BSA Submission
on
TRAI Consultation Paper on Privacy, Security and Ownership of the Data

October 30, 2017

Shri Arvind Kumar
Advisor (BB&PA)
Telecom Regulatory Authority of India
Mahanagar Door Sanchar Bhawan
Jawahar Lal Nehru Marg (Old Minto Road)
New Delhi – 110012

Dear Sir,

Subject: BSA Submission on TRAI Consultation Paper on Privacy, Security and Ownership of the Data in the Telecom Sector

This is with reference to the Telecommunications Regulatory Authority of India's (TRAI's) Consultation Paper on Privacy, Security and Ownership of the Data in the Telecom Sector issued on 9th August, 2017.

In this regard, please find enclosed the following:

- Submission from BSA | The Software Alliance ("BSA") on the Consultation Paper [Annexure I]
- BSA Personal Data Protection Principles [Annexure II]

We hope our submissions are useful to the consultation process and will merit your kind consideration. We look forward to participating in this important discussion, and stand ready to answer any questions you may have.

Thanking you,

Yours sincerely

Venkatesh Krishnamoorthy
Country Manager- India
BSA | The Software Alliance

Annexure I

BSA Submission
on
TRAI Consultation Paper on Privacy, Security and Ownership of Data

BSA I The Software Alliance (BSA)[1] thanks the Telecom Regulatory Authority of India (TRAI) for the opportunity to offer comments on the Consultation Paper on Privacy, Security and Ownership of the Data in the Telecom Sector (Consultation Paper) released on 9th August,2017.

As the leading advocate for the global software industry, BSA wishes to contribute to initiatives that seek to advance the protection of privacy and personal data. We commend the efforts of the TRAI to conduct this Consultation.

The comments below provide a brief introduction to the potential of the appropriate use of data to unleash economic growth and drive solutions to persistent societal challenges, introduce the BSA Personal Data Protection Principles, and then provide responses to many of the questions posed in the Consultation Paper.

Introduction

Software innovation continues to spark unprecedented advances that transform the world around us, empower us as individuals, and grow our economies. Yet the full potential of this digital transformation can only be realised if we tap the potential of the data these innovations have unleashed. We are, in fact, living through a data revolution – driven by the abundance and renewability of data as a resource, as well as by the fundamental technologies that change the way we gather, store, analyse and transform information. Almost everything we do generates data and entirely new streams of data are being created every day. In fact, 90 percent of the world's data today has been created in the last two years alone, and we are now doubling the rate data is produced every two years.[2]

Most of this data being generated is not personal data. This is an important distinction because, while it is imperative that we protect privacy, more often than not the data that is helping to improve our lives was generated by a sensor attached to a machine. Our challenge is to harness data and put it to work, using our ingenuity to make sense of the valuable learnings locked within it. From an economic perspective, making better use of data could lead to a 'data dividend' of $1.6 trillion in the next four years alone.[3] Economists estimate data-enabled efficiency gains could add almost $15 trillion to global GDP by 2030 – the equivalent of adding another U.S. economy.[4] A policy environment that enables businesses, consumers, and governments to leverage the full potential of data and data transfers is the key to driving the digital economy. We observe that countries with clear accountability

[1] BSA | The Software Alliance (www.bsa.org) is the leading advocate for the global software industry before governments and in the international marketplace. Its members are among the world's most innovative companies, creating software solutions that spark the economy and improve modern life. With headquarters in Washington, DC, and operations in more than 60 countries, BSA pioneers compliance programs that promote legal software use and advocates for public policies that foster technology innovation and drive growth in the digital economy.

BSA's members include: Adobe, Amazon Web Services, ANSYS, Apple, Autodesk, AVEVA, Bentley Systems, CA Technologies, Cisco, CNC/Mastercam, DataStax, DocuSign, IBM, Intel, Microsoft, Oracle, salesforce.com, SAS Institute, Siemens PLM Software, Splunk, Symantec, The MathWorks, Trend Micro, Trimble Solutions Corporation, and Workday.

