ASSOCHAM INDIA

Privacy in the data economy

pwc

www.pwc.in

Contents

सत्यमेव जयते

अजय साहनी, आई.ए.एस.
AJAY SAWHNEY, I.A.S.

सचिव
इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय
भारत सरकार
Secretary
Ministry of Electronics &
Information Technology (MeitY)
Government of India

MESSAGE

I congratulate ASSOCHAM for organising 2nd Global Summit on the theme- **"Data Protection, Privacy & Security in the world of Digital Economy"** - Reforms, Challenges & Opportunities.

India is focused on promotion of digital economy and has already launched an ambitious initiative of Digital India. In today's world of Digital Economy, data is one of the most important assets. Thus protection of data is of paramount importance. A fine balance needs to be struck between an individual's right to privacy and the legitimate business requirements of any entity.

Increased and voluminous digitalization poses added challenges with regard to data security, privacy and data protection. India, as the world's largest democracy has to harness the opportunities of the emerging digital landscape but at the same time ensure that the rights of the citizens are protected.

Recognizing the importance of data protection and privacy and strengthening security and protection of personal data of citizens, Government of India has set up a Committee of Experts under the Chairmanship of Justice (Retd.), Shri B N Srikrishna for data protection framework in India.

I sincerely hope that this event will discuss different facets of this exciting topic and come up with recommendations that will lead to enhanced security and safety of personal data of citizens and a healthier growth of digital economy.

I wish the Summit great success.

(Ajay Sawhney)

Place: New Delhi
Dated: 16th July, 2018

इलेक्ट्रॉनिक्स निकेतन, 6, सी.जी.ओ. कॉम्पलेक्स, नई दिल्ली–110003 / Electronics Niketan,6, C.G.O. Complex, New Delhi-110003
Tel. : 011-24364041 • Fax : 24363134 • email : secretary@meity.gov.in

ASSOCHAM
INDIA

THE ASSOCIATED CHAMBERS OF COMMERCE AND INDUSTRY OF INDIA

D S RAWAT

Secretary General

Message

Greetings from ASSOCHAM!

In the digital data-driven economies, an unprecedented amount of personal and financial data lies in control of two powerful entities i.e. sovereign governments and private sector players. The data in itself is not lesser than a personal asset for an individual or organization, but when it interplays freely between cross-sections and different verticals of businesses, it is exposed to high risks of privacy.

Given that nations under European Union have already got GDPR implemented and through which they have largely protected their respective data like any other protection of assets. Any unauthorized & unlawful processing of personal data or violation to the regulations under GDPR is subject to serious penalties and consequences. In this backdrop, India should have comprehensive protection of data, which is presently at high risk in the absence of regulations under laws of the land.

In an effort to contribute to a strong draft regulation for data protection and privacy in India, the ASSOCHAM has submitted the draft policy papers to the government and regulators which were mostly based on discussions and recommendations as outcomes of the 1st Global Summit that was organized in May 2018. As one advance step forward towards strong data protection regulation in India the chamber is organizing 2nd Global Summit on **"Data Protection, Privacy & Security in the world of Digital Economy- Reforms, Challenges & Opportunities"** on Friday, 27th July, 2018 in Bangalore, India. The summit is expected to bring out more clarity on what is essential, what is desirable and what should not be avoided in the inputs under regulation for data protection, privacy & security.

I wish to acknowledge the joint contribution made by the expert team of PwC India and ASSOCHAM, Dept. of Fintech, Digital Assets & Blockchain Technology and Competition Law for bringing out the knowledge report as well as for organizing the summit of utmost significance.

I am sure the study will provide rich insights and adequate knowledge to all the stakeholders on the subject.

I wish the participants and the stakeholders of the summit a great success.

With best wishes,

(D. S. Rawat)

July, 2018
New Delhi

ASSOCHAM Corporate Office : 5, Sardar Patel Marg, Chanakyapuri, New Delhi-110021
Tel. : +91-11-46550555 (Hunting line) • Fax : +91-11-23017008 / 9 • E-mail : assocham@nic.in • Website : www.assocham.org

Foreword

Sivarama Krishnan
Leader, Cyber Security
PwC India

Against the backdrop of an increasingly connected and data-hungry world, we are looking at a paradigm shift in how integrated and intertwined we are becoming with each other.

With the increase in perceived value of personal data, the rise in the use of data for profit and advent of technologies such as big data analytics and artificial intelligence, there is a compelling need for governments around the world to come up with regulations for preventing the misuse of personal information. Governments, at the same time, are faced with the challenge of ensuring that the cost of privacy and protection of personal data are not onerous for enterprises.

We are noticing that even developed economies around the globe, with already mature data privacy and protection laws, are undergoing revisions to address the challenges and threats of the twenty-first century. It is of paramount importance that jurisdictions with weak or no privacy regulations address these concerns promptly.

Most of the privacy laws and regulations are focused on individual rights, data protection, breach identification and notification, and enforcement and consequence management.

As the new data privacy and protection regime plays out, timely planning/action will help organisations continue their business as usual and, more importantly, enhance business reputation.

1 Rise of the data economy

Businesses have always been collecting and managing information about customers, clients and prospects. Businesses have been capturing, storing, analysing and reacting to data right from inception. Customer data has always been strategic in nature and research has shown that organisations that leverage customer behaviour insights outperform their competitors. With the advent of the digital imperatives and Internet penetration, customers are generating a plethora of data. As technologies like the Internet of things (IOT) and artificial intelligence continue to develop, companies have begun capturing and analysing more and more data.

