International Journal of Law
ISSN: 2455-2194
Impact Factor: RJIF 5.12
www.lawjournals.org
Volume 4; Issue 2; March 2018; Page No. 01-08

Issues of personal data protection and privacy policy: A comparative analysis for different countries

Sheshadri Chatterjee
Master of Law & Research Scholar, National Law University, Delhi, India

Abstract
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 way the organizations can, practically, comply with these privacy and security laws. This paper is providing a comparative analysis of data protection policy and privacy that are applicable in different countries.

Keywords: data protection, digital era, comparative analysis, IT Act 2000, policy, privacy

Introduction
The 21st century has witnessed such an explosive rise in the number of ways in which we use information that it is widely referred to as 'the information age'. It is believed that by 2020, the global volume of digital data we create is expected to reach 44 zettabytes.1 much of that new information will consist of personal details relating to individuals, including information relating to the products they have purchased, the places they have travelled to and data which is produced from "smart devices" connected to the Internet. With the rapid development of technology, computers can process vast quantities of information to identify correlations and discover patterns in all fields of human activity. Enterprises around the world have realized the value of these databases and the technology for its proper mining and use is evolving every day. Proprietary algorithms are being developed to comb this data for trends, patterns and hidden nuances by businesses. Many of these activities are beneficial to individuals, allowing their problems to be addressed with greater accuracy. For instance, the analysis of very large and complex sets of data is done today through Big Data analytics. Employing such analytics enables organizations and governments to gain remarkable insights into areas such as health, food security, intelligent transport systems, energy efficiency and urban planning. This is nothing short of a digital revolution. This digital revolution has permeated India as well. Recognizing its significance, and that it promises to bring large disruptions in almost all sectors of society, the Government of India has envisaged and implemented the "Digital India" initiative. This initiative involves the incorporation of digitization in governance; healthcare and educational services; cashless economy and digital transactions; transparency in bureaucracy; fair and quick distribution of welfare schemes etc. to empower citizens.

Personal Data and Privacy
With nearly 450 million Internet users and a growth rate of 7-8%, India is well on the path to becoming a digital economy, which has a large market for global players. This digital economy is expected to generate new market growth opportunities and jobs in the coming 40-50 years. While the transition to a digital economy is underway, the processing of personal data has already become ubiquitous in both the public and private sector. Data is valuable per se and more so, when it is shared, leading to creation of considerable efficiency. The reality of the digital environment today, is that almost every single activity undertaken by an individual involves some sort of data transaction or the other. The Internet has given birth to entirely new markets: those dealing in the collection, organization, and processing of personal information, whether directly, or as a critical component of their business model. As has been noted by the Supreme Court in Puttaswamy. Something as simple as hailing a taxi now involves the use of a mobile application which collects and uses various types of data, such as the user's financial information, her real-time location, and information concerning her previous trips. Data is fundamentally transforming the way individuals do business, how they communicate, and how they make their decisions. Businesses are now building vast databases of consumer preferences and behavior. Information can be compressed, sorted, manipulated, discovered and interpreted as never before, and

can thus be more easily transformed into useful knowledge. There are many benefits to be gained by collecting and analyzing personal data from individuals. Pooled datasets allow quicker detection of trends and accurate targeting. For instance, in the healthcare sector, by collecting and analyzing large data sets of individual's health records and previous hospital visits, health care providers could make diagnostic predictions and treatment suggestions; an individual's personal locational data could be used for monitoring traffic and improving driving conditions on the road; banks can use Big Data techniques to improve fraud detection; insurers can make the process of applying for insurance easier by using valuable knowledge gleaned from pooled datasets. At the same time, the state processes personal data for a plethora of purposes, and is arguably its largest processor. In India, the state uses personal data for purposes such as the targeted delivery of social welfare benefits, effective planning and implementation of government schemes, counter-terrorism operations, etc. Such collection and use of data is usually backed by law, though in the context of counter-terrorism and intelligence gathering, it appears not to be the case. Thus, both the public and the private sector are collecting and using personal data at an unprecedented scale and for multifarious purposes. While data can be put to beneficial use, the unregulated and arbitrary use of data, especially personal data, has raised concerns regarding the privacy and autonomy of an individual. Some of the concerns relate to centralization of databases, profiling of individuals, increased surveillance and a consequent erosion of individual autonomy. This was also the subject matter of the landmark judgement of the Supreme Court in Puttaswamy, which recognized the right to privacy as a fundamental right. The Supreme Court stated that the "right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 of the Constitution and as a part of the freedoms guaranteed by Part III of the Constitution". Further, it went on to recognize informational privacy as a facet of the right to privacy and directed the Union Government to put in place a robust data protection regime to ensure protection against the dangers posed to an individual's privacy by state and non-state actors in the information age. In this light, to harness the benefits of the digital economy and mitigate the harms consequent to it, formulating a data protection law is the need of the hour for India.