[2] BSA 'What's the Big Deal with Data" report at http://data.bsa.org/wp-content/uploads/2015/12/bsadatastudy_en.pdf

[3] "The Return on the Data Asset in the Era of Big Data: Capturing the $1.6 Trillion Data Dividend." Cloud Platform News Bytes Blog 2015. Web. http://blogs.technet.com/b/stbnewsbytes/archive/2014/04/15/the-return-on-the-data-asset-in-the-era-of-big-datacapturing-the-1-6-trillion-data-dividend.aspx

[4] Evans, Peter C., and Marco Annunziata. Pushing the Boundaries of Minds and Machines. GE, 2012. Web. http://files.gereports.com/wp-content/uploads/2012/11/ge-industrial-internet-vision-paper.pdf

frameworks, effective privacy principles, and unrestricted cross-border data flows are best placed to tap into this potential. We also find that many countries recognise that coordination of national data protection laws and frameworks, both internally and with those of other nations, will facilitate benefits for all countries participating in the global economy.

As Page 18 of the Consultation Paper highlights, India is yet to formulate a comprehensive privacy and data protection law. In such a case, it is important for the Government of India to keep any data protection framework for India in line with emerging international trends and practices. Following an overly-regulated approach to many of the issues highlighted in the Consultation Paper is likely to inhibit the capacity of Indian businesses and other entities to tap into the business and efficiency potential of data analytics and innovation.

This potential is not restricted to the IT sector - data analytics and innovation can benefit almost all sectors of the economy. Companies that already use data-directed decision-making report a 5 percent to 6 percent boost in productivity.[5] Further, data innovation is also a powerful new job creation engine – 61 percent of senior executives in the US and 58 percent in Europe say data analytics is important to their companies' hiring plans.[6] For every data-related IT job created, another three jobs are estimated to be created for people outside of IT – creating millions of more jobs throughout the economy.[7]

Keeping the above in mind, as the Government of India develops a data protection framework for India, it is paramount that TRAI and other agencies of the Government of India work together and adopt clear and predictable stances on various issues relating to data protection and a data-centric economy. As TRAI has done with this Consultation Paper, it is also critical that the Government of India continue to seek the input of interested and relevant private sector stakeholders to inform policy making in this area.

This will allow investors to plan and execute long term strategies and investments in the Indian market. It will also help ensure that India is positioned to become a global leader in developing an effective, trusted, transparent and restrained regulatory environment that works well with emerging international practices, and allows Indian businesses and consumers to fully benefit from the opportunities presented by the data revolution.

Such opportunities have already begun to materialise for Indian citizens, tying data innovation into tangible improvements to their daily lives. Internet kiosks in India are giving more than 4 million farmers access to crop price, weather, and other information in local languages.[8] This is but one example where enabling policies have benefited legacy industries — and any measures that restrict this transformative ability of data can result in the Indian economy losing out on this potential it offers.

BSA Personal Data Protection Principles

As a global organization, BSA actively follows privacy developments around the world. Our member companies are at the forefront of data-driven innovation, and have a deep and long-standing commitment to protecting consumers' personal data across technologies and business models.

As part of its efforts to advance effective privacy regimes internationally, BSA has developed BSA Personal Data Protection Principles (Principles). These Principles rest on five Pillars of Personal Data Protection – (1) Scope and Definition of 'Personal Data'; (2) Collection, Use, Processing and Disclosure of Personal Data; (3) Allocation of Obligations and Liability; (4) International Data Transfers; and (5) Personal Data Breach Notifications. The BSA Personal Data Protection Principles are attached to this submission as Annexure II.

[5] Economist Intelligence Unit. The Deciding Factor: Big Data & Decision Making. Cap Gemini, 2012. Web. Point Of View. http://bigdata.pervasive.com/Solutions/Telecom-Analytics.aspx
[6] BSA/IPSOS Global Data Analytics Poll, November 2014 at www.bsa.org/datasurvey
[7] Gartner, "Gartner Says Big Data Creates Big Jobs: 4.4 Million IT Jobs Globally To Support Big Data By 2015." 2012. Print. http://www.gartner.com/newsroom/id/2207915
[8] "Supply Chain Management Solution for Fast Moving Consumer Goods & Food Industries - Farm to Fork Tech Mahindra." *Tech Mahindra*. 2015. Web at http://www.techmahindra.com/en-US/wwd/solutions/Pages/Enterprises/retail_farm_fork.aspx

Data is now emerging as one of the most revolutionary forces for economic gains. We hope these Principles will assist governments worldwide in the development and implementation of effective data protection policies and privacy rules that protect consumers' personal data and also shape the growth of an emerging data-centric economy.

