BIF RESPONSE TO TRAI CP ON PRIVACY, SECURITY & OWNERSHIP OF DATA IN THE TELECOM SECTOR

Broadband India Forum (BIF) welcomes the development of a technology and platform neutral data protection law which applies horizontally across all the sectors. The Ministry of IT is already working to draft a comprehensive data protection law that would cover all the sectors and bring uniformity. The Supreme Court has recognized this Committee's role in its recent ruling on privacy being a fundamental right. While drafting this law it is important to take into account the socio-economic impact of Internet-enabled services and apps in India. BIF recommends that in drafting a new policy framework for data protection, the Government look to well-established international standards governing data protection, such as the APEC Privacy Framework and the OECD Privacy Frameworks. These frameworks provide users with control over their personal data, while also allowing businesses to use data and to transfer data across borders with proper safeguards.

A recent study by ICRIER estimates that apps contributed a minimum of USD 20.4 billion in the year 2015-16 to India's GDP, and this contribution is expected to grow to USD 270.9 billion by 2020.This would be nearly eight percent of India's GDP. Interestingly, the study also finds that while 10% increase in total Internet traffic and mobile Internet traffic globally increases global GDP by 1.3% and 0.7% respectively, for India the impact is much higher - 10% increase in total Internet traffic, delivers on average a 3.3% increase in India's GDP, and a 10% increase in mobile Internet traffic, delivers on average a 1.3% increase in India's GDP. A report by Analysys Mason estimates that data driven innovation contributed USD 10 billion to India's Gross Value Added (GVA) in 2015 and this contribution is expected to rise to USD 50 billion by 2020.

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

Below are some of the key considerations for drafting the data protection law to boost the tech led economic growth:

● **APEC Privacy Framework** is a business friendly and user centric framework which also supports cross border data flows and should be considered when formulating the law. It recommends privacy principles of ***Preventing Harm, Notice, Collection Limitations, Uses of Personal Information, Choice, Integrity of Personal Information, Security Safeguards, Access &***

Correction and Accountability. The principles of ***Preventing Harm and Accountability*** particularly standout for being pragmatic and outcome focused by making organizations responsible without stifling trade and innovation. In addition, these principles are informed by the Fair Information Practice Principles (FIPPs) and the OECD principles and were drafted with the digital economy in mind.

● Instead of prescribing privacy practices in form of administrative requirements, the privacy framework should define the broad principles and requirements and allow organizations to design their own privacy programs that could be based on due diligence guidelines. While organizations should be allowed to self-regulate, they should be held accountable for any violations. In case of any breach or complaint, the onus to prove due diligence should lie with the organizations.

● It may not be sufficient to write a good piece of legislation unless it is supported by an adequate implementation ecosystem- institutional capacities and capabilities, industry self-regulation, effective grievance redressal system, user awareness, active civil society, and research. Therefore, privacy law should be outcome driven and focus on building the necessary ecosystem rather than just exclusively focusing on regulating data controllers.

● Data driven innovation and privacy are compatible

● Data is important but ideas continue to matter more

● Personal information needs to be defined contextually & protections applied proportionally

● User consent remains to be valid - a flexible consent regime should be developed

● Users should be empowered through transparency and choice - the law should recognize the market driven developments (e.g. data portability) that have led to increase in user transparency and trust

● Regulatory focus should be on preventing harm & misuse of data than collection per se

● Organizations should be accountable through self-regulation minus regulatory prescriptions

● Regulatory interventions should be evidence based and provide regulatory certainty and consistency

● Cross border data flows should be promoted to enable trade and innovation

● Introducing right exceptions & exemptions (e.g. anonymized data, data processors) in the law, along with necessary checks & balances, should help in supporting economic growth and strengthening human rights

● Privacy framework should be outcome driven - legislation alone is not enough unless supported by an adequate implementation ecosystem including an effective grievance redressal system and user awareness

It is felt that India would do better if it were to instead of copying any country's/region's law , were to develop its own based on its requirement as each society has its own culture and expectations of privacy which needs to be considered. However Global best practices should be considered wherever relevant. **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?**

BIF Response

- There is a need to differentiate between two types of data. Data collected by third parties such as a bank, credit card provider, an over the top application provider etc. as against data carried/stored by telecom operators public policy focus should be on providing regulatory certainty and consistency, preventing harm to users, misuse of personal information and making companies accountable through self-regulation without being prescriptive. The framework should recognize the market/industry driven developments have led to an increase in user transparency and trust. as intermediaries in provision of bearer services to third parties. The data collected by telecom operators for their own use will of course be included in the first type.
- In our view, TRAI being the sectoral regulator for Telecom sector, should only be concerned with the data carried/stored by the telecom operators as intermediaries/bearers. We fully agree that there is a need for a relook at safety of this data in view of the evolving technology and the new data protection law which is being developed. Once the data protection law is enacted, TRAI should review the existing provisions in the Indian Telegraph Act and licensing conditions to recommend changes to the Department of Telecommunications (DoT) to align with the new requirements. DoT/TRAI could also issue advisory or guidelines for the telcos to comply with these new requirements.
- For the data collected by third parties, it is our understanding that a comprehensive data protection Act is under active consideration of the Government.
- Having a technology/platform neutral data protection law which applies horizontally across the ecosystem should be the path forward. The Ministry of IT is already working to draft a comprehensive data protection law that would cover all the sectors and bring uniformity. The Supreme Court has recognized this Committee's role in its recent ruling on privacy being a fundamental right. While drafting this law, it is important to take into