The growth of Internet and mobile data

India has seen exponential growth in the mobile market, both in terms of mobile-cellular and mobile-broadband subscriptions. Internet access and smartphone use are growing rapidly and the cost of data communication is also declining. India has witnessed a surge in mobile data consumption, mainly with the introduction of competitive data plans introduced by telecom service providers. India is poised to take advantage of this enormous efficiency potential that has been unlocked with the use of affordable information and communication technologies (ICT).

E-wallets: The new purse

Digital payments have also surged in India, and a key trend was the emergence of mobile as the preferred means of payments and consumption over the Internet. E-wallet companies, various apps, online shopping, banking and travel sites complete the ecosystem. This trend is attributed to the increase in the use of smartphones and decrease in data prices, supported by the Aadhaar and demonetisation exercises.

Doing business digitally

Digital technologies have profoundly changed the ways we do business, buy, work and live. As digital technologies offer new ways to connect, collaborate, conduct business and build bridges between people, they touch the core of all business functions and even the ways organisations are managed.

Digital communication has presented India an opportunity to overcome the hindrances posed by deficiencies in its brick-and-mortar-based physical infrastructure and opened doors to new paradigms in all sectors of the economy whereby the common man is being served much more efficiently and at a fraction of the cost incurred earlier. Enterprises across sectors are embracing digital business models leading to a plethora of data being collected, and this will only be enhanced with greater adoption of IOT, machine learning and artificial intelligence.

E-governance: Benefit endowment and surveillance

While much of the focus has been on the companies collecting data, another entity which has more data on us than we know is the government. Governments across the world are not only leveraging citizen-centric data to provide benefits but also delivering security through their surveillance programmes. Governments are leveraging big data to improve healthcare or social security or provide tax benefits to citizens, thereby delivering better governance. Law enforcement agencies worldwide and central and state police are capturing information about thousands of users at a time, irrespective of whether or not they are targets of an investigation, through social media or mobile records.

Consumer's point of view: A day in the life of a consumer

In today's digitally transformed and connected world, data is produced in vast streams daily, at a mind-boggling volume and pace. Smartphones and the Internet have made data abundant, ubiquitous and far more valuable. We have started waking up with our voice-controlled home help, who will already know the weather and the state of traffic to office. As we step outside, our smartphone will direct us to the nearest ridesharing service cab, having our office and home location, and making the payment when we reach our destination from the connected E-wallet. As soon as we enter the office, our wearable tech updates us on the schedule for the day and the planned meetings. At lunchtime, we can use a food delivery app to order our preferred meal or make a reservation at our favourite restaurant. Similarly, we can book a weekend break on an online hospitality service and order new clothes from an ongoing sale on an e-commerce portal. As evening draws near, we will either book tickets for a new movie online or catch up on our favourite drama on an online streaming service. In addition, we post updates on our social and professional life on social media during the day. During this normal day, we have created both passive and active digital footprints.

Global

Internet users

3.5 billion or **48%** of the world population (2017)

2.0 billion or **28.9%** of the world population (2015)

Connected 'things'

8.4 billion (2017)

6.3 billion (2016)

India

Internet users

478 million (March 2018)

243 million (June 2014)

Smartphone users

456 million (March 2018)

220 million (June 2014)

Source: http://digitalindia.gov.in/; https://www.itu.int/; https://www.gartner.com/

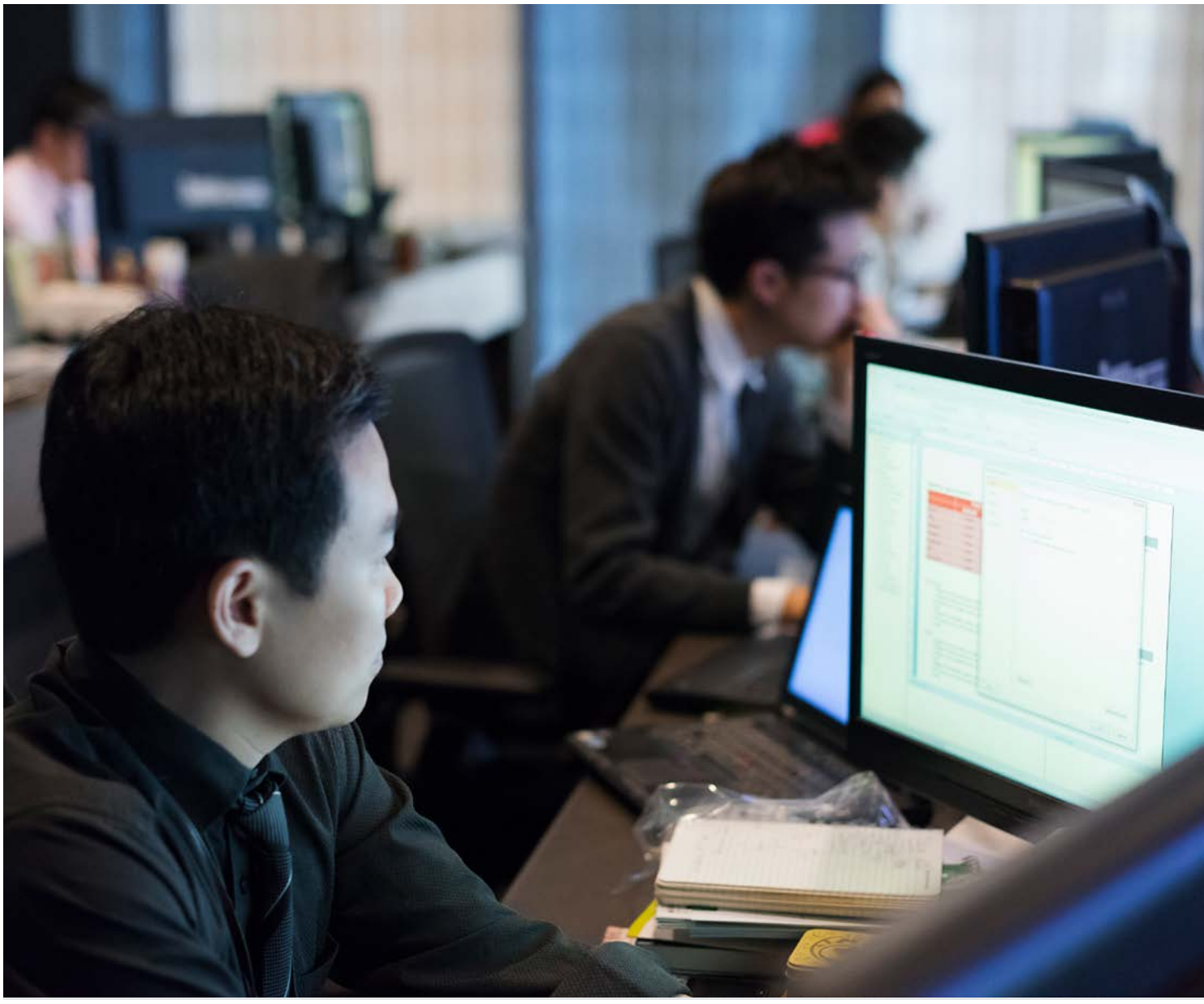
All the while, we are monitored as never before. Not surprisingly, a heightened focus on providing privacy to the end consumer and protecting data has gained paramount importance.