BSA and its members have extensive experience working with governments and other stakeholders around the world on policies that promote the protection of data. We share our views to the Consultation Paper, as well as our Personal Data Protection Principles with the hope of assisting TRAI in its efforts to map out the policies necessary to promote the security and privacy of data protection in the telecommunications sector specifically, and for India's digital economy in general.

BSA's Response to Questions in the Consultation Paper

Because BSA is an industry association representing many of the leading global software companies, we have attempted to focus our responses on those questions that have implications for the entire digital ecosystem in India and are amenable to industry wide input. We have chosen not to answer all of the questions in the Consultation, especially where we felt questions were specific to individual company practices or experiences and not suitable to an industry wide response, or where such questions were relating to issues outside the practices and experiences of our member companies.

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?

Personal Data

The definition of 'Personal Data' should be limited to data that is reasonably linked to an identified or identifiable natural person

As any government seeks to protect individuals' personal data, it should also ensure that the scope of information included within the definition of personal data is information that, if mishandled, would have a meaningful impact on an individual's privacy.

If the scope is not limited, and stringent legal obligations apply to a broad range of data regardless of its context and the risk of harm to users, the law is likely to have a chilling effect on data-driven innovation, negatively impacting economic growth.

For instance, internet protocol (IP) addresses are widely used for e-commerce. If IP addresses were regarded as "personal data," it would significantly increase compliance costs — raising prices for consumers even in situations in which there is no privacy benefit. Defining IP addresses, without more, as personal data would also negatively impact the effectiveness of cybersecurity defense measures and investigations.

Similarly, anonymized data, which is not linkable to a specific individual and, therefore, does not implicate individual privacy interests, should be excluded from data protection regulations.

Consent

The standard for obtaining consent should be contextual

Consent is an important basis for collecting, using, processing, and disclosing (collectively, 'handling') personal data. However, there must be other legal bases for handling personal data, including for the legitimate interest of companies handling the data where obtaining consent may not be suitable or

practicable, the performance on contracts with the data subject, and compliance with legal obligations, among other things.

According to international best practices, when consent is used as the legal basis for handling personal data, context is important to determining the level of consent that is appropriate.

In circumstances that do not implicate heightened sensitivity, implied consent may be appropriate, as may one of the other bases for handling personal data discussed below. In today's world, a large amount of data is created through individuals' interactions with Internet-connected devices, and express consent is not suitable or practical in all instances. For example, the future of public transportation services may be impacted if an individual must provide express consent to allow an electronic gate to generate data every time he or she uses a public transportation card. In other circumstances, such as the handling of sensitive health or financial data, affirmative express consent may be appropriate. Any system for protecting personal information should consider this context and allow sufficient flexibility for determining the timing, standard, and mechanism for obtaining consent. Where consent is appropriate, there are a range of tools that could be considered to help individuals express their preferences.

However, relying solely on explicit or express written consent as a legal basis for handling data would create two risks: (1) stymying growth and innovation in the digital economy; and (2) not meeting individual privacy expectations by leading to 'click fatigue', where users simply accept whatever terms are presented to them without fully reviewing or understanding the information presented to them.

In addition to consent as a legal basis for handling data, it is important to ensure that a personal data protection system also recognizes other legal bases such as legitimate interest, contractual performance and compliance with legal obligations further elaborated below.

Legitimate interest

The legitimate interest legal basis for handling personal data would create the flexibility that companies need to carry out their business operations. For example, businesses may need to handle personal data as part of network security or fraud prevention efforts.

The legitimate interest legal basis also serves a particularly important role where it may not be suitable or practicable to obtain consent, or where it is premature to enter into a contract with the data subject. For example, if a telecom operator seeks to use call records to identify fraudulent accounts, it may not be suitable to request the data subject's consent to do so, but there is a legitimate interest that would justify the handling of the personal data.

As long as the data subject's fundamental rights and freedoms are respected, legitimate interest should be accepted as a valid basis for handling personal data.

Contractual performance

Similarly, companies should be able to handle personal data to perform contracts with the data subject. For example, a company may need to handle personal data to fulfill a product shipment ordered by an individual, or to open accounts at the request of the data subject. This should be permitted without the need for the data subject to expressly consent to the use of the data for this purpose.