Background studies

The 1970s witnessed increasing use of automated data systems containing personal information about individuals. To address concerns surrounding this, the Government of the United States appointed an Advisory Committee in the Department of Health, Education and Welfare (HEW Committee) to examine the various legal and technological issues raised visa-vis increasingly automated processing of data. The HEW Committee went on to issue a landmark report titled 'Records, Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems', which recommended that the United States Congress develop a Code of Fair Information Practices based on Fair Information Practices Principles (FIPPS). The FIPPS are a set of principles which prescribe how data should be handled, stored and managed to maintain fairness, privacy and security in a rapidly growing global technology environment. FIPPS are now deemed to be the bedrock of modern data protection laws across the world. The FIPPS were soon followed by the Organization for Economic Cooperation and Development Privacy Guidelines (OECD Guidelines) in the 1980s [1]. The OECD Guidelines were significantly inspired by the FIPPS and were intended to provide a framework for harmonizing national privacy legislations amongst OECD members, while upholding human rights, and preventing interruptions in international flows of data. The OECD Guidelines are deemed to be the first internationally agreed upon statement of core information privacy principles and have considerably influenced data protection frameworks around the world. The OECD Guidelines [2] have inspired multiple data protection frameworks such as the European Directive 95/46/EC on the processing of personal data and the free movement of such data (Data Protection Directive), the 2004 Asia-Pacific Economic Cooperation Framework (APEC Framework) as well as data protection legislations such as the Australia's Privacy Act, 1988 (Privacy Act), New Zealand's Privacy Act, 1993 and Japan's Protection of Personal Information Act, 2003.42 However, despite the popularity that traditional privacy principles have enjoyed, they have come under considerable scrutiny in recent times. It has been argued that traditional privacy principles may not be well-suited to address the challenges posed by the dramatic increase in the volume and use of personal data, advances in computing, and global flows of data. Because of these concerns, an expert group was constituted to revise and modernize the OECD Guidelines. The OECD Guidelines as updated in 2013 (2013 OECD Guidelines) are the product of this attempt. While the 2013 OECD Guidelines keep the core privacy principles such as collection limitation, data quality and purpose specification etc. intact, several new elements to strengthen data safeguards have been introduced. These include: privacy management programs to enhance accountability of the data controller, data security breach notification45 which oblige data controllers inform individuals/authorities of a security breach and establishment and maintenance of privacy enforcement authorities.46 further cross-border flows of data and international cooperation to improve global interoperability of privacy frameworks have been recognized as essential for a global data economy. The 2013 OECD Guidelines have been criticized as being fundamentally incompatible with modern technologies and Big Data analytics which have revolutionized how data is collected and processed.49 presently, corporations possess data that has been generated or collected from a wide variety of sources. Such data may include financial data, employee data and customer data. It may be relevant to note that at the time when these guidelines originated, data processing, including collection activities were more linear and easier to define. However, now the situation has changed with data being collected and used in ways not envisaged at the time these principles were developed. We have, as a consequence, been ushered into the era of modern technologies and Big Data analytics. While Big Data does not have a precise definition, it can be understood as essentially involving gathering large quantities of data and

