PART II
SCOPE AND EXEMPTIONS

CHAPTER 1: TERRITORIAL AND PERSONAL SCOPE

1.1. Introduction

The borderless nature of the Internet raises several jurisdictional issues in data protection. A single act of processing of personal data could very easily occur across multiple jurisdictions. Traditional principles of sovereignty and territorial jurisdiction have evolved in circumstances where such cross-border actions were uncommon. As such, it is not easy to determine the kind of application clause which a data protection legislation must have.

The power of a State to prescribe and enforce its laws is governed by the rules of jurisdiction in international law. Broadly, the territory of a State is where its jurisdiction ends and States are prohibited from exercising jurisdiction in the territory of another State, unless so permitted under a treaty or customary law.[176] Thus, for instance, a State in whose territory a crime occurs has jurisdiction to deal with the crime. While the principle of territoriality ordinarily connotes jurisdiction of a State over an act committed within its territory, under the principle of objective territoriality, jurisdiction can be exercised over acts which take place outside the State but have consequences within the State. A common illustration is that of a gun being fired in one country causing a death in across the border in another State. [177]

In addition to these general rules, there are certain circumstances in which extraterritorial action may be permissible under other rules. Under the nationality principle, a State may claim jurisdiction over actions of its nationals even on foreign territory.[178] Conversely, under the passive personality principle, a State may exercise jurisdiction over actions which affect its nationals, no matter where the act has occurred. The application of this principle is contested.[179]

1.2. Issues

The frequency of cross border actions on the Internet might require some thinking outside the framework of these principles.[180] A legislation which adheres to any strict notion of territoriality will fail to adequately protect Indian residents and citizens as a large number of actions which the State may have a legitimate interest in regulating will fall outside the scope

[176] "S.S. Lotus" (*France v. Turkey*), 1927 PCIJ (SER.a) No. 10., available at: http://www.icj-cij.org/files/permanent-court-of-international-justice/serie_A/A_10/30_Lotus_Arret.pdf, (last accessed 1 November 2017).
[177] Crawford, Brownlie's Principles of International Law', 456 (Oxford, 8th Ed, 2008).
[178] Crawford, Brownlie's Principles of International Law, 457 (Oxford, 8th Ed, 2008).
[179] Crawford, Brownlie's Principles of International Law, 458 (Oxford, 8th Ed, 2008),.
[180] Dan Jerker B. Svantesson, 'Extraterritoriality in the context of Data Privacy Regulation', 7(1) Masaryk University Journal of Law and Technology 87 (2012); Christopher Kuner, 'Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law', University of Cambridge Faculty of Law Research Paper No. 49/2015 (30 August 2015).

of the law. Second, the ease of cross border transactions on the Internet means that foreign parties can effectively transact in India without having any office or establishment in India while ostensibly maintaining their status as entities not subject to the jurisdiction of Indian law. The nature of cloud data as a location-independent, mobile asset also poses similar jurisdictional difficulties.[181]

On the other hand, every act on the Internet which has a local dimension cannot be regulated by a State. In some cases, the link between the State and the actor will be so tenuous that the State would not be justified in exercising jurisdiction over the foreign party. For instance, the fact that a foreign website can be accessed in India would not by itself furnish a ground for subjecting that website to Indian law. Such a law might have the undesired effect of legislating to govern the entire Internet.[182]

The question of jurisdiction is not one of prescription alone. The power to prescribe laws is merely one aspect of jurisdiction. In the context of data protection, jurisdiction must be considered from the perspective of investigative powers, the exercise of judicial power and enforcement of laws. The last of these factors, enforceability can serve as a key objective determinant of the extent of applicability of the law.[183]

1.3. International Practices

Faced with these issues, several jurisdictions have responded by making laws which have considerable extraterritorial and personal scope.[184]

European Union

Article 3 of the EU GDPR sets out the territorial scope of the said regulation. Clause (1) states that the regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or processor in the Union. Clause (2) widens the reach of the regulation by making it applicable to processing of personal data of data subjects who are in EU by controllers and processors outside the EU, if the processing activities are related to the offering of goods and services to persons in the EU or if the behaviour of such persons in the EU is monitored by such activities. While the first clause incorporates the territorial principle as in the earlier Data Protection Directive, the newer rules in clause (2) incorporate the principles of passive personality and objective territoriality with the intent of

[181] For a consideration of the issue adopting a contrary view, *See* Andrew Keane Woods, 'Against Data Exceptionalism', 68(4) Stanford Law Review 729 (April 2016).

[182] *Bodil Lindqvist v. Åklagarkammaren i Jönköping*, Case C-101/01 (2003), European Court of Justice, the Court noted: 'If Article 25 of Directive 95/46 were interpreted to mean that there is 'transfer [of data] to a third country' every time that personal data are loaded onto an Internet page, that transfer would necessarily be a transfer to all the third countries where there are the technical means needed to access the Internet. The special regime provided for by Chapter IV of the directive would thus necessarily become a regime of general application, as regards operations on the Internet.'

[183] Christopher Kuner, 'Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law', University of Cambridge Faculty of Law Research Paper No. 49/2015, 16 (30 August 2015).

[184] Dan Jerker B Svantesson, 'A Layered Approach To The Extraterritoriality Of Data Privacy Laws', 3(4) International Data Privacy Law Review 278 (November 2013).

protecting the privacy of EU residents against cross border action.[185] The exact extent of the new rules of jurisdiction under the EU GDPR are not yet clear, particularly the clause on tracking the behaviour of EU residents. For instance, use of persistent cookies or IP address logs (along with some other data) could result in the monitoring of online behaviour of residents.[186]

The territorial principle in clause (1), on its own, has a significantly wide reach. In the case of *Google Spain*,[187] the argument that processing of data by Google Inc (based in the US) for operating Google Search was not subject to EU law was rejected by the European Court of Justice. The Court held that this processing was in the context of the activities of Google Spain, an establishment in the EU despite the fact that it was only operating in the area of advertising.

Australia

Australia adopts a different approach by prescribing two tests to determine whether the Privacy Act applies to an organisation.[188] First, the Privacy Act applies to all Australian organisations, such as companies or trusts incorporated in Australia irrespective of where personal data is collected by such organisations. Second, in respect of organisations and operators not constituted in Australia, they are subject to the jurisdiction of Australian courts if they have an Australian link. An organisation has an Australian link if it carries on business in Australia and the personal data has been collected or held in Australia. The phrase "carries on business in Australia" has not been defined and the Office of the Australian Information Commission (OAIC) has suggested that the application of the Act is to be guided by judicial interpretation in this regard.[189] Consistent and regular activity in Australia with the aim of profit has been held to be carrying on business in Australia.[190]

Singapore

The data protection legislation of Singapore (the Singapore Personal Data Protection Act, 2012 or the Singapore Act) does not explicitly set out its territorial jurisdiction. However, the Singapore Act includes any individual, company, association or body of persons, corporate or unincorporated, whether or not, formed or recognised under the law of Singapore, and whether or not resident, or having an office or a place of business, in Singapore within the

[185] Dan Jerker B. Svantesson, 'Extraterritoriality in the context of Data Privacy Regulation', 7(1) Masaryk University Journal of Law and Technology 87 (2012).
[186] 'New Rules, Wider Reach: The Extraterritorial Scope of the GDPR', Slaughter and May (June 2016), available at: https://www.slaughterandmay.com/media/2535540/new-rules-wider-reach-the-extraterritorial-scope-of-the-gdpr.pdf, (last accessed 31 October 2017).
[187] *Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, Case C131/12, (2014), European Court of Justice.
[188] Section 5 B, Privacy Act.
[189] OAIC, 'APP Guidelines- Key Concepts' (March 2015), available at: https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-b-key-concepts#australian-link, (last accessed 1 November 2017).
[190] OAIC, 'APP Guidelines- Key Concepts' (March 2015), available at: https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-b-key-concepts#australian-link, (last accessed 1 November 2017).

ambit of the term organisation.[191] This may well be construed to be an indirect claim of jurisdiction over foreign entities as well.

South Africa

The Protection of Personal Information Act, 2013 (POPI Act) of South Africa applies to processing of personal information by parties domiciled in South Africa or where parties not domiciled in South Africa, use automated or non-automated means within the territory of South Africa.[192]

Canada

The experience of Canada in applying the PIPEDA is also instructive. Section 4 of the PIPEDA is silent on extraterritorial jurisdiction. Canadian courts have interpreted this silence to mean that there is no bar on applying the PIPEDA to foreign entities in all circumstances where there is a real and substantial link to Canada.[193]

From these practices it is clear that in area of data protection, claims of jurisdiction under the exceptions to the territoriality norm, such as passive personality are commonly found in statutes. Vulnerability to harm arising from action which may not be strictly within territorial jurisdiction is perhaps the reason why most jurisdictions have clauses which permit such extraterritorial jurisdiction or jurisdiction over foreign entities as the case may be.

1.4. Enforceability of provisions of laws

Prescribing provisions that depart from ordinary principles of territoriality may not by themselves be sufficient to ensure that the interests of a State in protecting the personal data of its residents are secured. In several cases, foreign entities have expressed reluctance to comply with orders of courts or directions of governments to comply with local laws. A common plea in such cases is that it is only the local arm (of a multinational corporation) that is answerable to the concerned jurisdiction. The primary method of enforcing jurisdictional claims against foreign entities remains the cumbersome processes of letters rogatory or through Mutual Legal Assistance Treaties.[194] There are suggestions that restricting access to markets may be a method of dealing with such issues.[195] For instance, a Brazilian Court in 2013 ordered that all Facebook IP domains be blocked for failure to remove offending content on the ground that it was the responsibility of entities incorporated in other jurisdictions.[196] A more acceptable approach may perhaps be to adopt penalties of the nature

[191] Section 2, Singapore Act.
[192] Section 3, POPI Act.
[193] *A.T. v. Globe24h.com 2017*, FC 114 (CanLII), available at: https://www.canlii.org/en/ca/fct/doc/2017/2017fc114/2017fc114.html, (last accessed 2 November 2017).
[194] Andrew Keane Woods, 'Against Data Exceptionalism', 68(4) Stanford Law Review 729, 748 (April 2016).
[195] Dan Jerker B. Svantesson, 'Extraterritoriality in the context of Data Privacy Regulation', 7(1) Masaryk University Journal of Law and Technology 87,138 (2012).
[196] Dan Jerker B. Svantesson, 'Extraterritoriality in the context of Data Privacy Regulation', 7(1) Masaryk University Journal of Law and Technology 87,138 (2012).

the EU GDPR prescribes based on global turnover.[197] Such fines as deterrents may coax global corporations into complying with local laws wherever they have a presence. Further, a failure to pay fines or to comply with any other sanctions imposed by the law could be linked to an order restricting market access.[198] In addition, other measures such as mandatory establishment of a representative office (for ensuring criminal law enforcement) and holding the Indian subsidiary/related entity liable for civil penalties or damages may be explored.

1.5. Provisional Views

1. The primary test for applicability of law may be processing of personal information which takes place in the territory of India by entities which have a presence in India. The term processing involves any action with respect to data including collection, use or disclosure of data. The clause would then cover individuals in India, companies and other juristic entities which have an establishment in India which process data.

2. However, it may be necessary to make the law applicable to all kinds of processing which the State may have a legitimate interest in regulating 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.

3. Carrying on a business, or offering of services or goods in India are parameters worth incorporating in the law in light of international practices. Thus, an entity which does not have a presence in India but offers a good or service to Indian residents over the Internet, or carries on business in India may be covered under the law.

4. It may also be worthwhile considering making the law applicable to any entity, no matter where they may be located that process personal data of Indian citizens or residents. This partially adopts the new EU GDPR formulation and puts the data subject squarely at the centre of the legislation, ensuring that the law is made applicable to anyone who would processes personal data of the data subject.

5. The extent of jurisdiction may not be so wide as to constitute an unnecessary interference with the jurisdiction of other states or have the effect of making the law a general law of the Internet. For instance, the mere fact that a website (operated from abroad) is accessible from India should not be a reason for subjecting the website to Indian law.

1.6. Questions

[197] Article 83, EU GDPR.

[198] Temporary dismissal of activities is permissible administrative sanction under Indonesian Law, See - Denny Rahmansyah and Saprita Tahir, 'Data protection in Indonesia: Overview', Thomas Reuters Practical Law (1 October 2017), available at: https://content.next.westlaw.com/Document/Ic7ba28fe5f0811e498db8b09b4f043e0/View/FullText.html?contextData=(sc.Default)&transitionType=Default&firstPage=true&bhcp=1, (last accessed 17 November 2017).

1. What are your views on what the territorial scope and the extra-territorial application of a data protection law in India should be?

2. To what extent should the law be applicable outside the territory of India in cases where data of Indian residents is processed by entities who do not have any presence in India?

3. While providing such protection, what kind of link or parameters or business activities should be considered?

   Alternatives:

   a. Cover cases where processing wholly or partly happens in India irrespective of the status of the entity.
   b. Regulate entities which offer goods or services in India even though they may not have a presence in India (modelled on the EU GDPR).
   c. Regulate entities that carry on business in India (modelled on Australian law), business meaning consistent and regular activity with the aim of profit.

4. What measures should be incorporated in the law to ensure effective compliance by foreign entities *inter alia* when adverse orders (civil or criminal) are issued against them?

5. Are there any other views on the territorial scope and extra territorial application of a data protection law in India, other than the ones considered above?

CHAPTER 2: OTHER ISSUES OF SCOPE

2.1 Natural/Juristic Persons

Several jurisdictions have deliberated on the applicability of a data protection law to individuals as well as corporate entities/juristic persons. For instance, the EU GDPR applies to 'natural persons' as the definition of 'personal data' is specifically linked to individuals and not legal/juristic persons. The EU GDPR relies on the understanding of a natural person as addressed in the Universal Declaration of Human Rights (UN Declaration).[199] The rights based framework as understood in the EU recognises that human beings are the subject of legal relations.[200] The POPI Act on the other hand, applies to natural as well as juristic persons. Data related to juristic persons such as confidential business information and corporate strategies should be protected against various types of processing activities on such data.[201] Further, such data should be subject to data security safeguards in order to ensure that the legitimate interests of juristic persons is protected.[202]

In India, the right to privacy as laid down in *Puttaswamy* flows from the right to life and personal liberty guaranteed under Article 21 of the Constitution of India. Components of this right can also be located in the autonomy and dignity of an individual guaranteed by the Constitution of India. In this context, a legislation that flows from a fundamental right such as the right to privacy, must include natural persons in its fold. While a juristic entity can claim and exercise certain fundamental rights, the ideas of autonomy and dignity may not be entirely applicable to it. Most key principles of data protection such as lawful processing and individual participation are intrinsically derived from the object of protecting the autonomy and dignity of the individual. It would be difficult to extend these principles to data relating to a juristic entity.