All of the above developments have made end consumer data the cornerstone of the data economy.

② Need for privacy and data protection is paramount

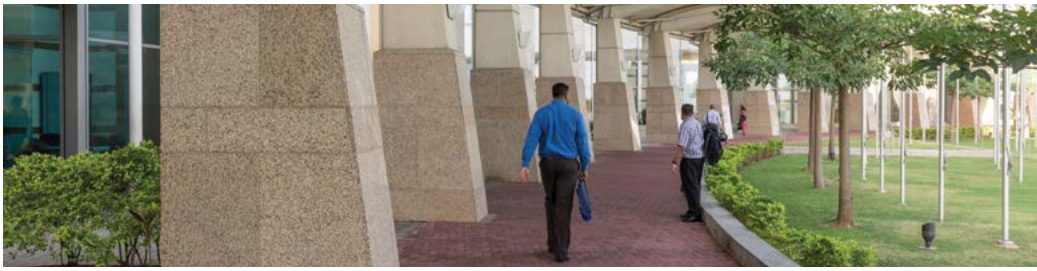
Profit motive of organisations leading to overreach in terms of data monetisation

Organisations are capturing consumer data that consumers provide consciously and also the digital footprint that they capture based on the activity of consumers. Massive amounts of data associated with an individual's attributes, movements, location and decisions are being captured by a plethora of entities. Technology platforms are harvesting, cleansing and summarising data and developing insights which they can then package and sell. A global 'rush' is now on to tap data flows and extract value. All of this is not restricted only to the technology giants or large manufacturing companies and start-ups, many of which use data to make new or niche markets that they want to dominate. In fact, in many entities, the entire business model hinges on data monetisation. Given this context, consumers are at the risk of being impacted with regard to privacy as organisations may cross the boundary of explicit consumer consent for use of the data in order to maximise their profit-seeking goal.



Inadequate investment in security could expose consumer data

In today's cyber security and privacy landscape, threats come from all sides, internal and external. Organisations not only have to look out for outsiders who target corporate networks to steal products, client and customer data, but also at insiders who already have access to the data and who may use it irresponsibly or for nefarious purposes.



External attacks, driven mostly by profit

Historically, the data breaches that make the news are typically carried out by outsiders, and are generally addressed with traditional security measures. External threats can be from cybercriminals and hackers looking for a payout. These can involve social media attacks, inadequately secured networks and end-points, and social engineering scams such as phishing.

- On 7 September 2017, a consumer credit reporting agency reported that hackers had exploited a vulnerability in its US website application to gain access to personally identifiable information such as address, social security numbers, driving licence details and, in some cases, credit card numbers of roughly 145.5 million US customers.
- An American restaurant chain and international franchise revealed that its website and app were hacked in October 2017, with personal information for an undisclosed amount of customers being jeopardised. The hack was believed to have compromised billing information including delivery addresses, email addresses and payment card information containing account numbers, expiration dates and CVV numbers of the affected users.

Internal attacks, driven mostly by lack of enforcement and exploitation of organisation practices

Threats from insiders are far harder to prevent, as insiders have access to sensitive information on a regular basis, and may know how that information is protected. This makes it far easier for them to steal it than for outsiders. Furthermore, insiders may also accidentally leak data or otherwise put it at risk. Whether by attaching the wrong file to an email being sent, oversharing on social media, losing a laptop or USB drive, or through some other mistake, insiders can put an organisation's data at risk with little effort.