account the socio-economic impact of Internet-enabled services and apps and data driven innovation. A recent study by ICRIER estimates that apps contributed a minimum of USD 20.4 billion in the year 2015-16 to India's GDP, and this contribution is expected to grow to USD 270.9 billion by 2020.This would be nearly eight percent of India's GDP. A report by Analysys Mason estimates that data driven innovation contributed USD 10 5 billion to India's Gross Value Added (GVA) in 2015 and this contribution is expected to rise to USD 50 billion by 2020.

- To make data driven innovation compatible with data privacy, it is critical to empower the users, without over-regulating the data controllers or data collection. The Building capacity of users through education and awareness and strengthening grievance redressal are important considerations. It may not be sufficient to write a good piece of legislation unless it is supported by an adequate implementation ecosystem.

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?

BIF Response

Personal Information: The Rules(Information Technology Rules 2011-Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) framed under Sec 43A of the Information Technology Act define personal information ***as 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***. The Indian definition of personal data is in line with international norms. The direct/indirect dual classification of personal data is found in the laws of the United States, most European countries, Australia, Singapore, Japan, and others. however, we believe that any proposed legislation should explicitly recognize the role that purpose, context and proportionality (including voluntary disclosure) play in determining whether a particular piece of information in isolation or in combination with other information constitutes personal information.

- When GDPR comes into force, the European definition of personal will expand to include online identifiers, location data, and genetic information.

    - Online identifiers include cookies, IP addresses, RFID tags, device IDs, and so on. Location data means information about a person's movements derived from cell towers, mobile apps, geo-location metadata from images or apps, and so on.
- Online identifiers and location data serve necessary purposes. They enable online advertising, without which the internet would no longer be a free resource.
    - A British study in 2014 found that without online advertising, users would each have to pay around ₹11,500 (£140) a year to access internet content.[1]
- The current estimated 450-465 million Indian internet users depend on online advertising to keep the internet free, affordable, and accessible. The rapid growth of the internet has been fuelled by revenues generated from online advertising.
- If online identifiers and location data is more heavily regulated, it will directly impact internet growth in India. Moreover, such regulation would slow the growth of India's nascent online advertising industry.

Whether a particular piece of data qualifies as PI or not is highly dependent on the context and situation. "The same piece of information can be personal in the hands of a certain data controller and functionally anonymous in the hands of another data controller- e.g.- possession of license plate number in the hands of an insurance company can be considered as personal information but the same plate number in the tape of a security camera in a petrol station will not be personal information, as the station has to take considerable efforts for determining the identity of the person." (Justice A P Shah Report; Page 67). Hence defining Personal Information (PI) broadly (e.g. encompassing data such as IP addresses) may not be the right approach.

Defining personal information broadly could unnecessarily increase the compliance burden on business, particularly small and medium-sized enterprises (SMEs) and startups, without necessarily increasing the level of data protection.

The definition of personal information should provide legal certainty, but as recognised by the Supreme Court it must also apply to various contexts and be applied proportionally. Proportionality means that the appropriate level of protection is applied to different kinds of information. For instance, the debate on financial information as sensitive personal information is a good example. While such transactional data may be personal to the user, it is also business information of the company making the financial transaction, and may assist the company in determining the user's potential and in offering her more focused services. Imposing additional emphasis on consent, restricts the growth of businesses especially in areas where the business may not have foreseen while taking consent.

Given that much of the economic value of data is generated through processing of anonymized and de-identified data, the data protection law under consideration should incentivize the

processing of such data over personal data where appropriate. While anonymized data should be kept out of scope of the law, for de-identified data, at a minimum, there should be reasonable exemptions. Singapore and Japan provide a good reference point when it comes to dealing with anonymized data.

● **Consent:**

BIF supports a regime that both puts users in control of their personal data and offers flexibility for businesses to use data in certain legitimate ways that further public and business interests. The policy framework pursued by the Government should aim at restricting potentially harmful uses of data while allowing for many beneficial uses. If consent is the only basis for the processing of data, the law may foreclose beneficial uses of data and fail to keep pace with technological developments that may render consent impractical or undesirable.