A distinction however has to be drawn between corporate data and some categories of data held by juristic persons which can reasonably identify an individual. Such data ought to be protected by a data protection law. However, data relating to a corporate entity which may otherwise require protection from theft, or unauthorized disclosure, cannot be protected by the data protection law. For instance, a company's Permament Account Number or its financial information, being data identifying a juristic person and not an individual, may be excluded from the purview of the data protection legislation.

---

[199] Article 6 of the UN Declaration states: 'Everyone has the right to recognition everywhere as a person before the law.'

[200] Article 29 Data Protection Working Party, 'Opinion 4/2007 on the Concept of Personal Data', European Commission (20 June 2007), 22, available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf, (last accessed 17 November 2017).

[201] South African Law Reform Commission, 'Privacy and Data Protection' Discussion Paper 109, Project 124 (October 2005), available at: http://www.justice.gov.za/salrc/dpapers/dp109.pdf; (last accessed 2 November 2017).

[202] South African Law Reform Commission, 'Privacy and Data Protection' Discussion Paper 109, Project 124 (October 2005), available at: http://www.justice.gov.za/salrc/dpapers/dp109.pdf; (last accessed 2 November 2017).

2.2 Horizontality of Application (Public versus Private Sector)

There is a large amount of personal data being processed by public and private entities alike. Further, an important dimension of the right to privacy is civil rights and surveillance, which involves the State.[203] Data protection laws in jurisdictions such as the EU apply to the Government, as well as private entities as far as their processing activities are concerned. The (Australian) Privacy Act contains thirteen Australian Privacy Principles (APPs) which apply to some private entities and most Australian and Norfolk Island government entities. In Canada, however, two separate laws apply to public and private entities. The Privacy Act 1983 (Canada Privacy Act) applies to the federal government institutions, and the PIPEDA applies to businesses.

There is a need to ensure that an individual's informational privacy is protected through a comprehensive data protection law which applies across the board. Additionally, the law may be devised to provide grounds for processing, and certain reasonable exemptions for data collected, used, disclosed, retained or stored by public entities. However, it is doubtful whether public entities can be completely excluded from the purview of the data protection law.

The Supreme Court has recognised that legitimate state interest must be protected through exemptions that may be carved out in a data protection law.[204] However, limited exemptions may be considered for well-defined categories of departments in Government or the public sector and similarly for entities in the private sector. In the former category, law enforcement agencies and intelligence agencies may have to be exempted from some of the rigours of the law. This is dealt with later in this White Paper. Second, the law may exempt entities such as charitable institutions or small business enterprises from all or some of the obligations under the law.[205] These exemptions will also have to be carefully designed.

2.3 Retrospective Application

A data protection law will apply ordinarily to data collected, used, stored, disclosed, retained etc. after the legislation enters into force. However, it may also apply to data that has been collected, used, stored, disclosed, retained etc. before the law was enacted. The data protection law will impose significant obligations for all entities involved in the collection, use, disclosure, retention and storage of personal data. To ensure effective implementation, the law should contain a transitory provision to ensure that all obligations are reasonable, and are complied with in the given time-frame. The provision for retrospective application may also be considered for certain reasonable obligations such as ensuring the integrity and confidentiality of information that is already in control of the processor. However, certain

[203] Joseph A. Cannataci, 'Report of the Special Rapporteur on the right to privacy', Human Rights Council, A/HRC/31/64 (2016).
[204] *Justice K.S. Puttaswamy (Retd.) v. Union of India & Ors*. (2017) 10 SCALE 1.
[205] *See* for instance Section 6 D, Canada Privacy Act

obligations like seeking fresh consent for personal data that has been collected, used, disclosed, retained or stored prior to the enactment of the law will be difficult to comply with.

The international experience in this regard is instructive. In South Africa, it is not clear whether the POPI Act has retrospective application. This is because Section 114(1) of the POPI Act states that "*All processing of personal information must within one year after the commencement of this section be made to conform to this Act*." However, it appears that there is legal consensus on the issue that the POPI Act does not have retrospective application.[206] Further, in Canada, where it is not explicitly clear from a reading of PIPEDA whether it applies retrospectively, the prevalent view is that it does not have retrospective application.[207] The implication of this is that PIPEDA being consent centric, it was not necessary for organisations to obtain consent for collection of pre-PIPEDA information. However, future use and disclosure of data will be regulated by the PIPEDA.[208]

2.4 Provisional Views

1. Given prevalent best practices, the law may apply to natural persons only. The primary object of the legislation being to protect the informational privacy right of an individual, the proposed law may not be extended to include data relating to companies and other juristic entities.

2. The law may apply to data about natural persons processed both by public and private entities. However, limited exemptions may be considered for well defined categories of public or private sector entities.

3. The law may have a transitory provision to address the issue of retrospective application.

2.5 Questions

1. What are your views on the issues relating to applicability of a data protection law in India in relation to (i) natural/juristic persons; (ii) public and private sector; and (iii) retrospective application of such law?

2. Should the law seek to protect data relating to juristic persons in addition to protecting personal data relating to individuals?

   Alternatives:

[206] Russel Luck, 'POPI - is South Africa keeping up with international trends?' 84(44) De Rebus (May 2014) , available at: http://www.saflii.org/za/journals/DEREBUS/2014/84.html, (last accessed 28 October 2017).
[207] 'Compliance with the Personal Information Protection and Electronic Documents Act', Aylesworth LLP, available at: http://documents.jdsupra.com/4217f03e-a265-4711-a230-103d2a5f3140.pdf, (last accessed 28 October 2017).
[208] 'Compliance with the Personal Information Protection and Electronic Documents Act', Aylesworth LLP, available at: http://documents.jdsupra.com/4217f03e-a265-4711-a230-103d2a5f3140.pdf, (last accessed 28 October 2017).

a. The law could regulate personal data of natural persons alone.
b. The law could regulate data of natural persons and companies as in South Africa. However, this is rare as most data protection legislations protect data of natural persons alone.

3. Should the law be applicable to government/public and private entities processing data equally? If not, should there be a separate law to regulate government/public entities collecting data?

Alternatives:

a. Have a common law imposing obligations on Government and private bodies as is the case in most jurisdictions. Legitimate interests of the State can be protected through relevant exemptions and other provisions.
b. Have different laws defining obligations on the government and the private sector.

4. Should the law provide protection retrospectively? If yes, what should be the extent of retrospective application? Should the law apply in respect of lawful and fair processing of data collected prior to the enactment of the law?

Alternatives:

a. The law should be applicable retrospectively in respect of all obligations.
b. The law will apply to processes such as storing, sharing, etc. irrespective of when data was collected while some requirements such as grounds of processing may be relaxed for data collected in the past.

5. Should the law provide for a time period within which all regulated entities will have to comply with the provisions of the data protection law?

6. Are there any other views relating to the above concepts?

CHAPTER 3: WHAT IS PERSONAL DATA?

3.1. Introduction

The definition of personal information or personal data is the critical element which determines the zone of informational privacy guaranteed by a data protection legislation. As noted by the Supreme Court in *Puttaswamy*, it is not merely intimate matters over which one has a reasonable expectation of privacy that fall within this zone. Rather, the object of data protection regimes is to protect the autonomy of the individual by protecting the identity of the individual.[209] The object of defining personal data or personal information is to demarcate facts, details or opinions that bear a relation to his or her identity.

3.2. Issues and International Practices

(i) Information or data?

The terms information and data are both used in the context of informational privacy and data protection. It appears that the word data is of comparatively more recent origin than the word information and is used in specialised scientific fields.[210] The word has specific connotations in the fields of computer science and information technology. 'Information' on the other hand simply means facts about something or someone.[211]

It is on these lines that the IT Act draws a distinction between these terms. Under Section 2 (1) (v) of the IT Act "information" includes data, text, images, sound, voice, codes, computer programmes, software and databases or micro-film or computer generated micro-fiche.[212] Subsection (o) of the same section defines data as "data" means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer.[213]

The SPDI Rules under the IT Act, building on these definitions of data and information, grant protection to a category of information termed "sensitive personal information or sensitive personal data".[214] These definitions may have to be revisited under the proposed law in light of global practices in which sensitive information has a different connotation.

---

[209] *Justice K.S.Puttaswamy (Retd.) v. Union of India (2017)* 10 SCALE 1 paragraph 177.
[210] Definition of data, can be found at: 'Data', Oxford Dictionaries, available at: https://en.oxforddictionaries.com/definition/data, (last accessed 1 November 2017).
[211] Definition of information, can be found at: 'Information', Oxford Dictionaries, available at: https://en.oxforddictionaries.com/definition/information, (last accessed 1 November 2017).
[212] Section 2 (1)(v), IT Act.
[213] Section 2 (1)(o), IT Act.
[214] Rule 3, SPDI Rules.

This distinction between data and information in its ordinary usage is perhaps not determinative in data protection. As the object of the law is to demarcate the sphere of information relevant to the protection of the identity of an individual, the choice of the term "data" or "information" may not matter as these terms would not be used in their ordinary sense. The definition will have to cover both data and information if it bears a connection to the identity of the individual.
This is reflected in international practice as well.

While the EU GDPR,[215] and Singapore[216] define the term personal data, Australia,[217] Canada[218] and South Africa[219] on the other hand use the term personal "information". As is clear from the next section, most of these terms roughly refer to the same category of information. However, the use of the term data in the EU may have some significance as it was the advent of new technology in the seventies resulting in easily accessible datasets that was the catalyst for the establishment of a data protection framework.[220] In keeping with this approach, the EU GDPR does not apply to non-automated processing of personal data which is not intended to be part of a filing system.[221]

For the purposes of this White Paper, we use the term data as the broader term which includes any form of information. It is clear that data can be facts, objective information or even opinions or any other sort of information. For instance, credit-worthiness of an individual which is an assessment of his or her ability to repay loans is an opinion/assessment which is nonetheless data. Some jurisdictions make this explicit in their legislations. Examples are Singapore and Australia where the legislations explicitly state that whether a piece of information is personal data does not depend on whether it is true or not.[222]

(ii) Information about/relating an individual

The object of data protection legislations as stated above is to ensure autonomy of the individual by protecting personal data. Information which is protected under the head of personal data must first and foremost be about such individual. The individual must be the subject matter of the information. For instance, a file maintained by a bank containing the KYC information of an individual is information about that individual.

[215] Article 4(1), EU GDPR.
[216] Section 2(1), Singapore Act.
[217] Section 6, Privacy Act.
[218] Section 2, PIPEDA.
[219] Section 1, POPI Act.
[220] Article 29 Data Protection Working Party, 'Opinion 4/2007 on the Concept of Personal Data', European Commission (20 June 2007), available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf, (last accessed 17 November 2017).
[221] Article 2, EU GDPR.
[222] Section 2, Singapore Act.

The relationship need not be as straightforward in all cases. For instance, information that a child is born with foetal alcohol syndrome is personal information both about the child and its mother.[223]

To signify this relationship, various connectors are used. The SPDI Rules use the phrase with *"information that relates to a natural person*". The EU GDPR uses a similar phrase "*any information relating* to an identified or identifiable natural person." The (Australian) Privacy Act uses the simpler phrase "*information about an individual."*

(iii) Identified or Identifiable Individual

All information about an individual is not personal data. As stated earlier, protection of identity is central to informational privacy. So the information must be such that the individual is either identified or identifiable from such information. In statutes or instruments which use both these terms "identified or identifiable" such as the EU GDPR, it refers to states in which the data could be. Data could be in a form where individuals stand identified or in other cases, it is possible that they could be identified.[224] Whether an individual is identifiable or not is a question of context and circumstances. For instance, a car registration number, by itself, does not reveal the identity of a person. However, it is possible that with other information, an individual can be identified from this information.

The question of identifiability being one of context, it is essential to prescribe standards by which data can be said to be identifiable or not. The EU GDPR does not prescribe the standard in the text of the provision. However, Recital 26 of the EU GDPR sets out the standard by stating that in determining whether a person is identifiable from data account must be had of all the means reasonably likely to be used.[225] For instance, in the EU, IP addresses are considered (atleast in some circumstances) to be data relating to an identifiable person as Internet Service Providers could identify Internet users using reasonable means.[226]

In the (Australian) Privacy Act, the definition of personal information makes the standard of "reasonably identifiable" explicit. "Personal information", under the Privacy Act means information or an opinion about an identified individual or an individual who is *reasonably identifiable*. Canada, in the PIPEDA, goes a step further and drops the term 'identified' from the scope of the definition entirely and refers only to information about an *identifiable individual*.[227]

---

[223] OAIC, 'What is personal information' (May 2017), available at: https://www.oaic.gov.au/agencies-and-organisations/guides/what-is-personal-information, (last accessed 4 November 2017).
[224] Article 29 Data Protection Working Party, 'Opinion 4/2007 on the Concept of Personal Data', European Commission (20 June 2007), 12, available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf, (last accessed 17 November 2017).
[225] Recital 26, EU GDPR.
[226] Article 29 Data Protection Working Party, 'Opinion 4/2007 on the Concept of Personal Data', European Commission (20 June 2007), available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf, (last accessed 17 November 2017).
[227] Section 2(1), PIPEDA.

(iv) Pseudonymisation and Anonymisation

Related to the notion of identifiability are the techniques of pseudonymisation and anonymisation. Pseudonymisation refers to the technique of disguising identities which ordinarily does not exclude data from the scope of personal data. The EU GDPR recommends pseudonymisation as a method of reducing risk to the data of individuals and as a method of meeting data protection obligations. It also prescribes technical and organisational safeguards in this regard.[228]

Anonymisation, by contrast, refers to data where all identifying elements have been eliminated from a set of personal data. No element may be left in the information which could, by exercising reasonable effort, serve to re-identify the person(s) concerned. Where data has been successfully anonymised, they are no longer considered to be personal data.[229]Anonymised data, thus falls outside scope of data protection legislation in such systems. Anonymisation is a standard practice in various processes particularly in data aggregation. However, as will be pointed out later, the extent of such anonymisation is now a contested issue with instances emerging where individuals having been identified from supposedly anonymised data sets.