- In 2014, an employee at a ridesharing service provider violated the company's policy by using its 'God View' tool to track a journalist who was late for an interview with its exec. The tool allowed the company's staff to track both its vehicles and customers. Though this tool was unavailable to drivers, it was, at the time, apparently widely available at the corporate level.
- An American multinational telecommunications holding company paid over 25 million USD in fines back in 2015, as a result of an investigation that discovered that employees at international call centres illegally disclosed the personal information of more than 2,80,000 customers. Even though the company had good intentions, it was subject to heavy fines for not adequately managing the cybersecurity threats by internal parties.

Although all these issues seem to stem from violation of security practices, they become privacy incidents when these breaches involve personal data. An increasing number of maligned people and groups are spending higher resources towards gaining access to sensitive data; organisations are not investing enough to build a defensible and scalable security infrastructure.

Free flow of personal data in the digital age, multiple touchpoints of data collection and processing, and the above-mentioned threats have led to a need for a holistic approach to data privacy and protection.

③ Growing recognition across the globe on the need for privacy regulations

Global perspective

The focus on data privacy began during the 1990s, with the developed economies recognising the importance of the personal data of its citizens, the challenges that came along with its misuse, and the need to protect such data from both private and state organisations. With this early focus, most of the global economic powers have come up with their own regulations and practices to be followed to safeguard the rights and freedom of their citizens. While holistic regulations have been put in place to prevent misuse and exploitation of personal data in the current data-intensive world, there are also sector specific laws (e.g. in the healthcare and banking sector) which further safeguard sectorial personal data in some of the countries.

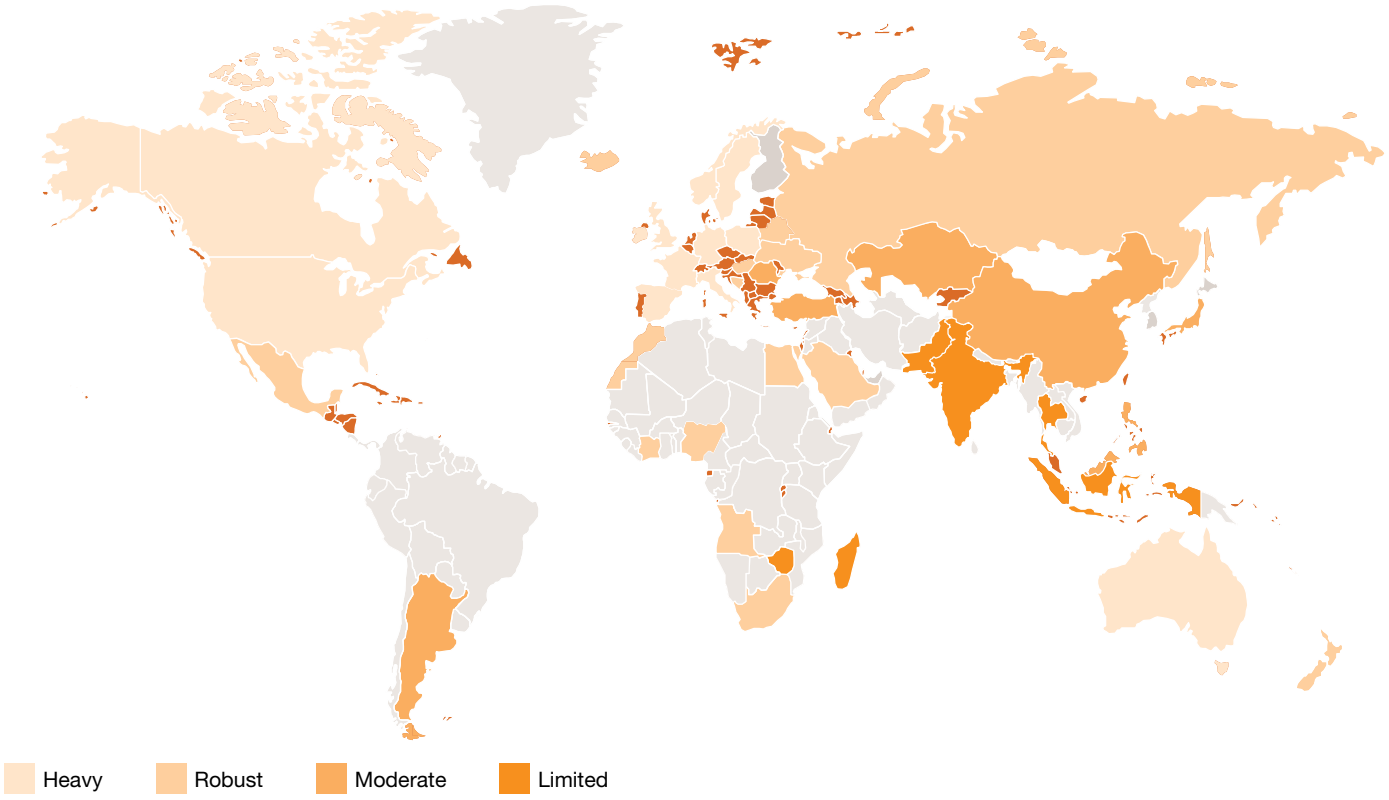
The US has traditionally been considered to have less regard for the importance of personal information protection. However, the US has had a Privacy Act regulating government departments and agencies since 1974, and many of the 50 states have their own privacy laws.

In the Asia-Pacific region, the early adopters of privacy and data protection laws – Australia, New Zealand and Hong Kong – have been joined by most of the other major jurisdictions.

Latin America has seen a noticeable increase in legislative initiatives in recent years. Only a handful of Latin American countries currently do not have specific privacy and data protection laws. Argentina and Uruguay have modelled their data protection laws after the EU approach, which explains why they are the only Latin American countries considered by the European Commission as providing an adequate level of protection.