It has been argued that consent is meaningless in the information age. This argument is too simplistic. While some have raised concerns around misuse of consent to put obligations on users and to acquire broad permissions, consent still plays an important role in being transparent with users. A better approach would be to contextualise the way consent is expressed by individuals according to the kind of service they are using, the sensitivity of the data and to the potential harm arising from its use. Appropriate balance is needed, keeping in mind various perspectives:

○ ***Sensitivity of information/transaction*** - while explicit consent may be important for collection and processing of sensitive personal information; PI can be collected and processed through implied consent provided it is coupled with user transparency, empowerment and control (e.g. easily opting out of a service later) and organizational accountability.

○ ***Consumer Behavior & Convenience*** - The law should be pragmatic and take into consideration consumer behaviour aspects when putting in place requirements around user consent, including the form and manner of obtaining such consent . For instance, users may also not like to provide consent for every transaction as it may adversely impact user experience and introduce latency in the transactional flow. Businesses typically design the consent flows based on consumer research. It is important to put users in control.

○ ***Legitimate interests***: For the persuasion of legitimate interests and justifiable reasons, the law should consider providing multiple legal bases for collecting and processing personal data rather than solely relying on user consent. Examples include medical emergencies, the need to detect and respond to fraud, cybercrime, cybersecurity threats, and spam, including security scans on devices which is critical for user safety. If users choose not to consent to the use of their data for these purposes, the safety and integrity of communications systems may be

compromised. For this reason, data protection laws in Singapore and the European Union, for example, permit the processing of data for certain purposes without user consent.

To harmonize privacy concern and effective data use, it is necessary to consider implementing flexible consent recognition based on various scenarios. It has been argued that "mandatory opt-in applied across contexts of information collection is poised to have several unintended consequences on social welfare and individual privacy:

- Dual cost structure: Opt-in is necessarily a partially informed decision because users lack experience with the service and the value it provides until after opting-in. Potential costs of the opt-in decision loom larger than potential benefits, whereas potential benefits of the opt-out decision loom larger than potential costs

- Excessive scope: Under an opt-in regime, the provider has an incentive to exaggerate the scope of what he asks for, while under the opt-out regime the provider has an incentive to allow for feature-by-feature opt-out.

- Desensitisation: If everyone requires opt-in to use services, users will be desensitised to the choice, resulting in automatic opt-in.

- Balkanisation: The increase in switching costs presented by opt-in decisions is likely to lead to proliferation of walled gardens."

- ● **User Empowerment**: Given that privacy means different things to different users, it is important to put users in control by providing the necessary information and options to exercise their choice meaningfully wherever relevant. For instance, any mobile OS platform empowers users to grant granular permissions to the apps they install on their devices through the Play store. The mobile OS platform requires apps to ask for runtime permissions when users install an app for the first time, after going through what permissions it would need before downloading and installing. Through easy to navigate settings, users can change these permissions anytime. To enhance user transparency and trust, many companies provide 'one stop shop' privacy help center, easy to understand privacy notices, single view of what PI is collected and processed by the company.

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.

BIF response

To make data driven innovation compatible with data privacy, it is critical to empower the users, without over-regulating the data controllers or data collection. The public policy focus should be on preventing harm to users, misuse of PI and making companies accountable through self-regulation without being prescriptive.

The responsibilities of data controllers are clearly set out in the Personal Data Rules(Information Technology Rules 2011 (Reasonable security Practices & Procedures and Sensitive Personal Data or Information).

They are:

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

- Data controllers and data subjects are not in conflict. The rights of one do not supersede the rights of the other. Data subjects voluntarily offer their personal data for the convenience of customised services, and data controllers are able to make such services commercially viable while improving the products and customer experience. It is symbiotic relationship in which both parties are winners.
- However, while user rights are enshrined in the Personal Data Rules, the rights of data controllers are absent.

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

- In terms of regulatory mechanisms for controllers, the TRAI should support privacy guidelines developed by industry and other stakeholders before moving toward regulation. Industry voluntary efforts, best practice codes and multi-stakeholder initiatives all drive privacy protections in ways that make sense for the providers and consumers of covered technologies.
-

When regulation is pursued, it should be as light-touch and flexible as possible. Any regulation should be based on general standards and not be overly prescriptive. Otherwise, regulation will not keep pace with rapidly evolving technology and markets.

Data processors: The data protection law should make distinction between a data controller (organization which determines means and purpose of data collection) and data processor (organization processing data on behalf of the data controller) roles. This is an important consideration given that legal liabilities and obligations would differ based on the role an

organization is playing. "The data controllers should primarily be responsible for complying with the law. If anything, data processors should be responsible to take the necessary technical and organizational measures to secure the data they process on behalf of the controller. The 'controller-processor' relationships are governed through contractual means and the law should not unreasonably intervene in these relationships. It is important to note that the Indian IT industry (acting as data processors) has been negatively impacted due to restrictions to the transfer of data under the EU Data Protection Regime. Also, the rules issued under Section 43A of the Information Technology Act did not make a distinction between controller and processor and this led to lot of confusion and backlash. To address industry concerns, the government later issued a clarification which helped create the desired distinction and exempted processors from certain requirements. The new law should avoid such a situation.