applying innovative technology (such as predictive analysis) to them to extract knowledge. Big Data is usually characterized by 3 Vs, namely 'volume' as in massive datasets, 'velocity' which relates to real time data, and 'variety' which relates to different sources of data. Other technological developments such as artificial intelligence, machine learning, the Internet of Things54 are all part of the Big Data ecosystem and their use is becoming increasingly commonplace. In light of these developments, the biggest challenge in regulating emerging technologies such as Big Data, artificial intelligence and the Internet of Things, lies in the fact that they may operate outside the framework of traditional privacy principles. These principles, as they were originally envisaged, were designed to protect a single static data set. Thus, it was possible to limit the collection of data to satisfy a particular purpose. However, this limited activity may no longer hold true with respect to current data processing activities. For instance, given that Big Data involves the processing of large data sets, usually the source of such data may not be directly from the individual, and consent may not be as relevant. Further, data may be generated as a by-product of a transaction or obtained by a service provider in return for a free service (such as free email accounts, social networks etc.) or obtained as a consequence of accessing a service (such as use of GPS navigation), and it may not be possible to specify the purpose for which personal data is collected at the time of collection.

Advent of new technologies and challenges

The advent of such technologies has also expanded the very definition of personal data. For instance, analyzing meta-data such as a set of predictive or aggregated findings, or by combining previously discrete sets of data, Big Data has radically expanded the range of personally identifiable data.57 Data which is viewed as non-personal information can now be combined with other data sets to create personally identifiable information. An example of this is how anonymized Netflix data on ranking of films could be easily combined with other data sets such as timestamps with public information from the Internet Movie Database (IMDb) to de-anonymize the original data set and reveal personal movie choices. Similarly, Big Data relies on accumulation of large volumes of data to extract knowledge from them, making it difficult to apply the principle of data minimization. [3] Additionally, technologies such as the Internet of Things relies on continuous collection of personal information from the users of "smart devices", which may then be interpreted to provide unique services. Therefore, in such instances as well, it may be difficult to adhere to the traditional privacy principles of consent, collection and use limitation. Given the dynamic pace of development of emerging technologies, alternatives to traditional privacy principles have thus been suggested that require careful scrutiny. Since technologies such as Big Data, the Internet of Things and Artificial Intelligence are here to stay and hold out the promise of welfare and innovation, India will have to develop a data protection law which can successfully address the issues relating to these technologies, so as to ensure a balance between innovation and privacy. Whether this involves a reiteration of traditional privacy principles, an alternative approach based on newer ex ante forms of regulation or a hybrid model, will have to be determined carefully.

Development in India for Data Protection

Drafting a data protection law for India is not a greenfield exercise. Though piecemeal, several legislative developments and judicial pronouncements are relevant for determining the contours of such a law.

1. Right to Privacy (Judicial Development)

The Supreme Court in Puttaswamy overruled its previous judgments of M.P. Sharma v.Satish Chandra (M.P. Sharma) and Kharak Singh *v.* State of Uttar Pradesh (Kharak Singh) which appeared to observe that there was no fundamental right to privacy enshrined in the Constitution of India. By doing so, it upheld several precedents following Kharak Singh, which had recognized a right to privacy flowing from Article 21 of the Constitution of India. The Supreme Court in M.P. Sharma examined whether the constitutionality of search and seizure of documents pursuant to a FIR would violate the right to privacy. A majority decision by an eight-judge Constitution bench observed that the right to privacy was not a fundamental right under the Constitution. Subsequently, in Kharak Singh, the issue at hand was whether regular surveillance by police authorities amounted to an infringement of constitutionally guaranteed fundamental rights [4]. A Constitution bench of six judges analyzed this issue in the backdrop of the validity of the regulations governing the Uttar Pradesh police which legalized secret picketing, domiciliary visits at night and regular surveillance., The Supreme Court struck down night-time domiciliary visits by the police as violative of 'ordered liberty'.109 Further, the Supreme Court held that Article 21 of the Constitution of India is the repository of residuary personal rights and it recognized the common law right to privacy. However, the Court observed that privacy is not a guaranteed fundamental right. It must be noted though, dissenting judge, Justice Subba Rao, opined that even though the right to privacy was not expressly recognized as a fundamental right, it was an essential ingredient of personal liberty under Article 21 and thus fundamental. Following this approach of Justice Subba Rao, the nine-judge bench of the Supreme Court in Puttaswamy recognized the right to privacy as an intrinsic part of the fundamental right to life and personal liberty under Article 21 of the Constitution of India, and in all fundamental rights in Part III which protect freedoms in general, and overruled the aforementioned judgments to this extent. Notably, it was held that the Constitution of India must evolve with the circumstances of time to meet the challenges thrown up in a democratic order governed by the rule of law and that the meaning of the Constitution of India cannot be frozen on the perspectives present when it was adopted. The right to privacy was grounded in rights to freedom under both Article 21 and Article 19 of the Constitution of India encompassing freedom of the body as well as the mind. It was held that "privacy facilitates freedom and is intrinsic to the exercise of liberty"111 and examples of the freedoms enshrined under Article 25, Article 26 and Article 28(3) of the Constitution of India were given to show how the right to privacy was necessary to exercise all the rights. The approach of the