Compliance with legal obligations

Companies should also be able to handle data to comply with legal obligations. Businesses are subject to a wide range of legal obligations, including financial reporting rules, other regulatory requirements, and obligations arising from court proceedings. In some instances, companies must handle personal data to satisfy these legal obligations. Any privacy framework should ensure that companies can continue to comply with these requirements.

Other bases

In addition to the foregoing examples, there are several other potential circumstances that could serve as valid legal bases for handling data. We recommend a flexible approach to personal data protection that both protects individuals' privacy and preserves companies' ability to carry out their legitimate business operations and provide innovative services.

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.

Responsibilities of Data Controllers and Data Processor should be clearly defined

The primary obligation for ensuring compliance with the applicable data protection requirements should fall on the data controller. The data processor's role is to comply with the instructions of the data controller, which assists the controller in meeting its own compliance obligations, and to ensure the security of the data they process. The relationship between the data processor and data controller should be governed by contractual relationships they have formed.

The clear allocation of responsibility and liability is critical and ensures that the increasingly widespread practice of outsourcing does not create uncertainty. This allocation allows the data subject and the legal authorities to know who to turn to in case of a problem, and companies to have clarity on their roles and responsibilities.

Imposing direct, joint, or several liabilities or other obligations on data processors would have a range of unintended consequences, would undermine the relationship between the relevant actors, and would create an unjustified compliance burden on data processors who have no direct visibility or knowledge of the data subjects. In addition, this could also have a negative impact on potential investments in data processing and outsourcing services.

In short, data controllers should have the primary obligation for ensuring compliance with applicable privacy rules, while data processors should only be required through contractual mechanisms to comply with data controller instructions and to ensure the security of the data they process.

Accountability frameworks may be used to allocate responsibility

The accountability model, first established by the Organisation for Economic Cooperation and Development (OECD)[9] and subsequently endorsed and integrated in many legal systems and privacy principles, provides an approach to cross-border data governance that effectively protects the individual and fosters streamlined, robust data flows. Other frameworks, such as the Asia-Pacific Economic Cooperation (APEC) Cross Border Privacy Rules (CBPR)[10] system are also useful models for India to reference in developing its own data privacy regime.

The accountability model requires organizations that collect personal data to be responsible for its protection, no matter where or by whom it is processed. As such, any organizations transferring data to a third party must take steps to ensure that any applicable obligations — in law, guidance, or commitments made in privacy policies — will be met.

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

[9] In the *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (available at: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm)

[10] The APEC CBPR system is available at: https://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/CBPR/CBPR-PoliciesRulesGuidelines.ashx

take on these responsibilities?

It is not feasible to expect an auditing system to keep pace with rapidly evolving technology. Instead, industry should be encouraged to use available standards and data verification tools.

BSA members already provide broad process-based data governance and technical controls to ensure that they are handling and using data appropriately, including in compliance with consent when that is the basis for handling data.

Rather than attempting to create a new, India-specific auditing technology architecture, we recommend TRAI promote the development and adoption of voluntary, transparently developed, industry-led international standards, and recognize certifications from internationally accredited entities.

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?

Data innovation empowers consumers to make better decisions and enables merchants to customize goods and services to serve individuals, businesses, and society better. Data innovation is not just about boosting economic growth. It is also about fuelling a **powerful new job creation engine**. An effective framework for personal data protection aims to protect consumers without hampering innovation and leverages the power of the digital economy to support governments and business alike.

Large and small businesses are learning to deploy cloud computing services to compete globally. They leverage data analytics to create new products and services to serve customers in the international market. This can only be possible if the policy environment **facilitates seamless transfer of data across international borders**.

Emerging areas like artificial intelligence (AI) have the potential to improve decision-making and outcomes across a broad range of sectors, including healthcare, manufacturing, education, finance, consumer services, and others. To avoid inadvertently stifling these benefits, policymakers and regulators should be open to taking a **fact-based and incremental approach to regulation** to realize the impact data-based businesses on the economy.

For consumers to consistently use new data-based businesses, providers of data services must be permitted to use the best available technology to thwart attacks against that data or the entities and individuals who depend on those services. The increasing **widespread use of strong encryption** will improve consumer trust and help keep data secure and protected.

Q.6 Should government or its authorized authority setup a data sandbox, which allows the regulated companies to create anony
mized data sets which can be used for the development of newer services?