● Given that Ministry of IT is already working on a comprehensive data privacy law which would be applicable across sectors, this issue will eventually be addressed. The rights of the data controllers and users are not necessarily in conflict.

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?

BIF Response

There is no need for proactive government monitoring as market forces are sufficient to drive this change and there are positive developments to show this evolution. Also, given the nature, scale and volume of transactions happening on the Internet every second and multiple players involved in each transaction, it may not be practically possible to create a centralized ex ante tech based compliance system.

A technology-enabled consent architecture with audit-based mechanisms and a workforce of auditors is not the most effective or efficient way to promote best practices and to ultimately avoid or minimize harm.

It would be more effective to develop mechanisms that incentivize privacy protective practices through self-regulation and accountability measures. , paired with explicit legal incentives such as statutory presumptions of compliance (by, for instance, limiting the scope of investigations or the frequency of audits or enabling paths for legitimate data transfers) and statutory reductions of fines.

Organizations should be required to develop self-enforced risk-based frameworks. This would allow them to focus on high-risk data uses to minimise harms while monitoring low-risk situations or other common and everyday uses of data.

Data harms must be empirically proven and mapped before there is further regulation, and any regulation must be narrowly tailored to prevent concrete, identified harms without hindering beneficial uses of data.

As discussed in response to Q2, the tech platforms are already building such capabilities to empower users to better understand their PI usage and control their data. It is recommended that policy responses focus on building understanding among users through education and awareness, making organizations accountable through self-regulation and strengthening grievance redressal. Also, the policy must take into account that the digital economy is thriving in part because most businesses work hard to maintain user trust and confidence. Brand safety is perhaps a motivation bigger than fear of regulations

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?

BIF Response

- In a free market, the proper role for the government is to prevent harms and promote security. Over-regulating the market interferes with the freedom of trade that businesses are guaranteed by the Indian Constitution and dis-incentivises competition and efficiency.
- When businesses compete, consumers benefit. For technology companies to develop products that offer the most convenience to users, they must invest in R&D and constantly find better ways of using data to deliver consumer benefits. Such techniques include features that enable users to control their data, data aggregation& annonymization,and analytics,.
- The direct result of these techniques is innovation and market disruption. The world's leading tech companies started small but grew because they constantly innovated and disrupted existing market monopolies.
- New businesses that are successful have followed the same high-innovation, disruptive-market approach. Several Indian businesses that have succeeded in winning consumers and capturing the market based on the superiority of their products.
- The government has an understandable interest in promoting Indian businesses. However, it should do that without sacrificing the interests of Indian consumers who continue to benefit from existing big data businesses.

To make data driven innovation compatible with data privacy, it is critical to empower the users, without over-regulating the data controllers or data collection. The public policy focus

should be on providing regulatory certainty and consistency, preventing harm to users, misuse of PI and making companies accountable through self-regulation without being prescriptive. Further, building capacity of users through education and awareness and strengthening grievance redressal are important considerations.

Legislation itself will not suffice, it must be supported by an adequate implementation ecosystem, including institutional capacities and capabilities, industry self-regulation, effective grievance redressal system, user awareness, active civil society, and research. Therefore, privacy framework should be outcome driven and focus on building the necessary ecosystem.

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?

BIF Response

Businesses should be able to use public data sets and share data responsibly, but mandating that businesses share data is not justified and in fact per se does little to nothing in favor of innovation. The private sector is best positioned to innovate and develop solutions to this problem. For example, GSMA's Big Data for Social Good initiative is conducting trials with its members in this area.

We urge allowing data access by academics or other researchers for public value rather than general publication of data sets (which has led to re-identification in many cases). The law can help this sharing by helping create standards for sharing and limited liability. The government should continue to promote publication of data sets by government agencies under the open data policy for national planning and development purposes.

Several experts and researchers have argued that data is just one input of many in the process of innovation and market success is not a barrier to entry. There have been several startups in the recent past that have become successful - Examples - Tinder — an online dating app that launched less than 3 years ago — is adding a million users a week and is already valued at over $1 billion. For example, the food startup Zomato is India's first e-commerce unicorn to break even, and is headed for profitability.

- The right to property is a constitutional right under Article 300A of the Constitution, which prohibits the state from depriving someone of their private property except through statutory law.
- According to the Supreme Court in the *Super Cassette* case (2008), "property" in Article 300A includes intellectual property, particularly data that is subject to copyright.[2]

Section 2(o) of the Copyright Act, 1957 defines data as a 'literary work,' thereby protecting it under copyright law and therefore qualifying it for constitutional protection under Article 300A.

o .