(v) Personal Data and New Technologies

One important challenge to the definition of personal data arises from modern technologies which collect newer forms of data from newer sources. While reviewing the OECD Guidelines, this was one of the main issues identified by the expert body for further research.[230] It was observed that the current definition views personal data in terms of a binary, i.e. identifiable data and non-identifiable data. The workability of this definition has been called into question. On the one hand, there are doubts whether the definition is under-inclusive when it excludes anonymised data entirely as the "robustness" of some of these techniques have been questioned. A well known example is of a data set of search queries released by AOL after having removed all identifiers which nonetheless resulted in the identification of an individual within days of release of the data set.[231]

At the same time, there are problems of over inclusion as well because often data exists in a form which permits identification at a high cost. In such circumstances, the definition of personal data could include such data as it relates to an identifiable individual. A further risk is that guaranteeing the full spectrum of rights to such data could in fact increase privacy

[228] Recitals 26, 28 and 29, EU GDPR.
[229] The European Union Agency for Fundamental Rights (FRA), the Council of Europe and the Registry of the European Court of Human Rights, 'Handbook on European Data Protection Law' (2014), available at: http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf, (last accessed 4 November 2017).
[230] OECD, OECD Digital Economy Papers No. 229, 'Privacy Expert Group Report on the Review of the 1980 OECD Privacy Guidelines', 10, available at: http://www.oecd-ilibrary.org/science-and-technology/privacy-expert-group-report-on-the-review-of-the-1980-oecd-privacy-guidelines_5k3xz5zmj2mx-en., (last accessed 1 November 2017).
[231] Paul Ohm, 'Broken Promises of Privacy: Responding to the surprising failure of Privacy', 57 UCLA Law Review 1701, 1717 (2010).

risks. For instance, if participation rights are given with respect to a data set which is supposedly anonymised, but may be capable of being re-identified, the data controller would be required to identify the individuals first from the data.[232]

The advent of the Internet of Things also poses a challenge to the degree of anonymity that can be achieved. New devices capture data in forms which are unique. An example is that of a person's gait being uniquely identified by a wearable activity tracker.[233] Such data can perhaps never be completely de-identified. The current methods of using aggregated anonymised data might not be secure enough when applied to such data.

In spite of these issues, several prominent jurisdictions continue to rely on definitions of personal data which are structured around the notion of information about/related to an identified or reasonably identifiable individual. Some nuance may be of relevance here. The EU GDPR also qualifies the above statement by noting that the identification may be direct or indirect thus broadening the scope of the definition.[234] Similarly, as pointed out earlier some legislations make it explicit whether information constitutes personal information is not dependent on its accuracy. A noteworthy feature of the POPI Act is that the definition has an illustrative component as well which lists some of the common forms of personal information.[235] These are some practices worth considering in constructing a definition of personal data under the law.

(vi) A layered approach?

A prominent jurisdiction not discussed above is the US where different kinds of definitions exist as a result of data protection being dealt with in sector-specific laws. The kind of information to be protected is broadly referred to by the umbrella term "Personally Identifiable Information" (PII). However, definitions of PII vary widely across statutes. Shwartz and Solove draw up a useful typology where they refer to definitions based on standards on one hand and rule-based definitions on the other hand.[236] Definitions in the EU, Canada and Australia referred to above are examples of standard-based definitions which are largely technologically neutral and rely on the standard of identification.

In the US, the Video Privacy Protection Act, 1988 (VPPA) is pointed out as an example of a similar approach. However, the VPPA protects only the category of information which identifies an individual and does not use the standard of identifiability. A different standard found in the GLB Act is that of non-public personal information. The standard used here is

[232] OECD, OECD Digital Economy Papers No. 229, 'Privacy Expert Group Report on the Review of the 1980 OECD Privacy Guidelines', 10, available at: http://www.oecd-ilibrary.org/science-and-technology/privacy-expert-group-report-on-the-review-of-the-1980-oecd-privacy-guidelines_5k3xz5zmj2mx-en., (last accessed 1 November 2017).
[233] Scott R Peppet, 'Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security and Consent', 93(85) Texas Law Review 156 (2014).
[234] Article 4 (1) , EU GDPR.
[235] Section 2, POPI Act.
[236] Paul M. Shwartz and Daniel Solove, 'The PII Problem: Privacy and a New Concept of Personally Identifiable Information', 86 NYU Law Quarterly Review 1814 (2011).

that the information is not in the "public domain." However, this approach may not be entirely satisfactory as in the absence of identifiability, the privacy interest of an individual in the information is not clear.[237] The third kind of definition which runs the risk of being outdated quickly is the approach which identifies specific types of data. California's Song - Beverly Credit Card Act of 1971 and the COPPA are examples of this approach, though the latter is an open ended definition which permits the regulator to add to the listed categories of personal information.[238]

Solove and Schwartz contrast these definitions with the EU model and propose an alternative. The EU model, in their opinion, is too broad in that even data from which an individual may be identifiable would be personal information entitled to the full spectrum of protection. Imposing, say, requirements of notice and consent on use of such information would require that the data be converted from *identifiable* state to an *identified* state. This would be a disproportionate response to the risk involved. They suggest that the law should only impose obligations of data security, transparency and data quality on such identifiable information.[239]

3.3. Provisional Views

1. It is data about/relating to an individual that may be the subject matter of protection under the law. Data in this context ought to include any kind of information including opinions or assessments irrespective of their accuracy.

2. Data from which an individual is identified or identifiable/reasonably identifiable may be considered to be personal data. The identifiability can be direct or indirect.

3. New technologies pose considerable challenges to this distinction based on identifiability. This standard may have to be backed up by codes of practice and guidance notes indicating the boundaries of personal information having regard to the state of technology.

3.4. Questions

1. What are your views on the contours of the definition of personal data or information?

2. For the purpose of a draft data protection law, should the term 'personal data' or 'personal information' be used?

   Alternatives:

[237] Paul M. Shwartz and Daniel Solove, 'The PII Problem: Privacy and a New Concept of Personally Identifiable Information', 86 NYU Law Quarterly Review 1814 (2011).
[238] Paul M. Shwartz and Daniel Solove, 'The PII Problem: Privacy and a New Concept of Personally Identifiable Information', 86 NYU Law Quarterly Review 1814, 1832 (2011).
[239] Paul M. Shwartz and Daniel Solove, 'The PII Problem: Privacy and a New Concept of Personally Identifiable Information', 86 NYU Law Quarterly Review 1814, 1881 (2011).

a. The SPDI Rules use the term sensitive personal information or data.
b. Adopt one term, personal data as in the EU GDPR or personal information as in Australia, Canada or South Africa.

3. What kind of data or information qualifies as personal data? Should it include any kind of information including facts, opinions or assessments irrespective of their accuracy?

4. Should the definition of personal data focus on identifiability of an individual? If yes, should it be limited to an 'identified', 'identifiable' or 'reasonably identifiable' individual?

5. Should anonymised or pseudonymised data be outside the purview of personal data? Should the law recommend either anonymisation or psuedonymisation, for instance as the EU GDPR does?

   [Anonymisation seeks to remove the identity of the individual from the data, while pseudonymisation seeks to disguise the identity of the individual from data. Anonymised data falls outside the scope of personal data in most data protection laws while psuedonymised data continues to be personal data. The EU GDPR actively recommends psuedonymisation of data.]

6. Should there be a differentiated level of protection for data where an individual is identified when compared to data where an individual may be identifiable or reasonably identifiable? What would be the standards of determing whether a person may or may not be identified on the basis of certain data?

7. Are there any other views on the scope of the terms 'personal data' and 'personal information', which have not been considered?

CHAPTER 4: SENSITIVE PERSONAL DATA

4.1 Introduction

All data within the category of information identified as personal data are not qualitatively similar. As discussed previously, personal data refers to information related to a person's identity. There are matters within this zone which are intimate matters in which there is a higher expectation of privacy. Unauthorized use of such information of the individual may have severe consequences. The observations of the Supreme Court in *Puttaswamy*,[240] on sexual orientation illustrate this aspect of sensitive information:

> *"Sexual orientation is an essential attribute of privacy. Discrimination against an individual on the basis of sexual orientation is deeply offensive to the dignity and self-worth of the individual."*

Thus, apart from the harm of intrusion of one's privacy, as pointed out by the Supreme Court, such data, if revealed, may also be the basis of discriminatory action.[241] It is necessary to identify kinds of data that are "sensitive" and accord higher protections to such data. Further issues relating to sensitive personal data are discussed in Part III, Chapter 6 of this White Paper.

4.2 Issues and International Practices

There are certain kinds of information which invariably find mention in the set of sensitive information across jurisdictions. Some of these intuitively are of the nature described above. These include health information, genetic information, biometric information and information about religious beliefs, ethnic or racial origin and information relating to sexual orientation. The EU GDPR[242] and the data protection legislations in Australia[243] and South Africa[244] all include these categories as sensitive personal data. The level of intrusion resulting from any unauthorised processing of such information is undoubtedly high.

There are other kinds of information such as philosophical beliefs, membership of political associations and membership of trade unions which are also categorised as sensitive personal data in the jurisdictions mentioned above. As noted above, the categorisation of information as sensitive personal data depends on whether such information is treated as as an intimate

---

[240] *Justice K.S. Puttaswamy (Retd.)& Anr. v. Union of India & Ors.*, (2017) 10 SCALE 1, Paragraph 126.

[241] *See also* Article 29 Data Protection Working Party, 'Advice paper on Special Categories of Data ("sensitive data")', European Commission (20 April 2011), available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2011/2011_04_20_letter_artwp_mme_le_bail_directive_9546ec_annex1_en.pdf (last accessed 2 November 2017); ICO, 'Guidance note on Special Categories of Data', available at: https://ico.org.uk/for-organisations/guide-to-data-protection/key-definitions/, (last accessed 2 November 2017), 'The presumption is that, because information about these matters could be used in a discriminatory way, and is likely to be of a private nature, it needs to be treated with greater care than other personal data.'

[242] Article 9, EU GDPR

[243] Section 6 , Privacy Act.

[244] Section 26, POPI Act.

matter in which there is a serious privacy interest. The application of these factors vary from country to country. It must thus be seen whether information in these categories are sensitive in the Indian context.

A *prima facie* indication of the position on these issues is reflected in the SPDI Rules.[245] The core categories identified by the Government in 2011 for protection as sensitive personal data were (i) passwords; (ii) financial information such as Bank account or credit card or debit card or other payment instrument details; (iii) physical, physiological and mental health condition; (iv) sexual orientation; (v) medical records and history; and (vi) biometric information. Racial or ethnic origin, philosophical beliefs, membership of political associations and membership of trade unions are all missing from this list. A fresh assessment would have to be carried out to ascertain whether such information should be included in the category of sensitive personal data.

The other category of data that requires specific consideration is financial data. The SPDI Rules prescribe financial data to be sensitive data. This is similar to the American practice of treating financial information such as credit card information as sensitive information.[246]Financial data, which finds mention in the SPDI Rules is not a category which finds mention as sensitive data in the EU, South Africa or Australia. In Australia, in the consultation processes leading to the amendment of the Privacy Act, it was suggested that financial information should be included in the category of sensitive personal data. The suggestion was rejected noting that while financial data shares certain characteristics with other sensitive data in that it has to be handled with care,[247] it does relate to any intimate personal or physical attribute like other sensitive data.

Other categories of information specific to India such as caste may also have to be considered for inclusion. Information about the caste of an individual falls within the zone where there is a higher expectation of privacy and it could be a reason for discrimination as well. These point to the fact that information about caste should be included in the list of sensitive data. It is important to distinguish information about caste from information from which caste of a person may be surmised such as a surname. The name of a person, even if it reveals his or her caste or religion cannot be the basis for treating the name itself as sensitive personal data. The question whether such information is sensitive data would be context dependent. For instance, a list of names where there is no reference to any other fact, does not mean that the entire list is sensitive personal information because the castes of some individuals may be surmised from their names. However, if a list is prepared indicating the caste of every person in a separate column, that could be sensitive personal data requiring a different standard of

[245] Rule 3, SPDI Rules.
[246] The FTC which draws its primary authority from the FTC Act also administers and acts under a number of other statutes such as the GLB Act, COPPA etc. FTC, 'Protecting Personal Information: A Guide for Business' (23 January 2015), available at: www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business, (last accessed 17 November 2017).
[247] Australian Law Reform Commission, 'The Privacy Act: Some Important Definitions', available at: https://www.alrc.gov.au/publications/6.%20The%20Privacy%20Act%3A%20Some%20Important%20Definitions/sensitive-information, (last accessed 3 November 2017).

protection. Subject to an evaluation of these issues, caste may be considered as a category for inclusion in the list of sensitive personal data.

All jurisdictions considered above list specific kinds of data as sensitive personal data and prescribe heightened protections for the same. A jurisdiction which adopts a different approach is Canada where there is no precise definition for sensitive personal data. Any personal data could be sensitive under the PIPEDA, if the context so warrants.[248] This approach has the advantage of being flexible and not limiting the safeguards of sensitive personal data to a predetermined list. At the same time, it lacks the precision of the model identifying specific kinds of data as sensitive personal. This could lead to difficulties in the Indian context.

4.3 Provisional Views

1. Health information, genetic information, religious beliefs and affiliations, sexual orientation, racial and ethnic origin may be treated as sensitive personal data. Caste information may also be treated as sensitive personal data.

2. Though qualitatively different from the information in the previous category, financial information may also be included as sensitive personal data. Financial information has been categorised as sensitive information in India since the formulation of SPDI Rules.

3. In other categories such as philosophical or political beliefs, an assessment may be made whether these are matters in which a person has an expectation of a high degree of privacy.

4.4 Questions

1. What are your views on sensitive personal data?

2. Should the law define a set of information as sensitive data? If yes, what category of data should be included in it? Eg. Financial Information / Health Information / Caste / Religion / Sexual Orientation. Should any other category be included?

   [For instance, the EU GDPR incorporates racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning health or sex life.]

3. Are there any other views on sensitive personal data which have not been considered above?

[248] *See* Schedule I, paragraph 4.3.4, PIPEDA.