The global gaps in coverage lie in Africa and the Middle East. However, the number of countries with laws impacting personal information is steadily rising in both regions.

Regulation and enforcement



Source: DLA Piper

Evolution of privacy

USA – Evolution of privacy

1996 Health Insurance Portability and Accountability Act (HIPAA)

1998 Children's Online Privacy Protection Act (COPPA)

2002 Federal Information Security Management Act (FISMA) and Confidential Information Protection and Statistical Efficiency Act (CIPSEA)

2010 The Gramm-Leach-Bliley Act, as amended by the Consumer Financial Protection Act

2013 HIPAA amended to increase regulation around use of protected health information

2014 COPPA updated to extend the scope to foreign countries

2018 California Consumer Privacy Act (claimed to be the nation's toughest data privacy law)

Latin America – Evolution of privacy

1999 **Chile:** Personal Data Protection Act came into force

2000 **Argentina:** Personal Data Protection Law No. 25,326 (PDPL) was enacted

2002 **Chile:** Personal Data Protection Act amended to make the regulatory landscape more robust

2008 **Uruguay:** Personal Data Protection and Habeas Data Action was adopted

2015 **Brazil:** The federal government submitted the 'Bill of law' which aims to heavily regulate the processing and protection of personal data

2016 **Argentina:** The Argentine National Congress passed Law No. 27,275 on Access to Public Information (LAPI)

2017 **Argentina:** A 'Draft Bill' modifying the current data protection regime was submitted to Congress

Chile: The government has proposed a 'new bill' to wholly replace the current Personal Data Protection Act

Europe – Evolution of privacy

1995 First EU Data Protection Directive

2012 General Data Protection Regulation (GDPR) proposed by the European Commission in place of the EU Directive

2015 Enforcement of the GDPR

Middle East – Evolution of privacy

2003 Regulating Telecommunications (Federal Law by Decree 3 of 2003 as amended)

2012 Cyber Crime Law (Federal Law 5 of 2012 regarding Information Technology Crime Control

2017 UAE's Central Bank published the 'Digital Payment Regulation'

APAC – Evolution of privacy

2000

India: Data privacy and data protection were given focus through the Information Technology Act (IT Act)

Japan: Act on the Protection of Personal Information (APPI) passed

2010

China: Tortious Liability Law

2015

China: Criminal Law, as amended by its Ninth Amendment

Japan: Extensive amendments to the Act on the Protection of Personal Information (APPI)

2017

India: Privacy declared as a fundamental right. The draft data protection bill and DISHA opened for public comments

China: General Provisions of the Civil Law of the People's Republic of China

Japan: APPI became enforceable

Common themes that stand out across data privacy regulation

Data privacy laws across the globe are built with a common objective of protecting the privacy and personal data of individuals. While specific requirements do exist, data privacy laws are built on common privacy principles such as Fair Information Practices (FIPS) and Organization for Economic Cooperation and Development (OECD) guidelines that aim to address individual privacy rights and freedom. Based on analysis of various data privacy laws across the world, we have identified a few common areas. These include:

Individual rights:

Rights of individuals to exercise control over their personal data processed by organisations. These include rights such as right to information, right to access, right to be forgotten and right to rectification. In addition to the above, regulations are increasingly giving importance to user consent and notice to allow users visibility and control over their personal information.

Data protection:

Multiple regulations across the globe emphasise the need for organisations to protect the personal data processed by them. The general requirement here is to take reasonable technical, physical and organisational measures to protect the security of personal data.

Breach identification and notification:

Multiple regulations require organisations to implement reasonable security measures to protect personal data and also have measures to ensure timely detection, notification and management of security incidents and breaches.

Enforcement and consequence management:

A majority of the regulations across the global have enforcement and penalties that ensure organisations have adequate governance in place to track compliance and make the right investments towards data protection and privacy.

4 India – moving in the right direction

Information Technology Act (IT Act), 2000, and section 43A of IT Act

Although India is at a nascent stage in the overall data privacy and protection maturity timeline, avenues under the law of torts and Indian Penal Code, 1860, have always existed. The concepts of data privacy and data protection were given focused attention through provisions of the IT Act after the amendments in 2009 (Information Technology (Amendment) Act, 2008) and subsequently in 2011 (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (Rules). They form the main laws governing data protection and information technology in India. These laws are considered to be relatively weak in the area of privacy as compared to global standards.

The Information Technology (Amendment) Act, 2008, brought into existence provisions such as section 43-A and Section 72-A. However, as per the amendment in 2011, section 43-A of the IT Act primarily focuses on 'reasonable security practices and procedures' and 'sensitive personal data or information' (SPDI). Section 72-A of the IT Act mandates punishment for disclosure of 'personal information' in breach of lawful contract or without the information provider's consent.

This laid the foundation for the data privacy law in India and steered the thought process in the direction of data privacy and protection.

Srikrishna Committee – the Draft Data (Privacy and Protection) Bill, 2017

In a historic verdict delivered by a nine judge constitution bench, the Supreme Court of India (the Court) unanimously recognised the right to privacy as a fundamental right guaranteed under the Constitution of India (the Constitution).

On 31 July 2017, the Ministry of Electronics and Information Technology, Government of India (MeitY) appointed a Committee of Experts under the Chairmanship of former Supreme Court Justice Shri B N Srikrishna to study various issues relating to data protection in India, offer recommendations on principles to be considered for data protection in India and suggest a draft Data Protection Bill. The objective is to 'ensure growth of the digital economy while keeping personal data of citizens secure and protected'.