Supreme Court in Kharak Singh and A.K. Gopalan *v.* State of Madras of putting the freedoms given under Part III of the Constitution of India under distinct compartments was also rejected. Instead, it was held that that these rights are overlapping and the restriction of one freedom affects the other, as was also held previously in the Maneka and Cooper judgments. Therefore, a law restricting a freedom under Article 21 of the Constitution of India would also have to meet the reasonableness requirements under Article 19 and Article 14 of the Constitution of India.

2. Data Protection and Indian Legislative

Though the *Puttaswamy* judgment is a landmark legal development in the discourse on privacy, especially informational privacy; prior legislative attempts have been made to secure informational privacy in various sectors in India. These includes the general data protection rules under the Information Technology Act, 2000 (IT Act) as well as various sector specific laws on data protection.

a) The Information Technology (Reasonable Security Practices and Sensitive Personal Data or Information) Rules, 2011 (SPDI Rules)

b) The Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016 (Aadhaar Act)

Data Protection Approaches in Different countries regions

In determining, India's approach to data protection, it will be instructive to look at practices followed in other jurisdictions, particularly recent models that have emerged. A perusal of foreign jurisdictions demonstrates that there are two distinct models in the field of data protection. The European Union or EU model and others like it, provide for a comprehensive data protection law couched in the rights based approach; and the American marketplace model has sector specific data protection laws. This is because of the distinct conceptual basis for privacy in each jurisdiction. The two approaches towards data protection are discussed briefly below.

European Union

In EU, the right to privacy is a fundamental right which seeks to protect an individual's dignity. The European Charter of Fundamental Rights (EU Charter) recognizes the right to privacy as well as the right to protection of personal data, in Article 7 and Article 8, respectively. The first principal EU legal instrument on data protection was the Data Protection Directive. The Data Protection Directive has been significantly inspired by the OECD Guidelines,68 and sought to achieve a uniformly high level of data protection in the EU by harmonizing data protection legislations to ensure that free flow of data was not impeded. The Data Protection Directive was eventually adopted as national legislations by EU Member States. Given that it was a non-binding instrument, it left some room for interpretation. The rapidly changing data landscape led the EU to update its regulatory environment on data protection. The product of this process is the EU General Data Protection Regulation of 2016 (EU GDPR). The EU GDPR is one of the most stringent data protection laws in the world72 and being a regulation, it will become immediately enforceable as law in all Member States. However, given the ambitious changes it envisages, Member States have been given two years (till 25 May 2018) to align their laws to the EU GDPR. The EU GDPR is a comprehensive data protection framework which applies to processing of personal data by any means, and to processing activities carried out by both the Government as well as the private entities, although there are certain exemptions such as national security, defense, public security, etc. Similarly, it continues to recognize and enforce the core data protection principles recognized in the OECD Guidelines. The EU GDPR follows a right based approach towards data protection, and places the individual at the center of the law. As a consequence, it imposes extensive control over the processing of personal data both at the time of, and after the data has been collected. Further, collection of certain forms of personal data, known as sensitive personal data (such as racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning health and sex life) is prohibited subject to certain exceptions. Thus, for processing to be lawful and fair, the entity collecting personal data must comply with an extensive range of principles such as that of purpose specification, data minimization, data quality, security safeguards, etc.