- Compelling businesses to surrender their proprietary datasets to the sandbox is a deprivation of property with constitutional implications.
- If proprietary datasets were forcefully but lawfully acquired in accordance with Article 300A, such an action would *prima facie* implicate the fundamental right to trade under Article 19(1)(g) of the Constitution.
- Big data businesses that have Indian subsidiaries and are governed by Indian law have brought cutting-edge technology and know-how to India. Such businesses continue to invest heavily in India. They are entitled to the equal protection of Indian laws.
- Since there is no dearth of data in India, which is a data-rich country, there is no need to create a data sandbox. 69 percent of Indian users are still offline and internet penetration is rapidly expanding.[3]Millions of new users are accessing the internet for the first time every year. There are still around 175 million future users in urban areas and around 750 million future users in rural areas.
- Requiring regulated companies to maintain this kind of data set would tantamount to regulatory overreach. The regulatory concerns here seem to be consumer protection and fair competition. But the private sector is best positioned to innovate and develop solutions to this problem. In fact, India is home to the third largest number of technology driven startups in the world that are innovating to address global and local market needs.
- While we agree that it is important users are not locked into one particular provider we do not think that static data sets with anonymized data are the right path to fostering innovation. Industry members are developing innovative solutions that support new market participants by allowing users to export their data and sign up with a competitor. Data portability from a consumer perspective should be encouraged.
- That said, we urge allowing data access by academics or other researchers for public value rather than general publication of data sets (which has led to re-identification in many cases). The law can help this sharing by helping create standards for sharing and limited liability. The government should continue to promote publication of data sets by government agencies under the open data policy for national planning and development purposes.

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?

BIF Response

-
- Across the world, data protection compliance has been achieved on the basis of evidence-based policy, market-based models such as compliance incentivisation, superior enforcement, and specific contractual performance.
- Technology developments are so dynamic that attempting to monitor for compliance will likely place significant, if not overwhelming, burden on a government owned and operated tech enabled compliance system. Additionally, this is likely to raise privacy concerns as it installs a system of government monitoring and surveillance. Industry is best placed to comply with the privacy principles under a self-regulatory framework and putting users in control is critical
- If a technology solution is created, it is crucial that it does not create geo-fences or attempt to achieve data localisation.
    - Because the data ecosystem is globalised, Indian IT companies have been able to thrive as the bulk of their revenues come from United States and Europe. In order to serve Indian interests, the globalised nature of the internet should be protected. We should not create any technical system to monitor the same as it could be visualized as creating geo fences and oversight by authorities on others' data. Given the pace of march of technology, this would lead to creation of bureaucratic hurdle in the process as before implementing a new technical solution, one would have to wait for monitoring process to be first in place.
- There should be no technical controls on cross-border data flows. Such controls would alter the internet's fundamental architecture. That would slow the growth of the internet in India.

Instead of government monitoring, the legislator should be encouraged to recognize and endorse a culture of corporate accountability, that would limit the ex ante enforcement approach to a minimum. This has been the approach of other privacy enforcement authorities who have seen how effective privacy and data protection are better achieved by incentivizing companies to adopt best practices and demonstrate that they are accountable to their users. This approach, which is perfectly compatible with effective enforcement, constitutes the essence of the APEC Cross Border Privacy Rules (CBPRs) regime.

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?

BIF Response

- There are three main inconsistencies regarding encryption regulation.
    - Firstly, while telecommunications is declared to be a 'critical information infrastructure,' no attempts have been made to secure that infrastructure through the use of strong encryption.

        - The primary means of achieving data security is through the widespread use of strong encryption. However, the Central Government has still failed to issue rules to govern encryption under section 84A of the IT Act to promote strong encryption.
    - Secondly, while Indian ISPs are bound to 40-bit encryption keys, the rest of the internet is significantly more secure.
        - The DoT's ISP licence restricts the use of encryption to key lengths of 40 bits and below, which is a primitively low standard. However, third-parties such as email service providers or OTT providers are not prevented from using longer encryption keys.
    - Thirdly, overlapping and inconsistent sectoral encryption standards have created an uneven playing field.
        - Specific regulators such as the RBI and SEBI stipulate the use of longer encryption keys for certain purposes, which has resulted in multiple, inconsistent encryption standards.
- The government should encourage the use of strong encryption wherever possible. Encryption regulations should be harmonised to unanimously promote the use of strong encryption. The government should issue rules under the IT Act to compel the use of strong encryption.
- Moreover, since weak encryption is a competitive disadvantage in privacy-conscious markets, the government should encourage Indian businesses to make strongly encrypted products to compete in global markets.

As mentioned in the responses above, the following steps need to be taken to secure the digital ecosystem:

o Empowering users by giving them control over their data; recognizing the industry efforts in this direction which are based on brand safety and competition

o Not restricting collection of data but focusing on misuse of data and preventing harm

o Making organizations accountable through self-regulation without being prescriptive

■ Example: for data security government mandating specific security standards or technologies is not the right approach. The cyber threat landscape is ever evolving and regulatory prescriptions will only drive organizations towards compliance instead of addressing such evolving threats. Security concerns can be best addressed through voluntary adoption of contemporary standards and technologies by organizations. They are accountable under the data protection framework to keep the data secure.

o Building capacity of users through education and awareness

o Strengthening grievance redressal mechanisms instead of proactive monitoring .