It is unclear whether there would be any benefit from the government or its authorized authority establishing a “data sandbox” to create anonymized data. It would certainly be problematic if the government required companies to provide data sets to such a sandbox, and the TRAI should not propose any mandates to do so.

On the other hand, it is important to allow companies to create and share anonymized or pseudonymized data. With the increasing availability of data analytics to identify new patterns and trends, it is valuable from a commercial and societal point of view to ensure that appropriately de-identified data may be used. The government can encourage data anonymization by ensuring that anonymized data is not considered personal information.

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?

Establishing a government developed technology solution for monitoring is likely to be ineffective. It is difficult to imagine how such a solution would keep pace with technological developments in the market. Rather than attempting to develop a centralized technology for monitoring and compliance, the government should instead incentivize the adoption and use of technologies and methods for protecting personal information as part of a risk-based accountability approach to personal data protection.

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?

Cybersecurity

Cybersecurity policies should be risk-based, adaptable, and aligned with international standards

The government may consider policy frameworks for defining cybersecurity standards for critical telecommunications infrastructure, including critical software and hardware components. Establishing clear, meaningful security standards may improve the operational resilience of India's telecommunications infrastructure and mitigate the risk of systemic failure. However, BSA urges the government to approach such standards with great caution, as overly-prescriptive standards that create unsustainable compliance burdens or that undermine international interoperability will be counterproductive and ineffective.

Cybersecurity policies and standards should be risk-based and scale recommended security measures in proportion to demonstrable risk. They should be adaptable and outcome-oriented, enabling covered entities to adopt the technological solutions that are best suited to their organization's needs and risk profile. And they should be developed in close collaboration with industry stakeholders they are most likely to impact.

Finally, it is critical that any cybersecurity policies or standards be aligned with relevant international standards. International cybersecurity standards are developed through inclusive, objective, transparent processes that enable stakeholders to address wide-ranging security concerns. These standards enable security professionals to establish common security requirements and performance metrics, enabling collaboration to confront shared threats. Moreover, by supporting economies of scale, international standardization improves efficiency and lowers development costs for technology products, enabling innovation and investment in the next generation of security technologies.

The 'Framework for Improving Critical Infrastructure Cybersecurity', developed by the United States National Institute for Standards and Technology,[11] represents an exemplar of industry-driven, risk-based, adaptable cybersecurity standards. Notably, the Framework is voluntary and tailorable to the risk profile of any operator across a wide variety of sectors and vulnerabilities. It is also aligned with international standards, making it a viable framework for nations beyond the United States. It stands as an international best practice in the development of cybersecurity risk management policy frameworks.

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

[11] The NIST Framework is available at https://www.nist.gov/sites/default/files/documents////draft-cybersecurity-framework-v1.11.pdf

to be put in place in order to address these issues?

Companies across the digital ecosystem, including leading software companies, use new technologies to provide innovative services to consumers and businesses alike. In some instances, those services require the use of personal data to function effectively. BSA encourages the TRAI to recognize these benefits and to adopt privacy principles that both provide appropriate safeguards and are sufficiently flexible to facilitate continued innovation and growth in an increasingly data-driven economy.

As governments and stakeholders seek to address this issue, they should consider the immense benefits that software-enabled data services provide so that any potential solutions do not unnecessarily impede this innovation. Software companies, including BSA members, provide services that spur economic growth across virtually all sectors of the global economy, transform business operations, and contribute to broader societal gains. Indeed, businesses are increasingly using software and cloud-enabled platforms to, among other things, improve global human resource management functions, detect financial fraud, optimize manufacturing operations, and enhance transportation services. Data-driven innovation is also advancing public health and safety. For example, AI technologies are transforming the lives of people with disabilities, including helping people with vision-related impairments interpret and understand photos and other visual content, and even to navigate their physical surroundings.[12] AI technologies are also helping doctors improve the diagnosis and treatment of cancer patients.[13]

Notably, these data-driven services often rely on the ability to move and access data around the globe. For example, companies use cloud-based storage across multiple geographic locations to protect against a wide range of risks, such as cybersecurity threats or natural disasters, by providing redundancy and eliminating single points of failure.

In light of the need to ensure the free flow of data so that data-driven services continue to operate seamlessly globally, it is imperative that privacy frameworks do not stymie innovation or impose burdensome restrictions on global data transfers. Instead, stakeholders should consider flexible, pragmatic approaches to achieve the dual goals of protecting privacy and spurring innovation. As discussed above, such approaches include recognizing a variety of legal bases for processing personal data, developing a contextual approach to the role of individual consent, and implementing an accountability-based model for global data transfers.

