Ministry of Industry and Commerce Chair on Intellectual Property Rights,
Institute of Excellence on IPR and Standards, and
Centre for Intellectual Property Rights and Advocacy (CIPRA)

National Law School of India University, Bengaluru

Presents

A Round Table on "Emerging Trends in Privacy and Data Protection in India"

Date: 2nd Dec 2017
Venue: Taj West End, Race Course Road, Bangalore

CONCEPT NOTE

The Concept of Privacy

The roots of the concept of privacy may be traced as far back as the teachings of Aristotle in ancient Greece, in the distinction he drew between politics (polis) and the domestic space (oikos). Over time, this concept has evolved into two distinct legal forms: (i) as an action for damages under tort law, as in cases where one's privacy has been unlawfully invaded; and (ii) constitutional recognition of individuals' right to privacy against unlawful Government intrusion.

However, this liberty-centric approach is insufficient to address the myriad privacy concerns that have arisen in the digital age. The internet is unique in the sense that it solicits information from users every step of the way, as a necessary precondition for participation in cyberspace.

In general data protection law across the globe, irrespective of their economic evolution however based on appreciation for right to privacy protects personal information (PI) of their citizen/resident. PD simply defined as all data/information relating to individuals (not legal entities) who are or can be identified from that very information and who are susceptible to adverse consequences from its use. Personal data may, however, be subject to less stringent controls than normal in fields such as: state security, defense and the investigation and prevention of criminal activities. This included in a private individual's files for purposes such as use in a diary or schedule, may also be exempted. A higher level of protection is accorded to sensitive information. This includes personal data revealing political or trade union membership, religious beliefs and information concerning a person's health, sex life or ethnic origin.

With today's technologies, it is easier for organizations to collect, copy and transfer personal data around the world. At the same time, the introduction of a wide range of privacy and security laws in several jurisdictions around the world impose complex and often inconsistent privacy and data protection standards. These inconsistencies in different jurisdictions often impact the manner in which the organizations can, practically, comply with these privacy and security laws.

An Introduction to Global Data Privacy

In this new (*modern will be a misnomer*) digital age, which runs on the fuel of Data, "Personal Data" is an increasingly valuable business asset. Technology provides the opportunity to understand and engage with customers and stakeholders like never. Deployed carefully, it can enhance relationships and provide tangible competitive advantage in the marketplace. It needs to be managed with care, as collecting, using and sharing data is subject to increasing levels of regulation by legislators concerned about personal privacy and cyber-attacks.

Global Evolution in Data Protection Regime

Data protection laws are built on fundamental rights enshrined in the Charter of Fundamental Rights of the European Union which are the core building blocks of the EU's legal regime. Privacy issues arising from an exponential growth in consumer and mobile

technologies, an increasingly connected planet and mass cross border data flows have pushed the EU to entirely rethink its data protection legislation to ensure that these fundamental rights are full protected in today's digital economy.

The European General Data Protection Regulation(GDPR) which comes fully into effect in May 2018 will herald some of the most stringent data protection laws in the world, imposing a heightened compliance regime underpinned by ramped-up enforcement including the potential for fines of up to 4% global corporate turnover.

Britain is pushing to closely mirror the EU's data protection laws after Brexit, in a bid to ensure the free flow of data across borders which is vital in underpinning the digital economy. In the last of its major policy papers before resuming Brexit talks next week, the government called for an "early" agreement to keep personal data flowing and assure legal certainty for businesses.

Japanese Act on the Protection of Personal Information are based on the principles expressed by the GDPR. On July 6, 2017, the European Commission and the Japanese government published a joint statement on international transfers of personal data. The statement mentions that the EU and Japan will continue their cooperation and aim by early 2018 to recognize each other as having adequate levels of personal data protection.

Similarly, other significant changes are Australian/New Zealand Privacy principle development which will rewrite of Australian Privacy Act 1988 & Privacy Act (1993) and its 12 Information Privacy Principles (NZ IPPs).