CHAPTER 5: WHAT IS PROCESSING?

5.1 Introduction

Having discussed the term personal data, it is important to demarcate actions performed on such data which would be the primary subject matter of the law. A compendious term that is used to address any action involving data is the term "processing". To give the broadest possible protection, data protection laws across the globe have tried to develop definitions of data processing in such a manner that they cover all the associated activities that are performed on data. These are considered below.

5.2 Issues and International Practices

(i) Processing of Personal Data

European Union

The EU GDPR defines 'processing' as any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. This definition explicitly refers to most activities that can be performed on data. It also covers both manual and electronic processing.[249]

United Kingdom

The UK DPA defines processing[250] as the means for obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including organisation, adaptation, alteration, retrieval, consultation, disclosure by transmission, dissemination or otherwise making available, alignment, combination, blocking, erasure or destruction of the information or data. This definition follows closely from the Data Protection Directive definition but does not explicitly cover manual data processing.

The UK Data Protection Bill, 2017 follows the EU GDPR definition of processing[251] and defines both in an inclusive and exhaustive sense, by covering any operation or set of operations, which are performed on personal data, or on sets of personal data, such as: collecting, recording, organising, structuring, storing, adapting or altering, retrieving, consulting, using, disclosing by transmission, disseminating or otherwise making available, aligning, combining, restricting, erasing or destroying.

[249] Article 4(2), EU GDPR.
[250] Section 1(1), UK DPA.
[251] Section 1(4), UK Data Protection Bill, 2017.

South Africa

The POPI Act defines processing[252] as any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including; the collection, receipt, recording, organisation, 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.

Canada and Australia

Other jurisdictions, such as Canada and Australia, adopt a different approach. In Canada, the PIPEDA defines processing of data using three terms—collection, use, and disclosure. The (Australian) Privacy Act, also focuses on the collection, use and disclosure of data rather than an elaborate definition of data processing. In these laws while the term processing is also used, the conditions for collection, use and disclosure are separately identified and isolated. Thus in the PIPEDA, for instance, collection and use of personal information are separately dealt with.[253] Similarly, under the Privacy Act, APP 3 deals with collection of Information while APP 6 deals with use or disclosure of information.

The distinction between collection use and disclosure of data is often thin and it is perhaps for this reason that the EU does not distinguish conceptually between these actions and uses the broad term processing. The advantage of the Canadian and Australian approach is that it appears more precise when conditions for collection, use and disclosure are separately listed.

(ii) Automated means versus manual processing

Data processing activities are carried out through automated means, as well as manual methods. In this context, it is necessary to examine whether a data protection law would apply to both types of processing.

European Union

The EU GDPR is applicable to personal data that has been processed wholly or partly by automated means. It also applies to data which forms part or is intended to form part of a

[252] Section 1, POPI Act.
[253] Paragraph 4.3 of Schedule I and Section 7, PIPEDA.

'filing system'.[254] A 'filing system' has been defined as 'any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.'[255] This refers to personal data that is contained in manual records but may be organised in a structured manner.

South Africa

South Africa follows a similar approach.[256] This approach is based on the premise that easily accessible datasets increase privacy risks and in respect of manual processing such risks arise only if the data is an easily accessible dataset in an organized manner.[257] An example of personal data processed manually is as follows: A hospital collects patient details manually and stores it as physical records. Here, personal data is collected or stored manually and therefore, is processed through non-automated means.

5.3 Provisional Views

1. The data protection law may not attempt to exhaustively list all operations that constitute processing.

2. The definition of processing may be broadly worded to include existing operations while leaving room to incorporate new operations by way of interpretation.

3. The definition may list the three main operations of processing i.e. collection, use and disclosure of data. It may be worded such that it covers the operations/activities incidental to these operations.

4. The law should cover both automated and manual processing.

5.4 Questions

1. What are your views on the nature and scope of data processing activities?

2. Should the definition of processing list only main operations of processing i.e. collection, use and disclosure of data, and inclusively cover all possible operations on data?

3. Should the scope of the law include both automated and manual processing? Should the law apply to manual processing only when such data is intended to be stored in a filing system or in some similar structured format?

   Alternatives:

[254] Article 2(1), EU GDPR.
[255] Article 4(6), EU GDPR.
[256] Section 3, POPI Act.
[257] *See also* Recital 15, EU GDPR.

a. All personal data processed must be included, howsoever it may be processed.
b. If data is collected manually, only filing systems should be covered as the risk of profiling is lower in other cases.
c. Limit the scope to automated or digital records only.

4. Are there any other issues relating to the processing of personal data which have not been considered?

CHAPTER 6: ENTITIES TO BE DEFINED IN THE LAW: DATA CONTROLLER AND PROCESSOR

6.1 Introduction

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.

Control over data, in such systems, refers to the competence to take decisions about the contents and use of data.[258] The entity that has control over data is responsible for compliance with data protection norms and is termed a "data controller." In addition to the data controller, other entities which take part in the processing of data are often identified and defined. For instance, a data processor is an entity which is closely involved with processing, which however, acts under the authority of the data controller.[259]

Identification of all entities participating in the entire cycle of data processing is not the only method of allocating responsibility. There are various models which have evolved in this regard in other jurisdictions. Each operates at a different level of specificity in identifying the entities involved in processing. These alternatives are considered below.

6.2 Issues and International Practices

European Union

The model that is most prescriptive is the EU GDPR which uses the concepts of data controller, data processor and third party to identify various entities involved in the processing of personal data.[260] A data controller is the entity which determines the purposes and means of processing data.[261] A processor is an entity which processes data on behalf of the controller.[262] The meaning of "third party" is not immediately apparent from the definition which refers to other entities apart from controllers or processors who under the authority of controller or processor are authorised to process data.[263] A useful illustration is of

[258] *See* 'Definition of data controller' in OECD, 'OECD Guidelines Concerning the Protection of Privacy and Transborder Flows of Personal Data' (2013), available at: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#part1, (last accessed 31 October 2017).
[259] Article 29 Data Protection Working Party Opinion, 'Opinion 01/2010 on the Concepts of 'Controller' and 'Processor'', European Commission (16 February 2010), available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf, (last accessed 31 October 2017).
[260] A fourth category of recipient is also identified in Article 4(9), EU GDPR.
[261] Article 4(7), EU GDPR.
[262] Article 4(8), EU GDPR.
[263] Article 4(9), EU GDPR.

an employee of the controller who gets to know data that she is not authorised to access in the course of her employment. She is a third party with respect to the data controller.[264]

As has been pointed out above, the objective of identifying these entities is to demarcate or allocate responsibility. The EU GDPR places some direct obligations on the processor which is not the case with the Data Protection Directive (which it will replace). Further, the EU GDPR attempts to be specific as to the methods to be adopted while entering into processing and sub-processing contracts. All these seem to require written contracts which are to be facilitated by the adoption of standard contractual clauses by data protection authorities.[265] This approach clearly has the advantage of specificity in the allocation of responsibilities.

Australia

Australia, by contrast, does not use the concept of data control. All entities and organisations which fall within the ambit of the law are accountable under the law for breach of the APP. Thus, an entity which 'holds' information may be acting under the directions of another entity which has control over the data. Nonetheless, it is equally bound by the applicable privacy principle.[266] While this approach appears straightforward, in complex situations such as use of foreign cloud providers, the absence of a party which is primarily accountable for compliance with data protection norms may cause some difficulty.

Canada

PIPEDA adopts a different approach in allocating responsibility. Under the PIPEDA, an organisation is responsible for personal information under its control.[267] In respect of other entities involved in processing, PIPEDA states that an organisation continues to be responsible for any information transferred to third parties for processing.[268] The organisation is required to use contractual or other means to ensure a comparable level of protection while the information is processed by a third party.[269]

While the PIPEDA certainly lacks the specificity of the EU GDPR, the approach is worth considering given that while introducing a data protection regime for the first time in India, it may not be advisable to be too prescriptive. Imposing the requirement of formal contracts on every agreement for processing may not be feasible and could have the result of impeding transactions for processing of data. Further, reactions to the EU GDPR suggest that there

[264] Article 29 Data Protection Working Party Opinion, 'Opinion 01/2010 on the Concepts of 'Controller' and 'Processor'', European Commission (16 February 2010), available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf, (last accessed 31 October 2017).
[265] Article 28, EU GDPR.
[266] OAIC, 'Australian businesses and the EU General Data Protection Regulation' (May 2017), available at: https://www.oaic.gov.au/resources/agencies-and-organisations/business-resources/privacy-business-resource-21-australian-businesses-and-the-eu-general-data-protection-regulation.pdf, (last accessed 1 November 2017).
[267] Principle 4.1 of Schedule 1, PIPEDA.
[268] Principle 4.1.3 of Schedule 1, PIPEDA.
[269] Principle 4.1.3 of Schedule 1, PIPEDA.

could be high compliance costs on data processors.[270] Concerns relating to enforceability of contracts and enforcement capabilities in India must also be taken into account while attempting to precisely allocate responsibility by identifying multiple actors in processing of data. On the other hand, there remains the possibility that the new law could be the catalyst for mature transactions in data processing and the market may adapt to the new norms, however specific they are.

6.3 Provisional Views

1. To ensure accountability, the law may use the concept of 'data controller'. The competence to determine the purpose and means of processing may be the test for determining who is a 'data controller'.

2. The need to define data processors, third parties or recipients depends on the level of detail with which the law must allocate responsibility. This has to be determined on an assessment of the likely impact of imposing obligations on processors and the compliance costs involved, amongst other things.

6.4 Questions

1. What are your views on the obligations to be placed on various entities within the data ecosystem?

2. Should the law only define 'data controller' or should it additionally define 'data processor'?

   Alternatives:

   a. Do not use the concept of data controller/processor; all entities falling within the ambit of the law are equally accountable.
   b. Use the concept of 'data controller' (entity that determines the purpose of collection of information) and attribute primary responsibility for privacy to it.
   c. Use the two concepts of 'data controller' and 'data processor' (entity that receives information) to distribute primary and secondary responsibility for privacy.

3. How should responsibility among different entities involved in the processing of data be distributed?

   Alternatives:

   a. Making data controllers key owners and making them accountable.

[270] Dr. Detlev Gebel and Tim Hickman, 'Chapter 11: Obligations of processors – Unlocking the EU General Data Protection Regulation', White & Case (22 July 2016), accessible at: https://www.whitecase.com/publications/article/chapter-11-obligations-processors-unlocking-eu-general-data-protection, (last accessed 29 October 2017).

b. Clear bifurcation of roles and associated expectations from various entities.
c. Defining liability conditions for primary and secondary owners of personal data.
d. Dictating terms/clauses for data protection in the contracts signed between them.
e. Use of contractual law for providing protection to data subject from data processor.

4. Are there any other views on data controllers and processors which have not been considered above?

CHAPTER 7: EXEMPTIONS FOR HOUSEHOLD PURPOSES, JOURNALISTIC AND LITERARY PURPOSES AND RESEARCH

7.1 Introduction

There are some activities which cannot be brought under the purview of a data protection law. In other words, a data controller can be exempted from certain obligations of a data protection law based on the nature and purpose of the processing activity. For instance, if a law enforcement officer wants to collect or use personal information for the purpose of an investigation, seeking consent of the data subjects or allowing them to access or rectify their data would delay the process and may even defeat its purpose. In general, the exemptions could either limit the rights of the individual/data subject, or limit the extent of obligations imposed on the entities/data controllers. Such exemptions in some circumstances will act as reasonable limitations on the right to privacy.

The broad parameters for such exemptions in India have been indicated by the Supreme Court in *Puttaswamy:*[271]

> *"The creation of such a regime requires a careful and sensitive balance between individual interests and legitimate concerns of the state. The legitimate aims of the state would include for instance protecting national security, preventing and investigating crime, encouraging innovation and the spread of knowledge, and preventing the dissipation of social welfare benefits."*

Jurisdictions such as the UK, EU, South Africa, Italy, Singapore etc. exempt certain data controllers from certain obligations under their data protection laws. The common exemptions found in these laws relate to the following – (1) processing of data for personal or household purpose; (2) processing of data for journalistic, artistic or literary purpose; (3) processing of data for research, historical or statistical purpose; (4) processing of data for investigation, apprehension or prosecution of offenders; (5) processing of data for national security purpose. Further, these laws grant varying exemptions to certain types of processing activities. Some activities enjoy wide exemptions; some activities are partially exempt, i.e. they do not have to comply with certain key data protection obligations. They may, however, be mandated to follow some measures to ensure that data is handled safely.

Broadly, any category of exemptions carved out under a data protection law will have to skillfully balance the need for exempting a specific data processing activity with the curtailment of rights of an individual.

[271] *Justice K.S. Puttaswamy (Retd.)& Anr. v. Union of India & Ors.*, (2017) 10 SCALE 1., Section T, Conclusions, paragraph 5.

7.2 Specific Exemptions and International Practices

(i) Personal or household purpose

In instances where the data controller is an individual who processes data for herself, or for household activities, such activity would be outside the scope of regulation. For instance, a personal diary maintained by an individual which may have references to friends and family, or an address book on a computer containing personal data of friends and acquaintances. However, if personal data collected for domestic processing use is published on the Internet and is available to a large audience, it may fall outside the remit of this exemption.[272] Similarly, some instances of domestic processing such as installation of CCTV cameras in residences, use of drones and wearable technology, use of blogs and social networks, recording of personal conversations etc. will have to be examined closely for the purposes of this exemption.

Collection and usage of personal data for personal uses or household purposes is outside the scope of data protection laws in several jurisdictions such as UK[273] EU,[274] and South Africa.[275]It will be difficult to identify processing for personal or household purposes as individuals have more 'publishing power' which was earlier available to commercial organisations.[276] The EU has formulated certain criteria to determine whether the processing falls under personal or household purposes.[277] These may be examined further for the purpose of articulating the exemption in law.