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?

Government requests for data should respect due process and international comity

BSA and its members share the priority that the Government of India places on ensuring that law enforcement, intelligence, and security authorities (LEAs) have the tools necessary to prevent attacks and prosecute criminals. Our members cooperate extensively — indeed, daily — with LEAs around the world to combat criminal activity, terrorism, and other security risks. However, LEA access to data also implicates international law, individual privacy, and free expression — and a comprehensive framework that reflects all of these values is needed.

Such a framework should ensure that orders compelling the disclosure of communications content are issued by a neutral judicial authority, based on a finding of probable cause. Moreover, when the

[12] For instance, Microsoft recently released an intelligent camera app that uses a smartphone's built-in camera functionality to describe to low-vision individuals the objects that are around them. *See* Microsoft, *Seeing AI*, *at* https://www.microsoft.com/en-us/seeing-ai/.

[13] IBM, *Watson for Oncology*, https://www.ibm.com/watson/health/oncology-and-genomics/oncology/; *see also* Jo Cavollo, The ASCO Post (June 25, 2017), at http://www.ascopost.com/issues/june-25-2017/how-watson-for-oncology-is-advancing-personalized-patient-care/.

government seeks access to information stored in the cloud, such orders should, whenever possible, be served directly on the data controller. In exceptional circumstances where disclosure orders must be served on a data processor (e.g., cloud provider), the framework should respect fundamental principles of international comity. To that end, when an LEA seeks access to data stored on overseas servers, deference is owed to the legal regime where the data resides and data processors should not be penalized for declining to comply with a disclosure order when doing so would violate the laws of the country in which the data resides.

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?

Accountability frameworks may be used to allocate responsibility

The accountability model, first established by the OECD[14] and subsequently endorsed and integrated in many legal systems and privacy principles, provides an approach to cross-border data governance that effectively protects the individual and fosters streamlined, robust data flows. Other frameworks such as the APEC CBPR[15] system are also useful models for India to reference in developing its own data privacy regime.

The accountability model requires organizations that collect data to be responsible for its protection, no matter where or by whom it is processed. As such, any organizations transferring data to a third party must take steps to ensure that any obligations — in law, guidance, or commitments made in privacy policies — will be met.

International Data Transfers

Policies should ensure the free flow of data across borders and avoid requirements that impose unnecessary or burdensome restrictions on global data transfers

The seamless transfer of data across international borders is critical to cloud computing, data analytics, and other modern and emerging technologies and services. An effective personal data protection law should ensure that global data transfers continue. Further, as part of ensuring the free flow of data, the law should prohibit data localization requirements for both the public and private sectors, which can frustrate efforts to implement security measures, impede business innovation, and limit services available to consumers.

[14] In the *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,* available at: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

[15] The APEC CBPR system is available at: https://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/CBPR/CBPR-PoliciesRulesGuidelines.ashx.

Annexure II

BSA Personal Data Protection Principles

BSA |The Software Alliance (BSA)[16] is the leading advocate for the global software industry before governments and in the international marketplace. Our member companies are at the forefront of data-driven innovation. BSA members have a deep and long-standing commitment to protecting consumers' personal data across technologies and business models. We recognize the importance of fostering trust and confidence in the online environment. As a global organization, BSA actively follows privacy developments around the world. An effective privacy regime protects consumers without hampering innovation and leverages the power of the digital economy to support governments and businesses alike.

BSA provides these Personal Data Protection Principles to advance the development of effective privacy and personal data protection regimes internationally. The Personal Data Protection Principles rest on five Pillars of Personal Data Protection.

PILLARS OF PERSONAL DATA PROTECTION

1. Scope and Definition of 'Personal Data'
2. Collection, Use, Processing, and Disclosure of Personal Data
3. Allocation of Obligations and Liability
4. International Data Transfers
5. Personal Data Breach Notifications

PRINCIPLES

1. SCOPE AND DEFINITION OF PERSONAL DATA

PRINCIPLE: **Definition of 'Personal Data' should be reasonably linked to an identified or identifiable natural person.**

RATIONALE: As any government seeks to protect individuals' personal data, it should also ensure that the scope of information included within the definition of personal data is information that, if mishandled, would have a meaningful impact on an individual's privacy.