India - Data Privacy Landscape

India has embarked on this digitization journey and has in fact showcased the world how new business industries like e-Commerce, digital payments, financial services, etc. can emerge, evolve, flourish and contribute in the digital economy of the nation. While India is leading in providing IT services to businesses across the globe; the domestic sector has emerged as a key IT investor; and organizations have started understanding the business potential of processing and using personal data. Private sectors such as BFSI, Telecom, Manufacturing, Travel and Healthcare are increasingly relying on IT to process transactions, offer diverse channels to their customers and collect and use personal data from plethora of varied channels. Government too has started various projects through its various departments in order to reach and provide benefits to citizens in a better and efficient manner. Projects and initiatives such as Digital India program, technology adoption trends in e-Governance projects, Smart cities, Aadhaar linked Direct Benefits Transfers, Income Tax eFiling, Health Management Information Systems, Digital Locker, Jan Dhan Yojna and many other projects at centre and state level, all collect and process personal information in huge volumes. But, in all of this, increasing information sharing and processing, along with linking different databases with identity projects like Aadhaar and mobile number has increased privacy risks. Information leakage of personal, sensitive information is a real threat to all Technology Led initiatives that India is undertaking. Most of the organizations and government departments have security policies, but effective implementation and enforcement remains a challenge. Security and Privacy is essential to provide assurance to citizens and consumers engaging in digital transactions.

Missing elements in current Privacy regime in India

Following is the list of some of the most critical aspects which are missing in the current regime:

- **Coverage**: Most of the Data Protection laws cover entire gamut of Personal Information (PI), while our existing laws do not cover it exhaustively. IT Act Sec 43A rules focus on Sensitive Personal Data or Information (SPDI) only. While Sec 72 and 72A talk about personal information, these sections are very narrowly focused in their scope and applicability. IT Act is limited only to Computer and Computer Resources, and does not apply on physical form of data. It means that the law is applicable only when personal data is in electronic form and leaves out the data available in hard copies such as medical records on paper, CAF forms by telecom operators, personal data collected on papers in various scenarios such as lucky draw at petrol pumps, etc. Similarly, Aadhaar Act and Regulations are limited to Aadhaar related information.
- **Applicability:** Reasonable Security Practices and Procedures Rules under Sec 43A of the IT Act are applicable only to body corporates which is narrowly defined as organizations providing professional services, and doesn't usually cover government departments and agencies which are collecting and processing PI for non-commercial purposes such as for providing social benefits, income tax/ revenue purposes, intelligence and national security, etc.
- **Jurisdiction**: Legislation is applicable to personal information in IT systems located in physical territory of India, and doesn't include Indian citizens' data stored in Cloud/ other systems hosted outside India.
- **Framework/Approach**: The regulation has addressed requirements of various privacy principles through rules notified in 2011 under section 43A, but has not listed them explicitly. The framework defining the privacy principles, their applicability and scope should be a standard approach.
- **Enforcement**: Unlike EU member states that have Data Protection Authorities or Information Commissioners or the USA where a nodal agency like Federal Trade Commission (FTC) oversees Privacy matters, and have the power to enforce privacy regulations, in India we do not have any such enforcement mechanism. Under ITAA, Adjudicating Officers are notified but they cannot take Suo-Moto action and can only order compensation to data subject, and not impose penalty or fines.
- **Unaddressed provisions**: There are various elements notified under the current regime, such as audit by government empaneled auditors, encryption requirements, data retention period, etc. which are not yet clearly defined in our laws. Hence, frequent reviews and guidelines on various aspects would be very crucial in upcoming data protection bill in India.
- **Rights of Data Subjects:** Although IT Act establishes certain rights like right to recourse and seek compensation, it is very limited when compared to EU laws.
- **Technology Evolution:** Most of the countries, including EU, continue to grapple with issue of how to contextually evolve Data Protection laws with changing technology landscape. IT Act provisions too could be termed as inadequate to address current challenges.

In absence of a comprehensive Data Protection law for significant number of years, the federal law regulating the collection and use of personal data is the Information Technology (Amendment) Act, 2008 and rules therein. Any person that is negligent in implementing reasonable security practices and procedures (RSPPs) in protecting sensitive personal data or information (SPDI) is liable to pay compensation for any wrongful loss or wrongful gain (section 43A, IT Act).

There are a few sectoral regulations that deal with confidentiality of information, including laws relating to healthcare, telecommunications, banking and securities. The Professional Code of Ethics of Doctors requires doctors to keep patient information confidential, although such information can be disclosed if there is a serious and identified risk to a person or community. Under telecommunications laws, customer accounting and user information (except roaming information) cannot be transferred overseas or accessed remotely from overseas. Banking laws prescribe certain principles based on which a bank can outsource its functions, where this results in data being processed, stored or accessed overseas.