(ii) Journalistic/Artistic/Literary purposes

This exemption seeks to strike a balance between an individual's right to privacy and the right to free speech and expression. For instance, newspapers routinely publish personal data of public figures or other individuals while reporting. However, the terms 'journalistic purposes' and 'journalist' are not defined in law currently. These terms need to be defined to ensure clarity in the scope of application. In some instances, non-media organisations which publish

[272] *Bodil Lindqvist v. Åklagarkammaren i Jönköping*, Case C-101/01 (2003), European Court of Justice– a representative of the local church used her personal computer to set up websites which was linked to a Swedish church website. It ended up displaying the names, addresses, hobbies, information about jobs of the defendant and her colleagues. The colleagues' consent had not been sought. Held to be outside the scope of the domestic processing exemption.
[273] Section 36, UK DPA.
[274] Article 2, EU GDPR.
[275] Section 6, POPI Act.
[276] Annex 2 – 'Proposals for Amendments regarding exemption for personal or household activities (EU)', European Commission, available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20130227_statement_dp_annex2_en.pdf, (last accessed 31 October 2017).
[277] Annex 2 – 'Proposals for Amendments regarding exemption for personal or household activities (EU)', European Commission, available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20130227_statement_dp_annex2_en.pdf, (last accessed 31 October 2017).

information for mass coverage may be covered as also bloggers and others who generate content online.[278] Further, art and literature are interpreted broadly.[279]

Various data protection laws grant different levels of exemptions for processing of personal data for journalistic purposes. For instance, the EU GDPR provides an option to Member States to provide for derogations from certain obligations if they are 'necessary to reconcile the right to the protection of personal data with the freedom of expression and information.'[280] According to the UK DPA, the exemptions granted in this category are from all data protection principles (except the one relating to organisational and technical safeguards), subject access request and right to prevent processing, rights in relation to automated decision making, and right to seek erasure, rectification and blocking.[281] Other jurisdictions which provide this exemption are South Africa,[282] Philippines,[283] Singapore,[284] and South Korea.[285]

As this exemption seeks to fulfill the right to free speech and expression several jurisdictions provide a wide exemption in this category. However, in the absence of a clear articulation of what these activities might be, or how terms such as 'journalist', 'journalistic', 'artistic', 'literary' are commonly understood, the provision may be misused. The way forward may be to identify only those activities in this category where the necessity or purpose of the activity and the corresponding right to free speech and expression outweighs the right to privacy of the data subject.

(iii) Research/historical and statistical purposes

This exemption seeks to balance the need for innovation with the right to privacy of an individual. A law on informational privacy should not be an impediment to research activities. This exemption can be availed if the data processing activity is being conducted for research/historical or statistical purposes. For instance, collection of personal data for Census.

---

[278] Information Commissioner's Office (UK) Guidance, 'Data Protection and Journalism: A Guide for the Media' (4 September 2014), available at: https://ico.org.uk/media/for-organisations/documents/1552/data-protection-and-journalism-media-guidance.pdf, (last accessed 2 November 2017).

[279] Information Commissioner's Office (UK) Guidance, 'Data Protection and Journalism: A Guide for the Media' (4 September 2014), available at: https://ico.org.uk/media/for-organisations/documents/1552/data-protection-and-journalism-media-guidance.pdf, (last accessed 2 November 2017).

[280] Article 85, EU GDPR; Article 85(2) states 'For processing carried out for journalistic purposes or the purpose of academic artistic or literary expression, Member States shall provide for exemptions or derogations from Chapter II (principles), Chapter III (rights of the data subject), Chapter IV (controller and processor), Chapter V (transfer of personal data to third countries or international organisations), Chapter VI (independent supervisory authorities), Chapter VII (cooperation and consistency) and Chapter IX (specific data processing situations)'.

[281] Section 32, UK DPA.

[282] Section 7, POPI Act.

[283] Philippines provides the strongest exemption in this category. *See* Graham Greenleaf, 'Asian Data Privacy Laws: Trade & Human Rights Perspectives', 481 (Oxford University Press, 2016).

[284] Singapore exempts 'news organisations' from seeking consent for collection of personal data strictly for 'news activities'. They are not exempted from other principles. *See* Graham Greenleaf, 'Asian Data Privacy Laws: Trade & Human Rights Perspectives', 481 (Oxford University Press, 2016).

[285] South Korea provides a general exemption for personal data that is collected for 'use for reporting by the press,' *see* Graham Greenleaf, 'Asian Data Privacy Laws: Trade & Human Rights Perspectives', 481 (Oxford University Press, 2016).

In India, collection of statistical information by the Government is governed by the Collection of Statistics Act, 2008 (Collection of Statistics Act). This legislation deals with the collection of statistical information relating to economic, demographic, social, scientific and environmental aspects by the Government. The appropriate Government can direct that a relevant statistics officer may supervise the collection of the requested statistical information[286]. The statistics officer requests the collection of necessary information by serving a written notice to an informant. Upon the receipt of a written request, the informant is bound to furnish information to the best of his/her ability. The statistics officer, or his authorized representative has the power to access relevant records or documents in the possession of the informant.[287]

In the case of South Africa, under the POPI Act, the Information Regulator may exempt processors from certain obligations in the following two conditions - if public interest in processing outweighs, to a substantial degree, any interference with privacy; or if processing involves a clear benefit to the data subject or a third party that outweighs, to a substantial degree, any interference with privacy. Public interest has been defined to include 'historical, statistical or research activity.' Jurisdictions such as Italy,[288] South Africa,[289] UK,[290] provide exemptions for personal data processed in for research/historical and statistical purposes.

This exemption promotes academic freedom of research, and processing of data in wider public interest. However, the term 'research' should be clearly defined to exclude non-academic research such as market research or processing of data for the purpose of advertising or other commercial purposes. For instance, names, addresses collected by a non-governmental organization or NGO for academic research that may also be used by the same NGO for targeted commercial activity.

(iv) Other categories of exemptions that have been incorporated by some jurisdictions

a. Regulatory activity (UK[291], Malaysia[292]);
b. Discretionary exemptions by a Data Protection Authority or minister (Singapore[293], Malaysia[294]);
c. Exemptions for small businesses (for e.g. Australia exempts small business operators which have a turnover of less than AUD 3 million, however, there are no exemptions for processing of health data) [295]; Further, some considerations such as (1) the size,

[286] Sections 4 and 5, Collection of Statistics Act.
[287] Section 8, Collection of Statistics Act.
[288] Section 100, 101, Italian Personal Data Protection Code, 2003.
[289] Section 27(1)(d), POPI Act.
[290] Section 33, UK DPA does not provide a blanket exemption for this category. Data protection principles such as the requirement to keep data secure etc. would still apply.
[291] Section 31, UK DPA.
[292] Section 45(2)(e), Personal Data Protection Act, 2010.
[293] Section 62, Singapore Act.
[294] Section 46, Personal Data Protection Act, 2010.
[295] Sections 6C, 6D and 6E, Privacy Act.

scope and nature of business, (2) the nature and amount of data stored, and (3) the need to ensure confidentiality of employee data, will have to be suitably provided in law;[296]

d. Important economic and financial interests of a public body (South Africa);[297]

e. Processing in pursuance of an order of a court.[298]

(v) Investigation and detection of crime

In India, several laws such as the Code of Criminal Procedure, 1973 (CrPC), the Unlawful Activities (Prevention) Act, 1967, the National Investigation Agency Act, 2008, the Prevention of Money Laundering Act, 2002 (PMLA) etc. empower law enforcement agencies and police officers to collect personal information for the purpose of investigation of a crime. The process of search and seizure for the purpose of criminal investigation can be understood from the perspective of certain criminal law legislation in India. For instance, Section 91 of the CrPC provides power to a Court or a police officer in charge of a police station to issue summons, or an order in writing, to an individual in possession of a document or thing to produce such documents or things if it is 'necessary or desirable for the purpose of any investigation, inquiry, trial or other proceeding under this Code.' Section 93 of the CrPC empowers the Court to issue a 'search warrant' to compel individuals to produce the necessary documents or things in certain circumstances.

Further, the PMLA provides powers of search and seizure to a 'Director or any other officer not below the rank of Deputy Director.'[299] The authorised officer under this provision may seize any record[300] or property found during the course of search, and may even retain the seized property or record if the retention is necessary for to conduct an inquiry under the PMLA.[301] The PMLA also provides certain safeguards to ensure that the powers listed above are not exercised arbitrarily. Section 62 of the PMLA provides a penalty for officers exercising their powers of search and seizure without reasons in writing.

Similarly, information 'which would impede the process of investigation or apprehension or prosecution of offenders' is exempted from disclosure under the Right to Information Act, 2005 (RTI Act).[302] This refers to information about 'targets of investigation' or an 'accused'. The term has been interpreted to include investigation during disciplinary proceedings, investigation by income tax authorities, etc.

In the UK DPA, the purposes specified for this exemption are – 'prevention or detection of crime'; or 'apprehension or prosecution of offenders'; or 'assessment or collection of any tax

---

[296] Oracle, Massachusetts Data Security Law Signals New Challenges In Personal Information Protection, Oracle White Paper (August 2010), available at: http://www.oracle.com/us/products/database/data-security-ma-201-wp-168633.pdf, (last accessed 17 November 2017).
[297] Section 37(2)(c), POPI Act.
[298] For instance, Section 35, UK DPA.
[299] Section 17, PMLA.
[300] 'Records' include the records maintained in the form of books or stored in a computer or such other form as may be prescribed, Section 2(w), PMLA.
[301] Section 20 and 21, PMLA.
[302] Section 8(1)(h), RTI Act.

of imposition of similar nature.' The exemption is available when the data is being processed for the above purposes, and complying with all data protection obligations such as giving privacy notices, subject access, rectification, data retention, etc. would impede the said investigation or apprehension/prosecution. The onus is on the data controller to prove that adhering to the aforesaid principles would prejudice the investigation or prosecution.[303] The EU GDPR provides restrictions for the purpose of 'the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.'[304] This exemption enables law enforcement authorities to secure access to information that may be necessary for conducting investigations in accordance with a law.

(vi) National security or security of State and other similar grounds

As has been stated in *Puttaswamy*, the State may have an interest in placing reasonable limits on informational privacy in the interest of national security, security of state and other similar grounds. Other grounds could include objectives such as upholding the sovereignty and integrity of India, maintaining friendly relations with foreign states, maintenance of public order and preventing incitement to the commission of offences. Some of these terms are not precise and may have to be examined on a case by case basis.[305] For example an act of sedition (Section 124-A of the Indian Penal Code, 1860 or IPC) or rioting (Section 146) is considered to be "an offence against the State", as it undermines or affects the security of the State.[306]

Processing of information in the interest of national security, or the security of the State and to prevent incitement to an offence is permissible as long as the law enforcement authority or the Government is able to demonstrate that processing of the information is necessary to achieve the purpose. The challenge lies in ensuring that the derogations to an individual's right to privacy must be permissible only if it is necessary for these objectives.[307] Further, procedural safeguards to ensure non-arbitrariness (specially in state surveillance) should be devised.

At present, under the Telegraph Act and the IT Act, surveillance orders are subject to executive review. For instance, as per Rule 419A of the Indian Telegraph Rules, 1951 provides the procedure for telephone tapping authorised by the Government. An order for interception must be sanctioned by the Home Secretary at the Centre or the Home Secretary in the concerned State. In certain unavoidable circumstances, an order may be issued by an

[303] *R v. Secretary of State*, [2003] EWHC 2073.
[304] Article 32(1)(d), EU GDPR.
[305] *Santokh Singh v. Delhi Administration*, 1973 AIR 1091. Furthermore, *Ram Manohar Lohia v. State of Bihar*, 966 AIR 740, suggests that one has to imagine three concentric circles. Law and order represents the largest circle. Public Order is a smaller circle within that, and the smallest circle is Security of the State. Therefore, an action, which may affect the law and order of a State, may not affect Public Order, just as an act, which affects the Public Order of a State, may not affect the Security of a State.
[306] *Romesh Thappar v. State of Madras*, 1950 AIR 124
[307] *ZZ v. Secretary of State for the Home Department*, C-300/11 (2013), European Court of Justice, paragraph 61; *European Commission v. Italian Republic*, C-239/06 (2009), European Court of Justice, paragraph 50.

officer not below the rank of a Joint Secretary to the Government of India, who has been authorised by the Home Secretary (Union or State) to this effect. Similarly, the UK DPA provides for National Security Certificates.[308] These Certificates are issued by a Minister of the Crown and have been subject to judicial review in the past. The law will have to take into consideration the extent of authority to be given to the executive or the judiciary to issue and implement the national security exemption.

Similarly in the case of the Aadhaar Act, some of the data protection principles outlined in the said Act, particularly confidentiality of identity information and authentication records of individuals, and the bar on disclosure of information stored in the CIDR or authentication records may be relaxed if the disclosure of such information is in the interest of national security.[309] In such cases, the said relaxations may be made only upon a direction/order issued by an authorised officer, not below the rank of a Joint Secretary of the Central Government.[310] Further, it has been provided that every direction issued in this category must be reviewed by an Oversight Committee consisting of the Cabinet Secretary and Secretaries of the Ministries of Law and Justice and Electronics and Information Technology of the Central Government.[311]

Section 28 of the UK DPA exempts personal data from provisions of the legislation (rights of data subject, enforcement, notification) if such data is required for the purpose of safeguarding national security. It can be seen that the UK DPA does not provide clarity on the scope of the operation of this exemption, and that the 'determination has passed on to the data processors themselves.'[312] Other jurisdictions which provide the national security exemption are EU[313] and South Africa.[314] Further, in Canada, as per the PIPEDA, organisations are permitted to disclose personal information of an individual to a government institution or an authorised representative, without her knowledge and consent if such information relates to national security, the defence of Canada or the conduct of international affairs.

Several government and private entities are involved in national security functions. These functions include anti-terror operations, providing data/intelligence for these functions, data-mining etc. For instance, personal data is collected or retained by airport officials during security searches/body scans, data being sourced by intelligence agencies from other government agencies/Ministries/private and public databases for the purpose of anti-terror operations. A clear classification will have to be made in law in order to ensure that specific agencies are exempted from the operation of the proposed data protection law, partially or entirely. Any such exemption should be subject to strict safeguards, such as, a judicial

[308] Section 28(2), UK DPA.
[309] Section 33(2), Aadhaar Act.
[310] Section 33(2), Aadhaar Act.
[311] Proviso to Section 33(2), Aadhaar Act.
[312] Stephen A. Oxman, 'Exemptions to the European Union Personal Data Privacy Directive: Will They Swallow the Directive?', 24(1) Boston College International and Competition Law Review 191 (2000).
[313] Article 23, EU GDPR.
[314] Section 6(1)(c)(i), POPI Act.

mechanism to provide prior approval invoking such a clause, similar to the Court as envisaged under the Foreign Intelligence Surveillance Act, 1978 (FISA) in the US.[315]

7.3 Provisional Views

1. A wide exemption may be provided for data processed for household purposes.

2. A wide exemption may be provided for data processed for journalistic/artistic and literary purposes. However, the requirement to have adequate security and organisational measures for protecting data against unauthorised access should be applicable.