EU General Data Protection Regulation (GDPR)

Purpose: To enable the free movement of personal data within the Union while protecting fundamental rights and freedoms of natural persons and, in particular, their right to the protection of personal data.

Material Scope: Applies to the processing of personal data wholly or partly by automated means, within the scope of Union law.

Territorial Scope: Applies to processing that takes place in the Union or by a processor who has an establishment in the Union within the context of activities in the Union or to processing activities that are related to the offering of goods and services to (or behavioral monitoring of) data subjects in the Union.

Personal Data: Personal data means any information relating to an identified or identifiable natural person.

Sensitive Personal: Special categories of data that are considered particularly sensitive are personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Data Controller: Means the natural or legal person, public authority, agency or other body, which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Data Processor: Means a natural or legal person, public authority, agency or other body that processes personal data on behalf of the controller.

Purpose Limitation: Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

Accuracy: Personal data should be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, is erased or rectified without delay. Personal data should be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

Accountability: The controller shall be responsible for and be able to demonstrate compliance with the principles of the processing of personal data under the GDPR. The controller and the processor shall designate a data protection officer where processing requires regular and systematic monitoring of data subjects on a large scale or the core activities of the controller or the processor consist of processing on a large scale of special (sensitive) categories of data or personal data relating to criminal convictions and offenses [6].

Access and Correction: The data subject has the right to obtain from the controller confirmation as to whether or not personal data concerning them are being processed, and to access the personal data and information about the processing, including what categories of data are processed, the recipients of the data, and rights to erasure and rectification of the personal data, the right to lodge a complaint with a DPA, the source of the data, whether the data was subject to automated profiling (and if so, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject).

Transfer of Personal Data to Another country: Personal data may only be transferred to third countries where the EU has considered the laws to provide adequate protection or where protected by binding corporate rules, approved model clauses, binding agreements combined with an approved code of conduct or approved certification [7].

United States

In the US, there is no single, comprehensive federal (national) law regulating the collection and use of personal data. However, each Congressional term brings proposals to standardise laws at a federal level. Instead, the US has a patchwork system of federal and state laws and regulations that can sometimes overlap, dovetail and contradict one another. In addition, there are many guidelines, developed by governmental agencies and industry groups that do not have the force of law, but are part of self-regulatory guidelines and frameworks that are considered "best practices". These self-regulatory frameworks have accountability and enforcement components that are increasingly being used as a tool for enforcement by regulators [5].

In the US, privacy protection is essentially a “liberty protection” i.e. protection of the personal space from government.94 Thus, the American understanding of the “right to be let alone” has come to represent a desire for as little government intrusion as possible. 95 While there is no provision in the US Constitution that explicitly grants a right to privacy, the right in a limited form is reflected in the Fourth Amendment to the US Constitution – the right against unreasonable searches and seizures. US courts however, have collectively recognized a right to privacy by piecing together the limited privacy protections reflected in the First, Fourth, Fifth and Fourteenth Amendments to the US Constitution. In addition to the distinction in the conceptual basis of privacy, the US approach towards privacy and data protection varies from the EU in multiple respects. First, unlike the EU, there is no comprehensive set of privacy rights/principles that collectively address the use, collection and disclosure of data in the US. Instead, there is limited sector specific regulation. Second, the approach towards data protection varies for the public and private sector. The activities and powers of the Government vis-à-vis personal information are well defined and addressed by broad, sweeping legislations99 such as the Privacy Act, 1974 which is based on the FIPPS (governing collection of data by the federal government); the Electronic Communications Privacy Act, 1986; the Right to Financial Privacy Act, 1978, etc. For the private sector, which is not governed by these legislations, certain sector-specific norms exist. These include: The Federal Trade Commission Act (FTC Act), The Financial Services Modernization Act (Gramm-Leach-Bliley Act or the GLB Act), The Health Insurance Portability and Accountability Act (HIPAA), and the Children's Online Privacy Protection Act (COPPA) etc. In addition, States have their own data protection laws [8].