In a groundbreaking series of events in Indian in this year (2017) in the data privacy domain, the honorable Supreme Court of India while revisiting the question of privacy 55 years after it decided that it is fundamental right for citizens. The nine-judge Bench's judgment gains international significance as privacy enjoys a robust legal framework internationally. The judgment, declares privacy as a fundamental right, and finally reconcile our laws with the spirit of Article 12 of the Universal Declaration of Human Rights, 1948, and Article 17 of the International Covenant on Civil and Political Rights (ICCPR), 1966, which advocates a framework to legally protects persons against the "arbitrary interference" with one's privacy, family, home, correspondence, honor and reputation.

As a next step and to create robust mechanism for making this fundamental right in actable - a committee, headed by former Supreme Court Judge B N Srikrishna, will produce a draft data protection bill after "identifing key data protection issues" in India and recommend methods to address any potential problems. The ten-member committee – which includes representatives from the department of telecommunications (DoT), the IT ministry, the Unique Identification Authority of India (UIDAI) and the academic community – will not only study the various issues around data protection in India but will also draft a data protection bill that will be taken up for consideration by the Centre. Sectorally too, there has been movement on Data Protection after TRAI brought a consultation paper on regulating data protection affairs for telecom sector.

With this background, we wish to seek views of stakeholders on this important subject through this workshop, and prepare a multi-stakeholder report. You are cordially invited to participate in the Roundtable on Privacy and Data Protection.

Prof (Dr) T Ramakrishna,
Professor of Law, Ministry of Industry and Commerce Chair Professor on IPR
National Law School of India University, Bengaluru, Karnataka, India

Programme schedule
2nd Dec 2017

Time	Tentative Agenda
10.30a.m – 11.10 a.m. **Welcome Address**	**Prof. (Dr.) T. Ramakrishna** Professor of Law, MIC Chair Professor, NLSIU, Bangalore.
Keynote Address	**Mr. Sanjay Sahay, IPS** Additional Director General of Police, Karnataka State Police, Bangalore.
Presidential Address	**Prof. (Dr.) R. Venkata Rao** Vice – Chancellor, NLSIU, Bangalore.
11.15a.m – 1.00 p.m. Panel Discursion	**Chair:** **Dr. S K Murthy,** Director of IP, Intel India **Discussants:** **Prof. Sridhar,** iiit-b, Bangalore **Mr. Venkatesh Murthy,** Deputy Director, DSCI. **Mr. Kumar Ranganathan,** Industry expert and Consultant. **Mr. Rahul Sharma,** Founder – The Perspective. **Mr. S K Prakash,** Senior Corporate Counsel – CISCO. **Ms. Kavita Gupta,** Co-Chair IAPP KNET, Bangalore. **Mr. Devender Kumar,** VP and Head IR and BC, Mphasis. **Mr. Na Vijayashankar (Naavi),** Cyber Security Expert. **Mr. S Gupta Boda,** Research Specialist and Former CISO. **Mr. Srinivas. P,** VP and Head Data protection, Infosys. **Mr. Sunil Varkey,** CISO, WIPRO. **Mr. Nilesh Patil,** Head Cyber Security Ops, CapGemini. **Mr. Vijay Ananad,** Data Analytics, Philips. **Mr. Nitin Pai, Founder,** Takshashila Foundation. **Mr. Ramesh Kautha,** CISO, SecurelyShare. **Mr. Srinivas B P,** KPMG.
Vote of Thanks	**Mr. Vivek Anand Sagar** Research Scholar, CIPRA, NLSIU
1.00 p.m	**Group Photo and Lunch**

For any queries related to the Roundtable or any assistance, please feel free to contact any of following members of organization body:

- **Mr. B. Vivek Anand Sagar,** Research Scholar, CIPRA, NLSIU e-mail: bvivek.nls@gmail.com / vivek.s@nls.ac.in (Mob. +91 9916590318)
- **Mr. Satyadeep Kumar Singh,** Research Associate, Institute of Excellence on IPRs and Standards, NLSIU, Bengaluru e-mail: satydeep2002@gmail.com/satyadeep@nls.ac.in (Mob. +91 9986524415).