On 28 November 2017, the committee released a white paper seeking public comments on the recommendations made on the draft data protection framework. The paper released by the committee is based on global leading practices on data protection from the European Union (EU), especially the General Data Protection Regulation (GDPR), the United Kingdom, Canada and the United States.

The committee was expected to meet a few more times to finalise its recommendations before submitting its final report to the IT Ministry. The draft bill will later be introduced in the Parliament, subject to the government's agreement on the same (with or without modifications).

While the proposed framework paves the way for a robust privacy regime, privacy laws should also cater to specific sectors such as healthcare, telecom, banking and finance to address the various nuances in each sector.

The following sections cover sector-specific privacy developments in India.

India – sector updates

TRAI – Recommendation on 'Privacy, Security and Ownership of Data in the Telecom Sector'

On 16 July 2018, the Telecom Regulatory Authority of India (TRAI) issued its Recommendations on Privacy, Security and Ownership of Data in the Telecom Sector. The recommendations issued by TRAI are applicable to the entire ecosystem used for delivery of digital services consisting of multiple entities like telecom service providers (TSPs), personal devices (mobile handsets, tablets, personal computers, etc.), machine to machine (M2M) devices, communication networks (consisting of base trans receiver stations, routers, switches, etc.), browsers, operating systems, over the top (OTT) service providers and applications.

The authority recommends some key measures around the definition of personal data, sufficiency of the existing data protection framework, user empowerment and data privacy, and security of telecom networks. The authority requires that the 'privacy by design' principle be made applicable to all the entities in the digital ecosystem. The concept of 'data minimisation' has to be inherent to the implementation of the 'privacy by design' principle. It is proposed that the right to choice, notice, opt-in consent, data portability, and right to be forgotten should be conferred upon telecommunication consumers. The authority also requires personal data of consumers to be encrypted during the motion as well as during the storage in the digital ecosystem.

Digital Information Security in Healthcare Act (DISHA)

DISHA is the proposed privacy and data protection law in India which seeks to regulate the generation, collection, storage, transmission, access and use of all digital health data. DISHA will set a precedent for the creation of digital health records, and will enable the digital sharing of personal health records between different hospitals and clinics. The Ministry of Health and Family Welfare (MoHFW) opened DISHA for public comments on 21 March 2018.

The proposed draft act primarily regulates 'clinical establishments' as well as 'entities' that generate, collect, access, transmit or use digital health data (DHD) and their associated personally identifiable information.

Under DISHA, anonymised or de-identified data can be used for specific public health purposes such as early identification and prevention of diseases and research for public health, clinical and academic purposes. However, it strictly prohibits access, use or disclosure of DHD (whether in identifiable or anonymised form) by any other entity for a commercial purpose. DISHA prohibits the use of DHD by employers, insurance companies, human resource consultants and pharmaceutical companies under any circumstances. Insurance companies can access a data owner's DHD from the clinical establishment to which an insurance claim relates but only for the purpose of processing that claim.

The act is in its draft stage for public consultation.

The above developments would help shape a strong privacy regime within India and bring it at par with robust privacy regulations of some of the developed markets. This would also change the way business is carried out.

5 Indian organisations are waiting for the regulation as opposed to taking proactive measures towards privacy

The World Economic Forum's 2018 Global Risks Report ranks both large-scale cyberattacks and major data breaches or fraud among the top five most likely risks in the next decade.[1]

However, there is some cause for optimism. Based on responses from 9,500 executives in 122 countries and territories, the results of PwC's Global State of Information Security Survey (GSISS) 2018 show that 87% of global CEOs are investing in cyber security to build trust with customers. Nearly as many (81%) say they are creating transparency in the usage and storage of data. Will it be enough? Unfortunately, less than 50% CEOs say they are taking these actions 'to a large extent'.[2]

Many India companies are still beginners in data use governance and only about half of the Indian respondents have put key measures in place.

State of data use governance in India

Source: PwC's GSISS 2018

While more than half the respondents say they have drafted an information security strategy, the same strength is not reflected in taking specific actions related to data privacy. Organisations are still struggling to maintain an accurate inventory of personal data they have collected through the various touchpoints in the data lifecycle. Only a third of the organisations are able to limit personal data collection, retention and access to the minimum necessary.[3] While many organisations have proactively included privacy aspects in their third-party compliance audits, many of them have not been able to force them to comply with their privacy policies.

Many organisations are awaiting the upcoming regulations to address privacy-related issues.

1 World Economic Forum. (2018). The Global Risks Report 2018. Retrieved from https://www.weforum.org/reports/the-global-risks-report-2018 (last accessed on 24 July 2018)

2 PwC. (2018). The Global State of Information Security® Survey 2018, Retrieved from https://www.pwc.com/us/en/services/consulting/cybersecurity/library/information-security-survey.html (last accessed on 24 July 2018)

3 Ibid.

⑥ Taking the right call on certain aspects will be the key

We believe certain nuances will need to be addressed appropriately in order to establish a robust, transparent and enforceable regulation.

Borderless Internet

The borderless nature of the Internet raises several jurisdictional issues on data protection. A single act of processing of personal data could very easily occur across multiple jurisdictions (outside the state territory) where the state may not have the authority to exercise its jurisdiction. To address this, not only should the regulation apply to entities (both public and private) within India that process personal data of Indian citizens and residents but it should also be applicable to all kinds of processing carried out on the personal data of Indian citizens and residents, even though such processing may not be entirely based in India or may be carried out by non-Indian entities that do not have a presence in India.