If the scope is not limited, and stringent legal obligations apply to a broad range of data regardless of its context and the risk of harm to users, the law is likely to have a chilling effect on data-driven innovation, negatively impacting economic growth.

For instance, internet protocol (IP) addresses are widely used for e-commerce. If IP addresses were regarded as personal data, it would significantly increase compliance costs — raising prices for consumers even in situations in which there is no privacy benefit.

Similarly, any proposed legislation should also recognize that anonymized data, which is not linkable to a specific individual and, therefore, does not implicate privacy concerns, should be excluded from the definition of personal data.

[16] BSA | The Software Alliance (www.bsa.org) is the leading advocate for the global software industry before governments and in the international marketplace. Its members are among the world's most innovative companies, creating software solutions that spark the economy and improve modern life. With headquarters in Washington, DC, and operations in more than 60 countries, BSA pioneers compliance programs that promote legal software use and advocates for public policies that foster technology innovation and drive growth in the digital economy.

BSA's members include: Adobe, Amazon Web Services, ANSYS, Apple, Autodesk, AVEVA, Bentley Systems, CA Technologies, Cisco, CNC/Mastercam, DataStax, DocuSign, IBM, Intel, Microsoft, Oracle, salesforce.com, SAS Institute, Siemens PLM Software, Splunk, Symantec, The MathWorks, Trend Micro, Trimble Solutions Corporation, and Workday.

2. COLLECTION, USE, PROCESSING, AND DISCLOSURE OF PERSONAL DATA

PRINCIPLE: **The legal bases for collecting, using, processing, and disclosing (collectively, 'handling') personal data should be sufficiently flexible so that they both ensure appropriate safeguards for personal data and allow businesses to continue to provide innovative services and stimulate economic growth.**

RATIONALE: The legal framework for personal data protection should provide protections that meet, and are appropriate to, consumer expectations, without unnecessarily stifling economic growth through the data economy. According to international best practices, the legal bases for handling personal data could include, among other things, the legitimate interest of the data controller or third party, the consent of the data subject, compliance with legal obligations, and performance of a contract with the data subject.

Legitimate interest

The legitimate interest legal basis for handling personal data would create the flexibility that companies need to carry out their business operations. For example, businesses may need to handle personal data as part of network security or fraud prevention efforts.

The legitimate interest legal basis also serves a particularly important role where it may not be suitable or practicable to obtain consent, or where it is premature to enter into a contract with the data subject. For example, if a financial institution is seeking to recover an outstanding debt and needs to collect, use, process, and/or disclose personal data as part of the debt-collection process (e.g., to debt-collecting agencies), it may not be suitable to request the data subject's consent to do so, but there is a legitimate interest that would justify the handling of the personal data.

As long as the data subject's fundamental rights and freedoms are respected, legitimate interest should be accepted as a valid basis for handling personal data.

Consent

Consent is another important basis for handling personal data. The standard for obtaining consent should be contextual to determining the level of consent that is appropriate.

In circumstances that do not implicate heightened sensitivity, implied consent may be appropriate. In today's world, a large amount of data is created through individuals' interactions with Internet-connected devices, and express consent is not suitable or practical in all instances. For example, the future of public transportation services may be impacted if an individual must provide express consent to allow an electronic gate to generate data every time he or she swipes a public transportation card. In other circumstances, such as the handling of sensitive health or financial data, affirmative express consent may be appropriate. Any proposed legislation should consider this context and allow sufficient flexibility for determining the timing, standard, and mechanism for obtaining consent.

Relying solely on explicit written consent as a legal basis for handling personal data would create two risks: (1) stymying growth and innovation in the digital economy; and (2) not meeting consumer privacy expectations by leading consumers to "click fatigue", where users simply accept whatever terms are presented to them without fully reviewing or understanding the information presented to them.

Compliance with legal obligations

Companies should also be able to handle personal data to comply with legal obligations. Businesses are subject to a wide range of legal obligations, including financial reporting rules, other regulatory requirements, and obligations arising from court proceedings. In some instances, companies must handle personal data to satisfy these legal obligations. Any privacy framework should ensure that companies can continue to comply with these requirements.