Japan

Japan's reformed privacy law came into full force May 30, 2017. Along with a significant number of changes, the new law also introduced a similar white-list concept. The mutual recognition will add Japan to EU's white list and make the EU Japan's first "white listed" jurisdiction. Even so, there remains a large number of differences between the privacy laws of the EU and Japan. However, particularly with Japan's recent reforms, the significance of the differences is less. In particular, the establishment of the Personal Information Protection Commission in Japan, which is dedicated to the establishment and enforcement of privacy regulations, significantly enhances Japan's privacy law system [9].

Japanese Act on Protection of Personal Information (APPI)

Purpose: To protect the rights and interests of individuals while ensuring due consideration for the usefulness of personal information by basic principles for the proper handling of personal information.

Material Scope: Applies to the use of a personal information for business. The APPI has a very broad and open concept of data processing [10].

Territorial Scope: The APPI does not have express provisions dealing with jurisdiction and territoriality.

Personal Data: "Personal Information" means the following two categories of information.

1. Information about a living individual which can identify a specific individual by the description contained in the information, such as name, date of birth or other description (including voice or behavior information), including information which can easily be combined with other information so as to enable the identification of that individual; and
2. Information that contains Personal Identifier Codes. "Personal Identifier Codes" means either (a) letters, numbers, marks or other codes for use with computers converted from a person's bodily information which may identify the person, or (b) letters, numbers, marks or other codes on cards or other documents which are unique to the user or purchaser and may identify the person. Apart from "Personal Information", "Personal Data" is separately defined to cover information stored in a business operator's database. Personal Data is defined as Personal Information constituting the business operator's "Personal Information Database". A "Personal Information Database" in turn is defined as: (i) an assembly of information systematically arranged in such a way that specific personal information can be retrieved by a computer; or (ii) an assembly of information in accordance with certain rules, and that has a table of contents, index or other means to facilitate the retrieval. Accordingly, once "Personal Information" is stored into a "Personal Information Database", such Personal Information becomes "Personal Data" under the APPI. There are some provisions in the APPI that specifically deal with Personal Data.

Sensitive Personal: Personal Information that needs special care ("Sensitive Data") is defined to include race, religion, social status medical history, criminal history and the fact that the person suffered damages by a crime.

Data Controller: There is no concept of a "Data Controller" under Japanese law. However, the APPI uses the term "business operator," which essentially refers to the entity responsible for the proper handling of all "Personal Information." This is similar to the concept of data controller under EU law.

Data Processor: There is no concept of a "Data Processor" under Japanese law. As such, handling of personal data under the APPI should pertain to how a "business operator" treats and manages the personal information or personal data in its possession.

Purpose Limitation: A business operator handling personal information shall not handle personal information beyond the scope necessary for achieving the purpose of use unless the business operator has obtained prior consent of data subjects. Purpose of use must promptly be notified to data subjects or publicly announced once a business operator acquires Personal Information unless the purpose of use has already publicly announced.

Accuracy: A business operator handling personal information must endeavor to keep the content of personal data accurate and up to date, within the scope necessary for achieving the purpose of use.

Accountability: Japan does not recognize the concept of a data processor. Accountability lies with the business operator, which is like a data controller under EU law. In the next section we shall discuss briefly on the issues of actions and corrections so far as Japanese laws and policy is concerned.

Access and Correction: The data subject may request the business operator to disclose, correct, add or delete the retained personal data.

Transfer of Personal Data to Another country: The APPI provides that Personal Data may not be transferred to a foreign country unless: (i) the data subject has given specific advance consent to the transfer of the data subject's Personal Data to the entity in a foreign country; (ii) the country in which the recipient is located has a legal system that is deemed equivalent to the Japanese personal data protection system, designated by the Japanese data protection authority; or (iii) the recipient undertakes adequate precautionary measures for the protection of Personal Data, as specified by the Japanese data protection authority.

Singapore

What is Personal Data?

Personal data refers to data, whether true or not, about an individual who can be identified from that data; or from that data and other information to which the organization has or is likely to have access. Personal data in Singapore is protected under the Personal Data Protection Act 2012 (PDPA).

What is the Personal Data Protection Act (PDPA)?