Preserving Data confidentiality is the fundamental motivation for ensuring security of telecom infrastructure as this sector is one of the key pillars of critical national infrastructure. Vulnerabilities in the telecom infrastructure can lead to disruption in basic services with severe impact on citizens , businesses and delivery of public services . Hence it is essential to ensure that each layer of telecom infrastructure and ecosystem as a whole is protected through adequate security measures.

In conformity to Section 70 of the IT Act which provides for declaration of certain areas as Critical information infrastructure (CII) and need for introducing appropriate measures for security of these systems , National Critical Information Infrastructure Protection Centre (NCIIPC) agency which has been mandated to facilitate protection of critical infrastructure has designated the telecom infrastructure to be one of the critical information infrastructures

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?

BIF response

Every data controller should be responsible for protecting the privacy of its users under the proposed legal framework. Breaking down the ecosystem to understand issues at various levels may be a good approach but having a technology/platform neutral data protection law which applies horizontally across the ecosystem should be the way forward. Also, it is important to recognize the market forces within different categories which are driving development of features that enhance privacy and provide more choices to users. For e.g. many browsers today provide incognito mode, do not track features to users; App permissions can easily be controlled by the users.

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?

BIF response

- OTT services are fundamentally different from traditional telecommunications services. There are physical, technological, and legal differences between the two, so demanding regulatory parity between the two is incorrect legally, conceptually, and practically.
- There are important differences between OTTs and traditional telecoms services providers:

- Telecoms operators control the underlying broadband access infrastructure, with few market players and high barriers to market entry.
- By contrast, OTTs do not control the underlying broadband access point, have significantly lower barriers to market entry and are faced with many competing services. Consumers can add or stop using OTTs at will and are typically not subject to long term contracts.

  Telecom operators enjoy several exclusive privileges that OTT players do not. These include the following:
  - right to acquire spectrum,
  - right to obtain numbering resources,
  - right to interconnect with the PSTN,
  - the right to establish telecommunications infrastructure such as towers, cable
  - Rights of Way

Given that telecom operators enjoy far greater rights than OTT players, it is logical that their obligations are correspondingly greater. To suggest that telecom operators and OTT players can be regulated in the same way is flawed. It ignores the important differences in the nature of their business as well as the substantive rights bestowed to them through their licenses.

The primary legislation governing the telecom operators and OTT players is different. In the former case, it is the Indian Telegraph Act, 1885 and in the latter it is Information Technology Act 2000. The latter legislation, and the rules framed under it, includes detailed provisions relating to privacy and security of data to protect consumers from potential harm through OTT and internet based services. In addition, OTT consumers have the same level of protection as their telco counterparts in matters of contracts.

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

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

Data protection, security and privacy norms should be treated equally on par for all stakeholders of the Digital ecosystem viz. content & application service providers, device manufacturers, browsers, Operating Systems, etc . Due to emergence of new applications like M2M, IoT, etc apprehensions are being cast regarding nature & extent of data being collected

and stored over the Internet cloud , the purpose for which it can be used and security of these devices and the underlying networks including the storage locations etc. Though some of these issues are perhaps covered under the provisions of the IT Act , however a larger and more comprehensive privacy & data protection law is perhaps required. Such a move would need to specifically address issues of identifying categories of data that are sought to be protected , stakeholders that would be bound by requirements of data protection and obligations to be cast on them & mechanisms for enforcement of such obligations

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?

BIF response

- The government has a duty to protect national security and public safety. Compliance with legally-valid government requests for user data is the default position of most data controllers.
- Encryption is a critical tool that the government has to promote privacy, national security and public safety.
    - Strong encryption protects against malicious actors, hostile countries, foreign intelligence agencies, and cyber criminals.
    - Deliberately introducing backdoors in encryption technology substantially undermines the fundamental privacy and security that encryption provides.
- When user data is protected by strong encryption, it may be impossible for data controllers to access that data themselves, much less give it to the government.
    - It is not technologically possible to make it easier for law enforcement to access encrypted communications without making it easier for cybercriminals and foreign governments to do so as well.
    - Creating an encryption backdoor is analogous to building a bank vault with a steel front door but a perpetually-unlocked wooden back door.
- Strong encryption is a competitive market edge.
    - Internet platform providers and mobile app developers that are subject to backdoor requirements will be at a significant competitive disadvantage.
    - The government should promote the use of strong encryption, which will allow Indian products to compete in privacy-conscious markets.