Cross-border transfer of data

Cross-border data transfer is unavoidable in today's global and digital age. Data seamlessly and freely flows across borders. This exchange of data leads to exchange of information and ideas which stimulate innovation and drive growth. However, it is not always easy for countries to exert control over data that leaves its territorial boundaries. Safeguarding a person's personal data transferred to an international geography remains a challenge.

In our view, the regulation should clearly restrict transfers only to countries that offer an adequate level of protection and propose additional measures that need to be ensured for data transfers that do not meet such standards.

Accountability of data

Accountability is a central principle in data protection. To translate data protection norms into action, a widely used method is to identify the party accountable for compliance with these norms. For this purpose, the concept of control over data is used.

However, given the recent trends across the globe (e.g. EU GDPR), the regulation should assign certain basic obligations to the data processor as well, such as ensuring the security of personal data, notifying breaches and supporting investigations. This is of significance since organisations these days rely extensively on third parties for services. Not considering this aspect may lead to inability in assigning absolute accountability to parties involved in managing and processing data. The regulations should go beyond the entity collecting the data directly from the end consumer (data controller).

Both the data processor and data controller should be equally accountable for safeguarding data.

State interest vs individual's privacy

Both public and private sector entities process personal data about data subjects. There is definitely a need to protect an individual's informational privacy rights through a comprehensive data protection regulation which covers both public sector and private sector entities. However, there are certain legitimate state interests for processing personal data, which may conflict with an individual's privacy rights. One such example is law enforcement and surveillance for national security.

The proposed regulations will need walk a tight line between right to privacy and national security considerations in order to strike the right balance and avoid excessive interference in citizens' personal life without justification. Such considerations, categories and exceptions should be clearly called out to avoid any ambiguity to the extent feasible.

Localisation of data

Under data localisation, entities are required to store and process personal data on servers physically present within their national boundaries. Although this approach helps address concerns over data privacy, security, surveillance and law enforcement to an extent, it increases the burden on businesses by way of increased cost of compliance and may also impact the building blocks of economy which rely on data exchange.

The regulation should take a call on data localisation after considering a cost-benefit analysis between the enforcement benefits derived from data localisation and the costs involved pursuant to such requirements. A one-size-fits-all model may not be the most fruitful model and may cause more harm than benefit to the industry.

Impact on micro, small and medium enterprises (MSMEs)

In the Indian context, it also important to ask questions on the applicability and impact of any such data protection regulation on small and medium businesses (SMBs). Stringent regulations may deter MSMEs due to the high costs and technology investments necessary for compliance. However, in the new age economy, a number of small enterprises are capturing and processing large volumes of data.

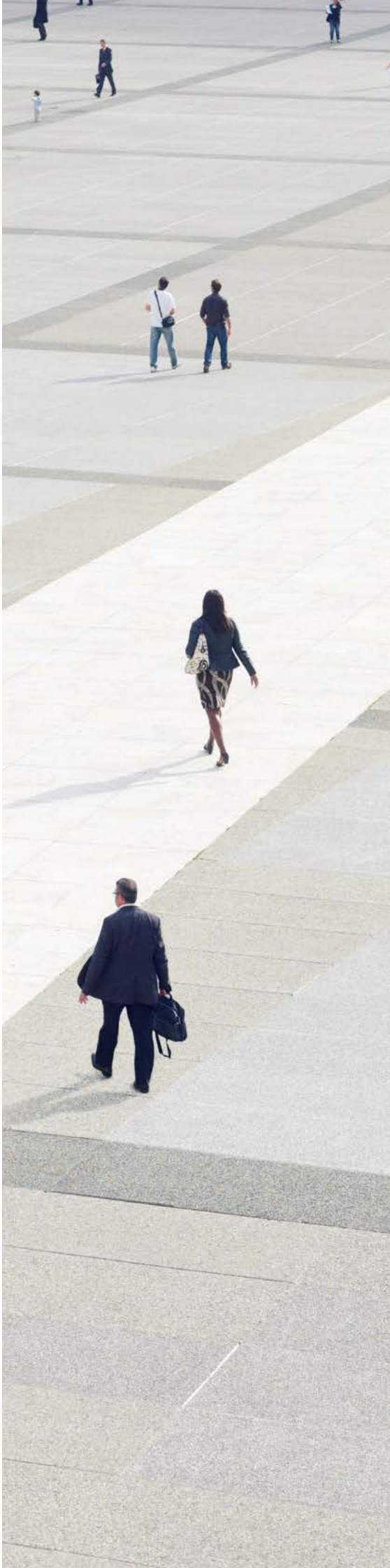
Further, certain categories of private processing, such as processing carried out by not-for-profit organisations or charitable institutes, may have to be dealt with categorically and provided with certain exemptions.

In our view, the regulation should adopt a risk-based approach and provide certain relaxations and exceptions for MSMEs under specific circumstances.

Penalties and compensation

It is important that the regulations provide adequate deterrence for non-adherence by way of penalties. To do so, the penalties should be commensurate with the size and nature of the business. Further, greater clarity around the quantum of penalty rather than discretion in the hands of the regulatory authority would be better in terms of transparency. Further, there should be a higher level of penalty for breaches of privacy that organisations wilfully make or that result from negligent security practices.

As regards compensation, there should be clarity around the quantum and nature of the same to the extent feasible.