Contractual performance

Similarly, companies should be able to handle personal data to perform contracts with the data subject. For example, a company may need to handle personal data to fulfill a product shipment ordered by an individual, or to open accounts at the request of the data subject.

Other bases

In addition to the foregoing examples, there are several other potential circumstances that could serve as valid legal bases for handling personal data. We recommend that governments adopt a flexible approach that both protects individuals' privacy and preserves companies' ability to carry out their legitimate business operations and provide innovative services to consumers.

3. ALLOCATION OF OBLIGATIONS AND LIABILITY

***PRINCIPLE:* Responsibilities of Data Controllers and Data Processors should be clearly defined.**

RATIONALE: The primary obligation for ensuring compliance with the applicable personal data protection law should fall on the "data controller." The "data processor" should only be concerned about complying with the instructions of the data controller, and to ensure the security of the data they process. The relationship between the data processor and data controller should be governed by contractual relationships they have formed.

This clear allocation of responsibility and liability is critical and ensures that the increasingly widespread practice of outsourcing does not insert confusion in the system. This allocation allows the data subject and the legal authorities to know who to turn to in case of a problem, and companies to have clarity on their roles and responsibilities.

Imposing direct, joint, or several liabilities or other obligations on data processors would have a range of unintended consequences, would undermine the relationship between these actors, and would create an unjustified compliance burden. In addition, this could also have a negative impact on potential investments in data processing and outsourcing services.

In short, data controllers should have the primary obligation for ensuring compliance with applicable privacy law, while data processors should only be required through contractual mechanisms to comply with data controller instructions and to ensure the security of the data they process.

4. INTERNATIONAL DATA TRANSFERS

***PRINCIPLE:* The law should ensure the free flow of data across borders and avoid requirements that impose unnecessary or burdensome restrictions on global data transfers.**

RATIONALE: The seamless transfer of data across international borders is critical to cloud computing, data analytics, and other modern and emerging technologies and services. An effective personal data protection law should ensure that global data transfers continue.

The accountability model, first established by the OECD[17] and subsequently endorsed and integrated in many legal systems and privacy principles, provides an approach to cross-border data governance that effectively protects the individual and fosters streamlined, robust data flows.

The accountability model requires organizations that collect personal data to be responsible for its protection, no matter where or by whom it is processed. As such, any organizations

[17] In the *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (available at: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm)

transferring personal data must take steps to ensure that any obligations — in law, guidance, or commitments made in privacy policies — will be met.

International data transfers are often made with commitments assumed in international cooperation agreements — including international industry codes of conduct or frameworks developed through open, multi-stakeholder processes — which provide additional assurances to consumers.

Further, as part of ensuring the free flow of data, the law should prohibit data localization requirements for both the public and private sectors, which can frustrate efforts to implement security measures, impede business innovation, and limit services available to consumers.

5. PERSONAL DATA BREACH NOTIFICATIONS

PRINCIPLE: **Personal data breach notification requirements should be reasonable and appropriate and cover only situations where there is a material risk of harm to affected individuals.**

RATIONALE: The creation of a personal data breach notification system applicable to all businesses and organizations would provide incentives to ensure robust protection for personal data, while enabling data subjects to take action to protect themselves in the event their data is compromised.

However, in creating such a system, it must be recognized that not all personal data breaches represent equal threats. In many instances, the breaches pose no actual risks to the individuals whose personal data was affected.

The notification requirements in the event of a personal data breach should therefore be carefully crafted to prevent the issuance of immaterial notices, principally by ensuring that notification is only required where there is a material risk of identity theft or economic loss to the user. Furthermore, it should also exclude from the notification obligation all instances where the personal data in question has been rendered unusable, unreadable or indecipherable to an unauthorized third party through any practice or method that is widely accepted as effective industry practices or industry standards (e.g., encryption).

To ensure that data subjects receive meaningful notifications in the event of a personal data breach, it is also critical that data controllers and data processors are afforded adequate time to perform a thorough investigation to determine the scope and impact of the breach and prevent further disclosures. We recommend using a standard that is flexible such as “as soon as practicable” or “without undue delay” instead of specifying an arbitrary, fixed deadline for providing notification.

# # # # #

Data is now emerging as one of the most revolutionary forces for economic gains. We hope these Principles will assist governments worldwide in the development and implementation of effective personal data protection policies and privacy rules that protect consumers’ personal data and also shape the growth of an emerging data-centric economy.