3. An exemption may be provided for data processed for the purpose of academic research, statistics and historical purposes. However, adequate safeguards may be incorporated in law to ensure that the data is being used for a bonafide purpose, and has been lawfully obtained. The law must provide for adequate security and organizational safeguards in the handling of such data.

4. The law may provide exemptions for the following purposes/processing activities: (i) information collected for the purpose of investigation of a crime, and apprehension or prosecution of offenders; (ii) information collected for the purpose of maintaining national security and public order.

5. The exemptions must be defined in a manner to ensure that processing of data under the exemptions is done only for the stated purpose. Further, it must be demonstrable that the data was necessary for the stated purpose.

6. In order to ensure that the exemptions are reasonable and not granted arbitrarily, an effective review mechanism must be devised.

7.4 Questions

1. What are the categories of exemptions that can be incorporated in the data protection law?

2. What are the basic security safeguards/organisational measures which should be prescribed when processing is carried out on an exempted ground, if any?

[315] The Foreign Intelligence Surveillance Court (FISC) is a high powered Court, which has the jurisdiction to "hear applications for and grant orders approving electronic surveillance anywhere within the United States" as per Section 103, FISA. The FISC decides whether the government requests for electronic surveillance, physical searches, access to business records, pen registers and trap and trace devices for "foreign intelligence purposes" should be approved. To get such a request approved, the government has to prove that the information is relevant to an investigation in order to protect against "international terrorism or clandestine intelligence activities".

Domestic /Household Processing

1. What are your views on including domestic/household processing as an exemption?

2. What are the scope of activities that will be included under this exemption?

3. Can terms such as ‘domestic’ or ‘household purpose’ be defined?

4. Are there any other views on this exemption?

Journalistic/Artistic/ Literary Purpose

1. What are your views on including journalistic/artistic/literary purpose as an exemption?

2. Should exemptions for journalistic purpose be included? If so, what should be their scope?

3. Can terms such as ‘journalist’ and ‘journalistic purpose’ be defined?

4. Would these activities also include publishing of information by non-media organisations?

5. What would be the scope of activities included for ‘literary’ or ‘artistic’ purpose? Should the terms be defined broadly?

6. Are there any other views on this exemption?

Research/Historical/Statistical Purpose

1. What are your views on including research/historical/statistical purpose as an exemption?

2. Can there be measures incorporated in the law to exclude activities under this head which are not being conducted for a bonafide purpose?

3. Will the exemption fail to operate if the research conducted in these areas is subsequently published/ or used for a commercial purpose?

4. Are there any other views on this exemption?

Investigation and Detection of Crime, National Security

1. What are your views on including investigation and detection of crimes and national security as exemptions?

2. What should be the width of the exemption provided for investigation and detection of crime? Should there be a prior judicial approval mechanism before invoking such a clause?

3. What constitutes a reasonable exemption on the basis of national security? Should other related grounds such as maintenance of public order or security of State be also grounds for exemptions under the law?

4. Should there be a review mechanism after processing information under this exemption? What should the review mechanism entail?

5. How can the enforcement mechanisms under the proposed law monitor/control processing of personal data under this exemption?

6. Do we need to define obligations of law enforcement agencies to protect personal data in their possession?

7. Can a data protection authority or/and a third-party challenge processing covered under this exemption?

8. What other measures can be taken in order to ensure that this exemption is used for bona fide purposes?

9. Are there any other views on these exemptions?

Additional Exemptions

1. Should 'prevention of crime' be separately included as ground for exemption?

2. Should a separate exemption for assessment and collection of tax in accordance with the relevant statutes be included?

3. Are there any other categories of information which should be exempt from the ambit of a data protection law?

CHAPTER 8: CROSS-BORDER FLOW OF DATA

8.1 Introduction

Data is the pulse of the modern global economy. With the advent of the Internet, huge quantities of personal data relating to employees and customers are being transferred internationally. Such data transfers often occur between and among units of the same corporate enterprise that are located in different countries as many of these global enterprises have customer databases and storage facilities in a number of regional locations.[316] Cross-border flow of data is vital to accessing valuable digital services. Providing strong rules to protect cross-border data flows is vital for small and medium sized enterprises or SMEs, consumers, and multi-national businesses.[317]

Anupam Chander in his article entitled 'Data Nationalism'[318] depicts the imagination of an Internet where data must stop at national borders, and it is examined to see whether it should be allowed to leave the country and is possibly taxed when it does. He warns that while it may sound fanciful, this is precisely the impact of various measures undertaken or planned by many nations to curtail the flow of data outside their borders.[319] Businesses use data to enhance research and development, develop new products and services, create new production or delivery processes, improve marketing, and establish new organizational and management approaches.[320] In order for companies to do business, be innovative, and stay competitive in global markets, they need to be able to send not only goods, capital, and competence (of people) across borders, but also data. If there are favourable laws facilitating cross-border data flows, it will greatly foster research, technology development and economic growth.[321]

8.2 Issues and International Practices

European Union

[316] David Bender and Larry Ponemon, 'Binding Corporate Rules for Cross-Border Data Transfer' 3(2) Rutgers Journal of Law & Urban Policy 154, 171 (2006).
[317] Coalition of Services Industries, 'Cross-Border Data Flows', available at: https://servicescoalition.org/services-issues/digital-issues/cross-border-data-flows (last accessed 30 October 2017).
[318] Anupam Chander and Uyên P. Lê, 'Data Nationalism', 64 Emory Law Journal 677, 680 (2015) available at: http://law.emory.edu/elj/_documents/volumes/64/3/articles/chander-le.pdf (last accessed 31 October 2017).
[319] Anupam Chander and Uyên P. Lê, 'Data Nationalism', 64 Emory Law Journal 677, 680 (2015) available at: http://law.emory.edu/elj/_documents/volumes/64/3/articles/chander-le.pdf (last accessed 31 October 2017).
[320] OECD, 'Exploring Data-Driven Innovation as a New Source of Growth: Mapping The Policy Issues Raised By "Big Data', OECD Digital Economy Papers No.222 (June 2013), available at: http://www.kooperation-international.de/uploads/media/OECD.DEP.No.222.pdf (last accessed 31 October 2017).
[321] Joshua Meltzer, 'The Internet, Cross-Border Data Flows and International Trade', 22 Issues in Technology Innovation, Brookings Center for Technology Innovation (February 2013), available at: https://www.brookings.edu/wp-content/uploads/2016/06/internet-data-and-trade-meltzer.pdf, (last accessed 20 November 2017).

To facilitate the cross-border transfers of data, the EU has created three mechanisms. These include the 'adequacy test' as set out under Article 45 of the EU GDPR,[322] Model Contractual Clauses[323] and Binding Corporate Rules (BCR).[324]Additionally, cross-border transfers of data between the EU and the US is done by way of the Privacy Shield Framework. Each of these will be discussed in greater detail below.

In the following section we provide an analysis of the various sets of data protection and transfer laws that are applicable across the globe.

(i) Adequacy Test

Article 45 of the EU GDPR[325] provides for an adequacy test for transfer of personal data to a third country. This test stipulates that personal data of EU subjects to non-European Economic Area or EEA countries is not permitted unless those countries are deemed to have an "adequate" level of data protection. While making this decision, the European Commission will examine whether the country to which data is intended to be transferred has data protection rules in place; whether they have effective and enforceable data protection rights and their effective administration; whether independent data protection supervisory authorities exist, who are vested with the power to ensure compliance; and finally, whether the country in question has entered into any international commitments with regard to data protection. Moreover, a periodic review of the adequacy standard must take place every four years.[326]

Under this provision, when assessing "the adequacy of the level of protection", the European Commission will take account of "rules for the onward transfer of personal data to another third country or international organization."[327] Further, this article allows transfers of personal data to third countries which do not have adequate data protection without the appropriate safeguards for the transfers as listed in Article 49,[328] if such transfer is necessary for important reasons of public interest.

Article 46 of the EU GDPR provides that if the European Commission has not made a decision with regard to the adequacy level of another country, a controller may transfer personal data only if appropriate safeguards are provided, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.[329] Appropriate safeguards can include (a) a legally binding and enforceable instrument between public authorities or bodies; (b) binding corporate rules in accordance with Article 47; (c) standard

[322]Article 45, EU GDPR.
[323] European Commission, 'Model Contracts for the Transfer of Personal Data to Third Countries', available at: http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm (last accessed 30 October 2017).
[324] European Commission, 'Overview on Binding Corporate Rules', available at: http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/index_en.htm (last accessed 30 October 2017).
[325] Article 45, EU GDPR.
[326] Article 45(3), EU GDPR.
[327] Article 45(2)(a), EU GDPR.
[328] Article 49, EU GDPR.
[329] Article 46, EU GDPR.

data protection clauses adopted by the European Commission[330] (d) standard data protection clauses adopted by a supervisory authority and approved by the Commission[331] (e) an approved code of conduct pursuant to Article 40; or (f) an approved certification mechanism pursuant to Article 42 together with binding and enforceable commitments of the controller. At present, the European Commission has deemed Andorra,[332] Argentina,[333] Canada,[334] Switzerland,[335] Faeroe Island,[336] Guernsey,[337] Israel,[338] Isle of Man,[339] Jersey,[340] New Zealand,[341] Uruguay[342] and the US (via the Privacy Shield) to be adequate.

[330] Article 93(2), EU GDPR.
[331] Article 93(2), EU GDPR.
[332] Commission Decision dated 19 October 2010 and notified under document C(2010) 7084, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32010D0625 (last accessed 30 October 2017); Article 29 Data Protection Working Party, 'Opinion 7/2009 on the level of protection of personal data in the Principality of Andorra', European Commission (1 December 2009), available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2009/wp166_en.pdf (last accessed 30 October 2017).
[333] Commission Decision dated 30 June 2003 and notified under document (2003/490/EC), available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1415636698083&uri=CELEX:32003D0490 (last accessed 30 October 2017); Article 29 Data Protection Working Party, 'Opinion 4/2002 by the Working Party on the level of protection of personal data in Argentina', European Commission (3 October 2002), available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2002/wp63_en.pdf (last accessed 30 October 2017).
[334] Commission Decision dated 20 December 2001 and notified under document 2002/2/EC, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32002D0002&qid=1415699250815 (last accessed 17 November 2017); Article 29 Data Protection Working Party, Opinion 2/2001 on the adequacy of the Canadian Personal Information and Electronic Documents Act, European Commission (26 January 2001), available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2001/wp39_en.pdf (last accessed 30 October 2017).
[335] Commission Decision dated 26 July 2000 and notified under document C (2000) 2304, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1415700329280&uri=CELEX:32000D0518 (last accessed 17 November 2017); Working Party on the Protection of Individuals with regard to the Processing of Personal Data, 'Opinion No. 5/99 on The level of protection of personal data in Switzerland', European Commission (7 June 1999), available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/1999/wp22_en.pdf (last accessed 17 November 2017).
[336] Article 29 Data Protection Working Party, 'Opinion 9/2007 on the level of protection of personal data in the Faroe Islands', European Commission (9 October 2007), available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2007/wp142_en.pdf (last accessed 30 October 2017).
[337] Commission Decision dated 21 November 2003, and notified under document number C(2003) 4309, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1415701941268&uri=CELEX:32003D0821 (last accessed 30 October 2017); Article 29 Data Protection Working Party, 'Opinion 5/2003 on the level of protection of personal data in Guernsey', European Commission (13 June 2003), available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2003/wp79_en.pdf (last accessed 30 October 2017).
[338] Commission Decision dated 31 January 2011, and notified under document C(2011) 332, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1415701992276&uri=CELEX:32011D0061 (last accessed 30 October 2017); Article 29 Data Protection Working Party, 'Opinion 6/2009 on the level of protection of personal data in Israel', European Commission (1 December 2009), available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2009/wp165_en.pdf (last accessed 30 October 2017).
[339]Commission Decision dated 28 April 2004, and notified under document C(2004) 1556; available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1415702956426&uri=CELEX:32004D0411 (last accessed 30 October 2017); Article 29 Data Protection Working Party, 'Opinion 6/2003 on the level of protection of personal data in the Isle of Man', European Commission (21 November 2003), available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2003/wp82_en.pdf (last accessed 30 October 2017).
[340]Commission Decision dated 8 May 2008, notified under document C(2008)1746, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1415703064772&uri=CELEX:32008D0393 (last accessed 30 October 2017); Article 29 Data Protection Working Party, 'Opinion 8/2007 on the level of protection of personal

(ii) Binding Corporate Rules

BCR are internal rules (such as codes of conduct) which are adopted by a multi-national group of companies. BCRs define the global policy of the multi-national group of companies with regard to the international transfers of personal data within the same corporate group, to entities located in countries, which do not provide an adequate level of protection.[343] Multinational companies use BCRs in order to adduce adequate safeguards for the protection of the privacy and fundamental rights and freedoms of individuals within the meaning of Article 47 of the EU GDPR.[344]

(iii) Model Contractual Clauses

The European Commission has the power to decide that certain standard contractual clauses offer sufficient safeguards with respect to data protection while undertaking transfer of data to non-EU/EEA countries.[345] As of date, the European Commission has issued two sets of standard contractual clauses: one for transfers from data controllers to data controllers established outside the EU/EEA; and one set for the transfer to processors established outside the EU/EEA.[346] Transfers of data made under these contracts are deemed to be protected under the EU GDPR. Since it is often difficult for stakeholders to comply with the 'adequate level' of protection for cross-border data transfers, alternatives such as Model Contract Clauses may play a crucial role in practice. The use of these alternatives should be facilitated for data controllers in any Member State.

---

data in Jersey', European Commission (17 November 2007), available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2007/wp141_en.pdf (last accessed 30 October 2017).