Checks and balances for lawful access: Presently, the data access requests and oversight are under Executive authority and the present system has been assessed as inadequate by different entities. **Justice AP Shah Committee** recognised these limitations as follows :

- Interception/access to data is addressed in two legislation, the Telegraph Act and the Information Technology Act, with varying standards and procedures for interception

through Rules, thus, creating similarities and differences in the Indian interception regimes. These differences have created an **unclear regulatory regime that is nontransparent, prone to misuse, and that does not provide remedy for aggrieved individuals.** The Committee recommended harmonization of the interception regime in India by suggesting that each legislation be in compliance with the National Privacy Principles.

- The Committee recognized the **absence of judicial oversight or authorization** and the resultant uncertainty as to which agency is legally authorized to undertake interception/access; lack of transparency in agencies regarding the effectiveness and cost of each intercept; absence of standardized orders, or additional safeguards against overreach of interceptions/access orders; and the lack of any notification to affected individuals.

It is therefore recommended that the data protection law should clearly establish the circumstances under which public authorities may issue demands for personal information and require judicial interventions and oversight for surveillance and lawful access to data. Companies should be permitted to report publicly on the number of demands that they receive for personal information on a periodic basis, in order to increase transparency and to inform public debate about the relevant laws. Also, the legal regime should enhance privacy safeguards based on sensitivity of the data being accessed/intercepted (e.g. content versus non-content data). While this will go a long way in safeguarding citizens' privacy, it would also help in enhancement in privacy standards to:

- achieve better interoperability for cross border data flows with other countries particularly the European Union (India has applied for adequacy status in the past but the same has been declined by the EU after negatively assessing the Indian legal framework)

- improve the chances of fructifying a India-US data sharing agreement in line with UK-US agreement which would improve sharing of data between US companies and Indian law enforcement agencies which in the present MLAT (Mutual Legal Assistance Treaty) arrangement is inefficient.

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?

BIF Response

There are three main reasons in support of the cross-border flow of information:

- a) Access to information is an international human right.
- b) Internet access and cross-border data flows comprise and enable international trade and are therefore subject to international trade laws and norms, the main ones being non-discrimination and transparency.
- c) All major international data protection instruments recognize the need to facilitate the free flow of data, including personal data.

Globalization and technology have made cross border data flows ubiquitous and an essential phenomenon for economic activity globally. The growth of the Internet and the ability to move data rapidly globally has been a key building block of the global economic order and this is relevant for companies that act as controllers and those who act on their behalf. Cross-border data flows have allowed business to communicate customer orders in real-time, make quick decisions about manufacturing loads and rapidly tweak designs in response to shifts in consumer desires. This has enabled the disaggregation by businesses of their supply chains across countries. In fact, there is no international data protection and privacy instrument that does not recognize the need to ensure that data can flow both domestically and internationally. Any disruption/hindrances to cross border data flows, introduced in the privacy law, would adversely impact innovation, economic competitiveness and availability of technology and services to users. Cloud Computing, for instance, is affordable for small businesses and startups because it relies on massive economies of scale with globally distributed datacenters. A 2014 ECIPE study had estimated that 'if 25 India were to introduce an economy-wide data localisation measure, the effect on GDP would be -0.8%. In addition, the domestic and foreign direct investments (FDI) that drive Indian exports and long-term growth, would drop by -1.9%. In terms of welfare loss, data localisation would cost the Indian worker almost 11 percent of one average month's salary.'

● Indian IT Industry and Cross border data flows Particularly for India, getting cross border data flows right is critical for growth of its Information Technology (IT)/outsourcing sector - India is the world's largest sourcing destination for the IT industry, accounting for approximately 67 per cent of the US$ 124-130 billion market. The industry employs about 10 million workforce. To increase market access for Indian IT companies in EU, the 26 Indian government as part of the India-EU Free Trade Agreement (FTA) negotiations has demanded that the EU relaxes the restrictions on movement of data of European citizens to India. Finally, India's flourishing global Information Technology Industry cannot be placed at a competitive disadvantage with others in the APAC region. A data transfer framework that prohibits data transfers except for very limited circumstances is bound to harm the domestic IT industry, who will not have the same level of choice of certain services due to those restrictions to foreign providers. In fact, India has the opportunity to look at international data transfers with fresh eyes, not restricted by very limiting legacy approaches that have proven to be insufficient to address the current demands and nature of the 21st century globalized economy and society.

Justice A P Shah Committee, recognised Technological Neutrality and Interoperability with International Standards as one of the five salient features, and recommended that any proposed framework for privacy legislation must be technologically neutral and interoperable with international standards. In particular, the Committee called for harmonization of the right to privacy with multiple international regimes, create trust and facilitate cooperation between national and international stakeholders and provide equal and adequate levels of protection to data processed inside India as well as outside it. Rather than focusing efforts around data localization provisions that are hard to implement and enforce, we believe that users are better served by providing a regulatory framework for international data transfers that sets adequate guarantees to users' data but does not restrict or prohibit the data flows from the outset. Below you will find some detailed observations pertaining to data flows that we believe should be considered when designing India's data transfer rules:

● **Cross regional instruments are preferred over unilateral adequacy models**

Homogeneous national privacy laws, is not practically possible nor desirable. National privacy laws need to respond to the specific legal and societal demands. But there are pragmatic arrangements like APEC Cross Border Privacy Rules (CBPRs) which are based on mutual recognition (unlike one way recognition systems like the EU adequacy model), accountability and commonly applicable privacy principles that enable efficient cross border data flows without unnecessary administrative burdens. The Indian government should consider becoming a member of such arrangements as this will help in enhancing market access for Indian companies especially the IT industry. APEC economies like the US, Canada, Mexico, Japan and Korea have started to using this mechanism. Requirements of APEC CBPRs should be considered in the development of the data protection law.

