growth of the internet and innovative, customised services and benefits that it offers can be vastly attributed to the advantage that service providers/companies can take of economies of scale at a Global level. The GSMA believes that clarity should be brought out on what user data cannot be shared outside than a blanket restriction that may be open to varying interpretations