[341]Commission Decision dated 19 December 2012 on the level of protection of personal data by New Zealand, notified under document C (2012) 9557, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1415703506367&uri=CELEX:32013D0065 (last accessed 30 October 2017); Article 29 Data Protection Working Party, 'Opinion 11/2011 on the level of protection of personal data in New Zealand', European Commission (4 April 2011), available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp182_en.pdf (last accessed 30 October 2017).

[342]Commission Decision dated 21 August 2012, on the level of protection of personal data by the Eastern Republic of Uruguay, notified under document C (2012) 5704, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1417090893822&uri=CELEX:32012D0484 (last accessed 30 October 2017); Article 29 Data Protection Working Party, 'Opinion 6/2010 on the level of protection of personal data in the Eastern Republic of Uruguay', European Commission (12 October 2010), available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp177_en.pdf (last accessed 30 October 2017).

[343] European Commission, 'Overview on Binding Corporate Rules', available at: http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/index_en.htm (last accessed 30 October 2017).

[344] European Commission, 'Overview on Binding Corporate Rules', available at: http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/index_en.htm (last accessed 30 October 2017).

[345] European Commission, 'Frequently Asked Questions Relating to Transfers of Personal Data From The EU/EEA To Third Countries', 11, (2009), available at: http://ec.europa.eu/justice/policies/privacy/docs/international_transfers_faq/international_transfers_faq.pdf (last accessed 29 October 2017).

[346] European Commission, 'Model Contracts for the Transfer of Personal Data to Third Countries', available at: http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm (last accessed 30 October 2017).

(iv) Privacy Shield

There are two Privacy Shield frameworks: (i) the EU-US Privacy Shield Framework, which is deemed adequate by the European Commission to enable data transfers between the EU and the US; and (ii) the Swiss-US Privacy Shield Framework, which is deemed adequate by the EU to enable data transfers between Switzerland and the US. In order to join either framework, US organisations wishing to engage in data transfers must self-certify their adequacy to the Department of Commerce and publicly commit to the framework requirements.[347]

South Africa

In South Africa, the POPI Act provides that a 'responsible party' in South Africa cannot transfer personal information about a data subject to a third party in a foreign country, unless the recipient is subject to a law, binding corporate rules or any other binding agreement which provides substantially similar conditions for lawful processing of personal information relating to a data subject. A 'responsible party' can also transfer personal information about a data subject to a third party in a foreign country if the following conditions are met: (i) if the data subject consents to such a transfer; (ii) if the transfer is necessary for the performance of a contract; (iii) if the transfer is for the benefit of the data subject and it is not practicable to obtain the consent of the data subject for that transfer.[348]

Australia

In Australia, the Privacy Act provides that where an entity discloses personal information about an individual to an overseas recipient, then the APPs will apply. An entity could mean an agency or an organisation (it is another term for data controller). APP 8 applies to the cross-border disclosure of personal information.[349] This principle provides that before an APP entity discloses personal information about an individual to a person (the overseas recipient), who is not located in Australia or if it discloses to someone who is not the data subject, the entity must take such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the APPs.[350] As an exception to this, APP entities are permitted to disclose personal information to the overseas recipient if: (i) the entity reasonably believes that the recipient is subject to a law, or binding scheme which has the overall effect of protecting the information in a way which is substantially similar to the way in which the APPs protect the information; and (ii) that there are mechanisms in place which allow the

[347] US Department of Commerce, 'Fact-Sheet: Overview of EU-US Privacy Shield Framework' (12 July 2016), available at: https://www.commerce.gov/sites/commerce.gov/files/media/files/2016/fact_sheet-_eu-us_privacy_shield_7-16_sc_cmts.pdf, (last accessed 30 October 2017).
[348] Section 72, POPI Act.
[349] APP 8, Privacy Act.
[350] OAIC, 'Chapter 8: APP 8 — Cross-border disclosure of personal information' (March 2015), available at: https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-8-app-8-cross-border-disclosure-of-personal-information, (last accessed 29 October 2017).

individual to take action to enforce the law or that binding scheme.[351] Additionally, an entity is allowed to disclose personal information to an overseas recipient if she consents to such disclosure, or if such disclosure is pursuant to an order of a court. Disclosure to overseas recipients is also allowed if the entity reasonably believes that the disclosure of the information is reasonably necessary for the enforcement related activities conducted by an enforcement body.[352]

Canada

In Canada, PIPEDA does not prohibit the outsourcing of personal information to another jurisdiction, whether by the private sector or a federal institution.[353] Canada follows an organisation-to-organisation approach while dealing with the cross-border transfer of information. Under the PIPEDA, organisations are held accountable for the protection of personal information transfers under each individual outsourcing arrangement or contract.[354] The Privacy Commissioner investigates complaints and investigates the personal information handling practices of organisations.[355]Principle 1 Schedule 1 of PIPEDA addresses the balance between the protection of personal information of individuals and the business necessity of transferring personal information for various reasons, including the availability of service providers, efficiency and economy.[356] It places responsibility on an organization for protecting personal information under its control. Schedule 1 also provides that personal information may be transferred to third parties for processing, and requires organisations to use contractual or other means to "provide a comparable level of protection while the information is being processed by the third party."

Under the Canadian Model, no additional consent needs to be sought[357] for the cross-border transfer of personal information collected as long as the following conditions are met: (i) the information is being used for the purpose it was originally collected and to which the subject already consented; (ii) the entity transferring the information ensures that a comparable level of protection of the personal information is provided by the receiving entity; and (iii) the

[351] OAIC, Chapter 6: APP 6 — Use or disclosure of personal information (February 2014), available at: https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-6-app-6-use-or-disclosure-of-personal-information, (last accessed 30 October 2017).
[352] APP 8, Privacy Act.
[353] Office of the Privacy Commissioner of Canada, 'Personal Information Transferred Across Borders' (1 November 2016), available at: https://www.priv.gc.ca/en/privacy-topics/personal-information-transferred-across-borders/, (last accessed 30 October 2017).
[354] Office of the Privacy Commissioner of Canada, 'Personal Information Transferred Across Borders' (1 November 2016), available at: https://www.priv.gc.ca/en/privacy-topics/personal-information-transferred-across-borders/, (last accessed 30 October 2017).
[355] Office of the Privacy Commissioner of Canada, 'Personal Information Transferred Across Borders' (1 November 2016), available at: https://www.priv.gc.ca/en/privacy-topics/personal-information-transferred-across-borders/, (last accessed 30 October 2017).
[356] Office of the Privacy Commissioner of Canada, 'Personal Information Transferred Across Borders' (1 November 2016), available at: https://www.priv.gc.ca/en/privacy-topics/personal-information-transferred-across-borders/, (last accessed 30 October 2017).
[357] Norton Rose Fulbright, 'Global Data Privacy Directory' (July 2014), 97, available at: http://www.nortonrosefulbright.com/files/global-data-privacy-directory-52687.pdf, (last accessed 30 October 2017).

persons concerned are notified that their information will be transferred outside the jurisdiction.

Under this provision, cross-border transfer of personal information does not require additional consent concerned provided that the organisation is transparent and provides notice of the fact that: (i) such transfers occur; and (ii) once in the foreign jurisdiction, the information is subject to the power of the authorities in that jurisdiction.

8.3 Provisional Views

There are two tests identified for formation of laws related to cross border data flow, namely the adequacy test and the comparable level of protection test for personal data. In order to implement the adequacy test, there needs to be clarity as to which countries provide for an adequate level of protection for personal data. The data protection authority should be given the power to determine this. The adequacy test is particularly beneficial because it will ensure a smooth two-way flow of information, critical to a digital economy.[358] In the absence of such an adequacy certification, the onus would be on the data-controller to ensure that the transfer is subject to adequate safeguards and that the data will continue to be subject to the same level of protection as in India. However, an adequacy framework would require a proactive data protection authority that needs to actively monitor the developments of law and practice around the world.

8.4 Questions

1. What are your views on cross-border transfer of data?

2. Should the data protection law have specific provisions facilitating cross border transfer of data? If yes, what should the adequacy standard be the threshold test for transfer of data?

3. Should certain types of sensitive personal information be prohibited from being transferred outside India even if it fulfils the test for transfer?

4. Are there any other views on cross-border data transfer which have not been considered?

[358] Vili Lehdonvirta. 'European Union Data Protection Directive: Adequacy of Data Protection in Singapore,' Singapore Journal of Legal Studies, 511 (2004), available at: http://vili.lehdonvirta.com/wp-content/uploads/2015/02/Lehdonvirta-2004-Adequacy-of-Data-Protection-in-Singapore.pdf, (last accessed 1 November 2017).

CHAPTER 9 : DATA LOCALISATION

9.1 Introduction

Data localisation requires companies to store and process data on servers physically located within national borders. Governments across the globe driven by concerns over privacy, security, surveillance and law enforcement have been enacting legislations that necessitate localisation of data. A nation has the prerogative to take measures to protect its interests and its sovereignty, but it must carefully evaluate the advantages and dangers of locally storing data before taking a firm decision on an issue has the potential to cause a major ripple effect across a number of industries.

9.2 Issues

(i) Protecting Rights of Data Subjects

Enacting a data localisation law may help in ensuring the protection of the rights of data subjects in some circumstances. For instance in the Microsoft case, it was held that US's Stored Communications Act cannot be applied extraterritorially, and can only be applied to data which is actually stored in the country.[359] This case referred to whether the government, by way of a warrant issued under the Stored Communications Act could request Microsoft to access and produce emails of a customer whose data was stored on a server in Ireland.[360]

(ii) Preventing Foreign Surveillance

One of the primary reasons for enacting a data localisation law is to prevent foreign surveillance. It is grounded in the belief that placing data abroad would allow foreign governments to impinge upon the privacy and security of the data of domestic nationals.[361] This has led to some countries attempting to keep data from leaving their shores, in order to protect it from falling into the hands of other governments.[362] While, a data localisation mandate may be effective in reducing foreign surveillance as data will be stored locally, such a mandate may increase the risk of local surveillance by law enforcement agencies.

(iii) Easy Access of Data in Support of Law Enforcement and National Security

Currently, jurisdictional claims against foreign entities are enforced through Mutual Legal Assistance Treaties.[363] The presence of personal information in the territory of a country

[359] *Microsoft Corporation v. United States of America*, No. 14-2985 (2d Cir. 2016).
[360] *Microsoft Corporation v. United States of America*, No. 14-2985 (2d Cir. 2016).
[361] Jonah Force Hill, 'The Growth Of Data Localization Post-Snowden: Analysis And Recommendations For U.S. Policymakers And Business Leaders', The Hague Institute for Global Justice, Conference on the Future of Cyber Governance 2014, 5 (1 May 2014) as cited in Erica Fraser, 'Data Localisation and the Balkanisation of the Internet', 13(3) SCRIPTed 359 (December 2016).
[362] Anupam Chander and Uyên P. Lê, 'Breaking the Web: Data Localisation vs. the Global Internet' UC Davis Legal Studies Research Paper No. 378, (April 2014).
[363] Andrew Keane Woods, 'Against Data Exceptionalism', 68(4) Stanford Law Review 729, 748 (April 2016).

could trigger the territorial basis for jurisdiction, thus giving additional powers to police and other law enforcement agencies. If data is locally stored in India, enforcement agencies will have access to a larger pool of data. This data could aid counter-terrorism efforts and may help protect national security. Further, local storage of data will ensure easier access to data in contradistinction to foreign storage of data wherein the sovereign power may choose not to grant access to Indian law enforcement agencies.

9.3 Industry Perspective

(i) Expensive, Reduces Foreign Investments and it is difficult to distinguish data

It is expensive to comply with a localisation mandate as local servers and data centres have to be created.[364] Economy-wide data localisation requirements have lead to a negative impact on GDP in several countries where such requirements have been considered (Brazil -0.8%, India -0.8% and Republic of Korea -1.1%) or implemented (Indonesia -0.7%).[365] A study indicates that it is hard to distinguish personal data from non-personal data for purposes of data localisation.[366] Data localisation measures are often motivated by the desire to promote local economic development. In fact, however, data localisation raises costs for local businesses, reduces access to global services for consumers, hampers local start-ups, and hinders access to the use of the latest technological advances. Data localisation also affects business continuity and disaster recovery management as having an offshore location helps mitigate domestic disruptions. The domestic benefits of data localisation go to the few owners and employees of data centres, and the few companies servicing these centres locally. Meanwhile, the harms of data localisation are widespread, felt by small, medium, and large businesses that are denied access to global services that might improve productivity.

(ii) Role of Data Transfers in Trade of Goods and Services

"Cross border data transfer" is a broad concept, which involves international cooperation in "data processing", storage, retrieval[367] and transmission borders. The ability to move data rapidly and globally has been a key building block of the global economic order and a legislation with a data localisation restricting the movement of data could become a burden for companies across all sectors of industry.

---

[364] Matthias Bauer *et al.*, 'Data Localisation in Russia: A self-imposed sanction', ECIPE No. 6/2015 (2015), available at:http://www.ecipe.org/app/uploads/2015/06/Policy-Brief-062015_Fixed.pdf, (last accessed 12 October 2017).

[365] United Nations Conference on Trade & Development (UNCTAD), 'Data Protection Regulations and International Data Flows: Implications for Trade and Developments' (2016), available at: http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf ,(last accessed 12 October 2017).

[366] Neha Mishra, 'Data Localisation Laws in a Digital World- Data Protection or Data Protectionism?', Public Sphere, 141 (2016), available at: http://publicspherejournal.com/wp-content/uploads/2016/02/06.data_protection.pdf, (last accessed 17 November 2017); referring to Matthias Bauer *et al.*, 'The Economic Importance of Getting Data Protection Right: Protecting Privacy, Transmitting Data, Moving Commerce', ECIPE for U.S Chamber of Commerce (March 2013).

[367] Retrieval is the process of identifying and extracting data from a database, based on a query provided by the user or application. It enables the fetching of data from a database in order to display it on a monitor and/or use within an application.

(iii) IT-BPO/BPM Industrial Growth

The Information Technology-Business Process Outsource (IT BPO) sector has become one of the most significant growth catalysts for the Indian economy. In addition to fuelling India's economy, this industry is also positively influencing the lives of its people through an active direct and indirect contribution to the various socio-economic parameters such as employment, standard of living and diversity among others.[368] Indian service sector grew at approximately eight percent per annum and contributed to about 66.1% of India's GDP in 2015–16.[369] The IT-BPO Industry has evolved over the past decade from offering Business Process Operations centric solutions to offering Business Process Management (BPM) solutions which involves services ranging from cloud computing to Internet of things based health care services. Data localisation requirements could severely impact the growth of this sector.