7 Conclusion

Privacy, security and trust are all increasingly at risk and also more important and intertwined in our data-driven economy. Digital technologies have profoundly changed the way in which we do business, buy, work and live. In today's digitally transformed and connected world, data is produced in vast streams daily, at a mind-boggling volume and pace. Not surprisingly, a heightened focus on providing privacy to end consumer and protecting the data has gained paramount importance.

The digital footprint and the massive data flow in the borderless digital world is continuously susceptible to attacks. The threats to data, intentional or unintentional, are real and will come from all sources, internal and external, driven mostly by profit. The misuse of an individual's personal data can violate his or her rights and freedoms. Hence, the onus of protection will be on enterprises.

While firm privacy regulations are in the making, some of the tenets of the laws should have already been discussed and debated. There should be adequate deterrence for non-adherence by way of penalties. Security practices to protect the data need to be more prescriptive rather than descriptive. However, this cannot come at the cost of doing business.

As the new data privacy and protection regime plays out, timely planning/action will help organisations continue their business as usual and enhance their business reputation.

Notes

Notes

About ASSOCHAM

The Knowledge Architect of Corporate India

The Associated Chambers of Commerce and Industry of India (ASSOCHAM), India's premier apex chamber covers a membership of over 4 lakh companies and professionals across the country. ASSOCHAM is one of the oldest Chambers of Commerce which started in 1920. ASSOCHAM is known as the "knowledge chamber" for its ability to gather and disseminate knowledge. Its vision is to empower industry with knowledge so that they become strong and powerful global competitors with world class management, technology and quality standards.

ASSOCHAM is also a "pillar of democracy" as it reflects diverse views and sometimes opposing ideas in industry group. This important facet puts us ahead of countries like China and will strengthen our foundations of a democratic debate and better solution for the future. ASSOCHAM is also the "voice of industry" – it reflects the "pain" of industry as well as its "success" to the government. The chamber is a "change agent" that helps to create the environment for positive and constructive policy changes and solutions by the government for the progress of India.

As an apex industry body, ASSOCHAM represents the interests of industry and trade, interfaces with Government on policy issues and interacts with counterpart international organizations to promote bilateral economic issues. ASSOCHAM is represented on all national and local bodies and is, thus, able to pro-actively convey industry viewpoints, as also communicate and debate issues relating to public-private partnerships for economic development.

The road is long. It has many hills and valleys – yet the vision before us of a new resurgent India is strong and powerful. The light of knowledge and banishment of ignorance and poverty beckons us calling each member of the chamber to serve the nation and make a difference.

Department Of Corporate Affairs, Fintech & Blockchain Technology

Santosh Parashar
Additional Director & Head
santosh.parashar@assocham.com

Jatin Kochar
Executive
jatin.kochar@assocham.com

Vikash Vardhman
Executive
vikash.vardhman@assocham.com

Abhishek Saxena
Assistant Director
abhishek.saxena@assocham.com

Anish Yadav
Executive
anish.yadav@assocham.com

The Associated Chambers of Commerce and Industry of India
ASSOCHAM Corporate Office:
5, Sardar Patel Marg, Chanakyapuri, New Delhi-110 021
Tel: 011-46550555 (Hunting Line) • Fax: 011-23017008, 23017009
Email: assocham@nic.in • Website: www.assocham.org

About PwC

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 158 countries with more than 2,36,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com

In India, PwC has offices in these cities: Ahmedabad, Bengaluru, Chennai, Delhi NCR, Hyderabad, Kolkata, Mumbai and Pune. For more information about PwC India's service offerings, visit www.pwc.com/in

PwC refers to the PwC International network and/or one or more of its member firms, each of which is a separate, independent and distinct legal entity. Please see www.pwc.com/structure for further details.

About the authors

This point of view has been co-authored by Siddharth Vishwanath, Sriram Sivaramakrishnan, Rushit Choksey and Sunil Prabhakaran.

Siddharth Vishwanath is a Partner and leads the Cyber Security Advisory practice for the firm. Sriram Sivaramakrishnan focuses on data privacy and protection within the Cyber Security practice. Rushit Choksey and Sunil Prabhakaran anchor the firm's data privacy and protection programme.

Contact us

Sivarama Krishnan
Leader, Cyber Security
sivarama.krishnan@pwc.com

Siddharth Vishwanath
Partner and Cyber Advisory Leader
siddharth.vishwanath@pwc.com

Anirban Sengupta
Partner, Cyber Security
anirban.sengupta@pwc.com

Hemant Arora
Partner, Cyber Security
hemant.arora@pwc.com

Krishna Sastry Pendyala
Executive Director, Cyber Security
sastry.pendyala@pwc.com

Manu Dwivedi
Partner, Cyber Security
manu.dwivedi@pwc.com

PVS Murthy
Partner, Cyber Security
pvs.murthy@pwc.com

Rahul Aggarwal
Partner, Cyber Security
rahul2.aggarwal@pwc.com

Ramanathan (Ram) V. Periyagaram
Partner, Cyber Security
ram.periyagaram@pwc.com

Sangram Gayal
Partner, Cyber Security
sangram.gayal@pwc.com

Sriram Sivaramakrishnan
Partner, Cyber Security
sriram.s@pwc.com

Sundareshwar Krishnamurthy
Partner, Cyber Security
sundareshwar.krishnamurthy@pwc.com

Unnikrishnan P
Partner, Cyber Security
unnikrishnan.padinjyaroot@pwc.com

Venkat Nippani
Partner, Cyber Security
venkat.nippani@pwc.com

Murali Krishna Talasila
Partner, Cyber Security
murali.talasila@pwc.com

pwc.in

Data Classification: DC0

HS/July2018-13871