● **Contractual freedom should be preserved**

In B2B data flows across jurisdictions (e.g. Indian banking customer using cloud services for which data processing happens in the foreign jurisdiction), the data protection law should allow Indian businesses to use cloud services provided the privacy protections are applied in the contractual arrangement between the two parties. However, the government should not intervene between businesses by prescribing specific provisions or contract templates. This would tantamount to regulatory overreach and would undermine the ability and flexibility of organizations to ascertain risks and take decisions when procuring services from third parties.

● **Exceptions to free data flows should be applied restrictively**

If the government is planning to regulate the space, it should restrict data flows where necessary to achieve other legitimate policy goals or if it hinders national security of the country. Such restrictions should also be designed and applied in a non-discriminatory, least trade restrictive and transparent manner. Governments should consider developing norms of conduct amongst governments with respect to the Internet i.e governments should develop principles governing access to and use of the Internet. For example, the US and

Japan have agreed to Internet principles that emphasize the preservation of an open and interoperable Internet and a balanced approach to issues such as privacy and intellectual property rights so as not to impede the cross-border flow of information.

● **Forced data localization should be rejected** as it is incapable of achieving the objectives behind these measures, whether economic, security or access to data for law enforcement purposes.

● **Forced location of data centers** Requiring data centers to be located domestically undermines the cost-effectiveness of cloud-based computing services where so-called location independence is important. Eg: it will undermine and defeat the purpose of cross border financial transactions.

● **Forced localization for law enforcement and security reasons**

● **Law enforcement**: There is growing frustration among governments and law enforcement agencies when it comes to accessing data residing in foreign jurisdictions. The MLAT process is broken and needs to be reformed to enable efficient sharing of data between companies based out of foreign jurisdictions and Indian law enforcement agencies. The law enforcement requests for digital evidence should be based on the location and nationality of users, not the location of data. This is important to continue benefiting from the unfragmented Internet ecosystem. There are developments in the US to improve MLAT process and US and UK governments are also working on a new bilateral agreement that would create an efficient data sharing regime. While working on reforming the MLAT process, the Indian government should work with the US government to develop a UK-US type agreement. This would require legislative changes on both sides including enhancing privacy standards on the Indian side for legally accessing data. Indian think tank ORF recently published a study on India-US data sharing. The Indian government should consider the recommendations of this study.

● **Security:** Some believe that storing data in the local jurisdiction enhances security. This is a misconception as storing data across jurisdictions actually increases security and reliability and is helpful in business continuity during disasters. Storing data in one location (through data localization measures) makes data more vulnerable.

- Technical security expertise is expensive and rare. Companies have invested hundreds of millions of dollars ensuring that their data centers are secure. Attackers and criminals can more easily overwhelm a less sophisticated server or network.
- If there is a technical failure or natural disaster, when one data center goes down, another can take over, ensuring that service isn't interrupted.
- Local data storage is more vulnerable to attacks because they are generally harder to update with the latest security software.
- Forced data localization doesn't protect against foreign government surveillance. Storing data in one location could create a more attractive target.

- Cross-border data flows are a regular feature of the globalised data ecosystem.
- Forced data localization directly undermines the free and open structure of the internet. Instead of traveling by the most technically viable routes, data flows would be constrained by geopolitical considerations and regulations.
    - Such requirements would fragment the internet, reduce consumers' access to valuable information and communication tools, and discourage innovation.
    - Data localization requirements would have a severe impact on companies — especially Indian start-ups and small businesses — and internet users alike due to the technical difficulty and cost of compliance.
    - That's why a growing body of trade agreements and principles explicitly guarantee free cross-border data flows.
- There are more efficient ways to secure data access.
    - A principled international framework to ensure that the Indian government can access data from foreign, chiefly American, servers would obviate the need for data protection.
        - In 2016, India and the United States released a 'Framework for the U.S.-India Cyber Relationship' that contains a commitment to "sharing information on a real time or near real time basis, when practical and consistent with existing bilateral arrangements, about malicious cybersecurity threats, attacks and activities, and establishing appropriate mechanisms to improve such information sharing."[4]
    - Creating new bilateral and/or multilateral international agreements between governments that would allow foreign companies to respond directly (outside of the cumbersome MLAT process) to requests for content made by Indian law enforcement authorities is necessary.

.