The PDPA establishes a data protection law that comprises various rules governing the collection, use, disclosure and care of personal data. It recognizes both the rights of individuals to protect their personal data, including rights of access and correction, and the needs of organizations to collect, use or disclose personal data for legitimate and reasonable purposes. The PDPA provides for the establishment of a national Do Not Call (DNC) Registry. The DNC Registry allows individuals to register their Singapore telephone numbers to opt out of receiving marketing phone calls, mobile text messages such as SMS or MMS, and faxes from organizations.

Objectives of the Personal Data Protection Act

Today, vast amounts of personal data are collected, used and even transferred to third party organizations for a variety of reasons. This trend is expected to grow exponentially as the processing and analysis of large amounts of personal data becomes possible with increasingly sophisticated technology. With such a trend comes growing concerns from individuals about how their personal data is being used. Hence, a data protection regime to govern the collection, use and disclosure of personal data is necessary to address these concerns and to

maintain individuals' trust in organizations that manage data. By regulating the flow of personal data among organizations, the PDPA also aims to strengthen and entrench Singapore's competitiveness and position as a trusted, world-class hub for businesses.

How does the Personal Data Protection Act Work?

The PDPA will ensure a baseline standard of protection for personal data across the economy by complementing sector-specific legislative and regulatory frameworks. This means that organizations will have to comply with the PDPA as well as the common law and other relevant laws that are applied to the specific industry that they belong to, when handling personal data in their possession.

The PDPA considers the following concepts

Consent – Organizations may collect, use or disclose personal data only with the individual's knowledge and consent (with some exceptions);

Purpose – Organizations may collect, use or disclose personal data in an appropriate manner for the circumstances, and only if they have informed the individual of purposes for the collection, use or disclosure; and

Reasonableness – Organizations may collect, use or disclose personal data only for purposes that would be considered appropriate to a reasonable person in the given circumstances.

Application of the Personal Data Protection Act

The PDPA covers personal data stored in electronic and non-electronic forms. The data protection provisions in the PDPA (parts III to VI) generally do not apply to:

a) Any individual acting in a personal or domestic basis.
b) Any employee acting in the course of his or her employment with an organization.
c) Any public agency or an organization in the course of acting on behalf of a public agency in relation to the collection, use or disclosure of the personal data. You may wish to refer to the Personal Data Protection (Statutory Bodies) Notification 2013 for the list of specified public agencies.
d) Business contact information. This refers to an individual's name, position name or title, business telephone number, business address, business electronic mail address or business fax number and any other similar information about the individual, not provided by the individual solely for his or her personal purposes.

These rules are intended to be the baseline law which operates as part of the law of Singapore. It does not supersede existing statutes, such as the Banking Act and Insurance Act but will work in conjunction with them and the common law.

When did the Personal Data Protection Act Come into Effect?

The PDPA took effect in phases starting with the provisions relating to the formation of the PDPC on 2 January 2013. Provisions relating to the DNC Registry came into effect on 2 January 2014 and the main data protection rules on 2 July 2014. This allowed time for organizations to review and adopt internal personal data protection policies and practices, to help them comply with the PDPA.

Development of the Personal Data Protection Act

In the development of this law, references were made to the data protection regimes of key jurisdictions that have established comprehensive data protection laws, including the EU, UK, Canada, Hong Kong, Australia and New Zealand, as well as the OECD Guidelines on the Protection of Privacy and Trans border Flow of Personal Data, and the APEC Privacy Framework. These references are helpful for the formulation of a regime for Singapore that is relevant to the needs of individuals and organizations, and takes into account international best practices on data protection.

Three public consultations were conducted since 2011 to seek feedback on the proposed data protection regime. The public consultation sought the public's views on topics including the coverage of the proposed law, the proposed data management rules and transitional arrangements for organizations to comply with the new law [11].

South Africa (The Protection of Personal Information Act, 2013)

The POPI Act defines processing as any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including; the collection, receipt, recording, organization, collation, storage, updating or modification, retrieval, alteration, consultation, dissemination by means of transmission, distribution or making available in any other form, merging, linking, restriction, degradation, erasure or destruction of information. In these legislations, the lawfulness of actions relating to data is set out with reference to the term processing. In other words, these statutes do not prescribe separate standards or limitations on different actions relating to data, for instance such as collection, use or disclosure. Example, the EU GDPR in Article 6 lays down the conditions for lawful processing. These conditions apply across the board any action involving data such as collection, use or disclosure [12].

OECD Guidelines

The Organisation for Economic Co-operation and Development (OECD; French: Organisation de coopération et de développement économiques, OCDE) is an intergovernmental economic organisation with 35-member countries, founded in 1960 to stimulate economic progress and world trade. In 1980, in an effort to create a comprehensive data protection system throughout Europe, the Organization for Economic Cooperation and Development (OECD) issued its "Recommendations of the Council Concerning Guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data". The seven principles governing the OECD's recommendations for protection of personal data were:

a) Notice: Data subjects should be given notice when their data is being collected;
b) Purpose: Data should only be used for the purpose stated and not for any other purposes;
c) Consent: Data should not be disclosed without the data subject's consent;

d) Security: Collected data should be kept secure from any potential abuses;
e) Disclosure: Data subjects should be informed as to who is collecting their data;
f) Access: Data subjects should be allowed to access their data and make corrections to any inaccurate data; and
g) Accountability: Data subjects should have a method available to them to hold data collectors accountable for not following the above principles.

Conclusion

The OECD Guidelines, however, were nonbinding, and data privacy laws still varied widely across Europe. The United States, meanwhile, while endorsing the OECD's recommendations, did nothing to implement them within the United States. However, all seven principles were incorporated into the EU Directive. The OECD Guidelines have inspired multiple data protection frameworks such as the European Directive 95/46/EC on the processing of personal data and the free movement of such data (Data Protection Directive), the 2004 Asia-Pacific Economic Cooperation Framework (APEC Framework) as well as data protection legislations such as the Australia's Privacy Act, 1988 (Privacy Act), New Zealand's Privacy Act, 1993 and Japan's Protection of Personal Information Act, 2003. However, despite the popularity that traditional privacy principles have enjoyed, they have come under considerable scrutiny in recent times. It has been argued that traditional privacy principles may not be well-suited to address the challenges posed by the dramatic increase in the volume and use of personal data, advances in computing, and global flows of data. As a consequence of these concerns, an expert group was constituted to revise and modernize the OECD Guidelines. The OECD Guidelines as updated in 2013 (2013 OECD Guidelines) are the product of this attempt. While the 2013 OECD Guidelines keep the core privacy principles such as collection limitation, data quality and purpose specification etc. intact, several new elements to strengthen data safeguards have been introduced. These include: privacy management programs to enhance accountability of the data controller, data security breach notification.

References

1. OECD, OECD Guidelines on the Protection of Privacy and Trans border Flows of Personal Data. 2013.
2. OECD, Thirty Years After The OECD Privacy Guidelines. 2011.
3. Fred H Cate. Failure of Fair Information Principles, in Consumer Protection in the Age of Information Economy, Jane K. Winn *ed*, Routledge, 2006.
4. Privacy management programmes are intended be integrated in the governance structure of a data controller and establish appropriate internal oversight mechanisms to ensure data is safeguarded Organization for Economic Co-operation and Development, Thirty Years After The OECD Privacy Guidelines. 2011.
5. Jeffrey Rosen, The Unwanted Gaze The Destruction of Privacy in America Random House, 2000.
6. Neil M Richards. The Dangers of Surveillance, Harvard Law Review 2013; 126(7):1934-1950.
7. Helen Nissenbaum. Privacy as Contextual Integrity, 79 Washington Law Review. 2004; 119.
8. Daniel Solove. Conceptualizing Privacy, California Law Review 2002; 90(4):1088-89, 1100-02, 1112-13, 1130-31.
9. Lee Bygrave. Data Protection Law Approaching Its Rationale, Logic, and Limits' 2 Kluwer Law International The Hague/London/New York, 2002.
10. See definition of processing' under Article of the EU General Data Protection Regulation, (Regulation (EU) 2016/679). 2016; 4(2).
11. Jerry Kang. Information Privacy in Cyberspace Transactions, 50 Stanford Law Review 1998; 1193, 1202-03.
12. Maria Tzanou. Data protection as a fundamental right next to privacy? Reconstructing a not so new right, International Data Privacy Law 88. 2013; 3(2).