(iv) Industrialisation 4.0 and Internet of Things

Industrialisation 4.0 introduces what has been called the "smart factory," in which cyber-physical systems[370] monitor the physical processes of the factory and make decentralised decisions. Physical systems become Internet of Things, communicating and cooperating both with each other using machine to machine (M2M) communciations and with humans in real time via the wireless web. Industry 4.0 digitises and integrates processes across the entire organisation, from product development and purchasing, through manufacturing, logistics and services.[371] These evolutions are leading to the creation of new services such as remote factory management, and managed agriculture farm services. The Indian service sector is likely to gain from these developments. These services would scale up the transfer of data across the borders. A data localisation mandate could perhaps create hindrances in promoting India as a hub for new age services.

(v) Digitisation of Product and Service Offerings

Digitisation of products includes the expansion of existing products, e.g. by adding smart sensors or communication devices that can be used with data analytics tools, as well as the creation of new digitised products which focus on completely integrated solutions.

---

[368] Nagalakshmi, 'Role of BPO and its Impact on Indian Economy', Asia Pacific Journal of Research, available at: http://apjor.com/files/1369674671.pdf, (last accessed 27 October 2017).

[369] 'Services Sector', Chapter 7 Economic Survey (2015-2016), available at: http://indiabudget.nic.in/budget2016-2017/es2015-16/echapvol2-07.pdf, (last accessed 20 November 2017).

[370] Cyber-Physical Systems or "smart" systems are co-engineered interacting networks of physical and computational components. These systems will provide the foundation of our critical infrastructure, form the basis of emerging and future smart services, and improve our quality of life in many areas.
NIST, 'Cyber-Physical Systems' (2017), available at: https://www.nist.gov/el/cyber-physical-systems, (last accessed 30 October 2017).

[371] Bernard Marr, 'What Everyone Must Know About Industry 4.0', Forbes (2017) available at: https://www.forbes.com/sites/bernardmarr/2016/06/20/what-everyone-must-know-about-industry-4-0/#501f783e795f, (last Accessed 30 October 2017).

(vi) India as a Capital of Analytics Services

Analytics capabilities and solutions have over the years scaled up from descriptive analytics capabilities being used for reporting and business intelligence, to predictive[372] modelling and later moving to prescriptive[373] ones. India has been growing as an analytics hub which provides analytics solutions across different sectors- energy, healthcare, banking, telecom, insurance, agriculture, aviation, retail/e-commerce, hospitality and even NGOs.

(vii) Cloud Services Brokerage

Cloud services brokerage (CSB**)** is an IT role and business model in which a company or other entity adds value to one or more (public or private) cloud services on behalf of one or more consumers of that service via three primary roles including aggregation, integration and customisation brokerage.[374]

(viii) Global in-house centers (GICs)

GICs were first established in India during the late 1990s with a focus on cost reduction by utilising inexpensive technical resources and relatively affordable real estate. GICs are offshore centers that perform designated functions for large organizations. GICs in India now number about 1,100, employing more than 800,000 individuals and generating approximately USD 23 billion in revenue. GICs' ability to create cost savings for an enterprise while tapping India's talent pool have led to that impressive growth.[375] They have played a pivotal role in ushering in an age of data analytics and digital transformation. India currently has GICs operating across numerous sectors, including IT and Information Technology Enabled Services (ITeS), engineering and software development, banking, financial services and insurance, telecom etc., with growing concentration in the aerospace, healthcare, pharma, and biotech industries. Knowledge-based services particularly analytics, finance and accounting, and technical support services are the leading functions being carried out in India centers. Data localisation and restriction of cross-border data flows could have a severe impact on the growth of the GICs in India.

(ix) Impact on Indian start-up eco system

Most start-ups rely on the cloud to host their businesses and provide computational services at a low cost in order to be competitive. Instead of making the capital investment to buy huge

[372] Use of data, statistical algorithms and machine learning techniques to identify the likelihood of future outcomes based on historical data.
[373] Thomas H. Davenport, 'Analytics 3.0', Harvard Business Review (December 2013), available at: https://hbr.org/2013/12/analytics-30, (last accessed 20 November 2017).
[374] Daryl Plummer, 'Cloud Services Brokerage: A Must-Have for Most Organizations', Forbes (22 March 2012), available at: https://www.forbes.com/sites/gartnergroup/2012/03/22/cloud-services-brokerage-a-must-have-for-most-organizations/#21efd19e2c6e, (last accessed 20 November 2017).
[375] Arpan Sheth *et al.*, 'Global In-house Centers in India', Bain & Company (2017), available at: http://www.bain.com/publications/articles/global-in-house-centers-in-india.aspx, (last accessed 27 October 2017).

amounts of computer hardware, they use cloud servers to meet their needs. Cloud computing works because for most purposes, it is not relevant to a consumer where their data is stored, as long as it is always available to them in network terms. Data localisation laws, however, threaten this model of low-capital-investment, high-availability services. According to studies in countries that are considering or have considered forced data localisation laws, local companies would be required to pay 30-60% more for their computing needs than if they could go outside the country's borders.[376]

(x) Impact on development of telecommunication sector

India currently has a data localisation mandate with respect to customer account information in the telecom sector. From industry experience, this does cause some inconveniences with regard to international clearing house activities particularly with regard to global telecom companies that are looking to provide enterprise level telecom consolidation.

9.4 International Practices

Russia

Russia enacted Federal Law No. 242-FZ, which, mandates that all data operators in Russia ensure that the recording, systematisation, accumulation, storage, change and extraction of personal data of Russian citizens occurs with the use of data centres located in the territory of the Russian Federation during the course of collection of relevant personal data of individuals, including via the Internet. Therefore, any organisation which collects data relating to Russian citizens must be stored on servers or IT systems which are located in Russia. A data operator could mean a state or municipal body, a legal or a physical person that organises or carries out (alone or jointly with other persons) the personal data and determines the purposes of personal data processing and other operations relating to personal data. This law also requires data operators to notify the Russian Data Protection Authority, the Roskomnadzor, of the location of the server where the data is stored.[377]

China

In China, the primary law relating to data localisation is the Chinese Cybersecurity Law,[378] which partially came into force in June 2017. The crux of this law relating to data localisation is found in Article 37, which states that Chinese citizen's personal information and important data, which are collected and generated by critical information infrastructure (CII) operators in China must be stored domestically on Chinese servers. CII operators must also provide

[376] Erica Fraser, 'Data Localisation and the Balkanisation of the Internet', 13(3) SCRIPTed 359 (December 2016).
[377] Article 16(4)(7), Federal Law No. 242-FZ.
[378] Cybersecurity Law, 2016. An unofficial English translation of this legislation is available at: The National People's Congress of the People's Republic of China, People's Republic of China Network Security Law (2016), available at: http://www.npc.gov.cn/npc/xinwen/2016-11/07/content_2001605.htm, (last accessed 11 November 2017).

encryption keys to government authorities. CII while not explicitly defined, is understood to mean public communication and information services. Further, network operators or providers of network products which violate Article 37, will be ordered by the relevant departments to correct their actions. In the event that they fail to comply with these instructions, then the departments can issue warnings, confiscate illegal income and impose penalties. They can also suspend business operations, shut down websites and revoke business certificates or licenses.

Australia

In Australia, the Personally Controlled Electronic Health Records Act, 2012 provides that where a system operator, a registered repository operator, or a registered contracted service provider holds the health records of an individual, or has access to such records, then such records cannot be taken outside Australia. The system operator is not permitted to process, or allow such information to be processed, outside Australia. The system operator is also not permitted to allow another person to hold the records, or take records outside Australia, or to process information relating to the records outside Australia.[379]

Canada

In Canada, the PIPEDA does not contain any data localisation requirements. However, provincial law in Nova Scotia (Personal Information International Disclosure Protection Act, 2006) requires that personal information created by public institutions (such as government agencies, schools and hospitals) be stored on servers located within Canada.[380]

Vietnam

In Vietnam, the Decree on Management, Provision, and Use of Internet Services and Information Content Online[381] (Decree 72) requires a range of Internet service providers to maintain within Vietnam, a copy of any information they hold in order to facilitate the inspection of information by authorities, specifically providing that organisations and enterprises must have at least one server system in Vietnam serving the inspection, storage, and provision of information at the request of competent authorities.[382] Decree 72 applies to general websites, social networks, mobile networks, and game service providers.[383]

Indonesia

[379] Section 77, Personally Controlled Electronic Health Records Act, 2012.
[380] Section 5, Personal Information International Disclosure Protection Act, 2006.
[381] Decree on the management, provision and use of Internet services and online information (No. 72/2013/ND-CP).
[382] Article 24(2), Decree on Management, Provision and Use of Internet Services and Online Information (No. 72/2013), available at https://vnnic.vn/sites/default/files/vanban/Decree%20No72-2013-ND-CP.PDF, (last accessed 17 November 2017).
[383] Article 25(8) (social networks), Article 28(2) (mobile networks), Art. 34(2) (game service providers) of the Decree on Management, Provision and Use of Internet Services and Online Information (No. 72/2013), available at http://www.moit.gov.vn/Images/FileVanBan/_ND72-2013-CPEng.pdf, (last accessed 20 November 2017).

In Indonesia, the regulation regarding the Provision of Electronic System and Transactions[384] mandates the local storage of data relating to electronic system operators for public service. Further, Regulation 20/2016 on Personal Data Protection in Electronic System provides that electronic system providers are required to process protected private data only in data centers and disaster recovery centers located in Indonesia.[385]

9.5 Provisional Views

From these practices it emerges that certain countries have embraced data localisation in some form or manner. However, most countries, do not have a data localisation mandate. India will have to carefully balance the enforcement benefits of data localisation with the costs involved pursuant to such requirement. Different types of data will have to be treated differently, given their significance for enforcement and industry. It appears that a one-size-fits-all model may not be the most appropriate. Thus while data localisation may be considered in certain sensitive sectors, it may not be advisable to prescribe it across the board.

9.6 Questions

1. What are your views on data localisation?

2. Should there be a data localisation requirement for the storage of personal data within the jurisdiction of India?

3. If yes, what should be the scope of the localisation mandate? Should it include all personal information or only sensitive personal information?

4. If the data protection law calls for localisation, what would be impact on industry and other sectors?

5. Are there any other issues or concerns regarding data localisation which have not been considered above?

[384] Regulation (20/2016) on Personal Data Protection in Electronic Systems.
[385] Baker McKenzie, 'Indonesia: New Regulation on Personal Data Protection' (3 January 2017), available at: http://www.bakermckenzie.com/en/insight/publications/2016/12/new-implementing-regulation-personal-data/, (last accessed 10 November 2017).

CHAPTER 10: ALLIED LAWS

Currently, there are a variety of laws in India which contain provisions dealing with the processing of data, which includes personal data as well as sensitive personal data. Consequently, such laws may need to be examined against a new data protection law as and when such law comes into existence in India. These laws include but are not limited to the following:

Financial Sector

1. Banking Regulation Act, 1949
2. Credit Information Companies (Regulation) Act, 2005
3. Credit Information Companies Regulation, 2006
4. The Insolvency and Bankruptcy Code, 2016 and the regulations framed thereunder such as the Insolvency and Bankruptcy Board of India (Information Utilities) Regulations, 2017
5. Payment and Settlement Systems Act, 2007
6. Reserve Bank of India Act, 1934 as well as the circulars/directions/notifications issued by the RBI from time to time including but not limited to Master Direction on Know Your Customer (KYC), 2016,[386] Master Circular on Credit Card, Debit Card and Rupee Denominated Co-branded Prepaid Card Operations of Banks and Credit Card issuing NBFCs[387]; Master Circular on Customer Service in Banks, 2015[388]; and Master Circular on Policy Guidelines on Issuance and Operation of Pre-paid Payment Instruments in India[389]
7. The Security and Exchange Board of India Act, 1992 as well as the regulations made thereunder including but not limited to SEBI (Stock-Brokers and Sub-Brokers) Regulations, 1992, SEBI KYC (Know Your Client) Registration Agency Regulations, 2011 and SEBI (Investment Advisers) Regulations, 2013
8. Securities Contract (Regulation) Rules, 1957
9. Insurance Act, 1938 as well as regulations issued thereunder by the Insurance Regulatory and Development Authority of India (IRDAI) including but not limited to Insurance Regulatory and Development Authority of India (Sharing Of Database for

[386] RBI Master Direction on Know Your Customer (KYC) Direction, 2016 dated 25 February 2016, updated as on 8 July 2016, available at: https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=10292&Mode=0 (last accessed 13 November 2017). This Master Direction was amended by RBI Amendment to Master Direction dated 8 December 2016, available at https://rbi.org.in/scripts/NotificationUser.aspx?Mode=0&Id=10770 (last accessed 13 November 2017).

[387] RBI Master Circular on Credit Card, Debit Card and Rupee Denominated Co-branded Prepaid Card Operations of Banks and Credit Card issuing NBFCs, available at Master Circular on Credit Card, Debit Card and Rupee Denominated Cobranded Prepaid Card operations of banks dated 1 July 2014, available at: https://rbi.org.in/Scripts/BS_ViewMasCirculardetails.aspx?id=8998 , (last accessed 5 November 2017). Some parts of this Circular were amended by RBI Notification on Customer Protection on Limiting Liability of Customers in Unauthorised Electronic Banking Transactions dated 6 July 2017, available at: https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=11040&Mode=0 (last accessed 13 November 2017).

[388] RBI Master Circular on Customer Service in Banks, 2015 dated 1 July 2015, available at: https://rbi.org.in/scripts/BS_ViewMasCirculardetails.aspx?id=9862 (last accessed 14 November 2017).

[389] RBI Master Direction on Issuance and Operation of Prepaid Payment Instruments dated 11 October 2017 available at: https://rbi.org.in/scripts/NotificationUser.aspx?Mode=0&Id=11142 (last accessed 13 November, 2017).

Distribution of Insurance Products) Regulations, 2010, Circular on Submission of Insurance Data of IRDAI to Insurance Information Bureau of India (IIB)[390] and Guidelines on Information and Cyber Security for Insurers.[391]

Health Sector

10. The Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations, 2002
11. Pre-Conception and Pre-Natal Diagnostic Techniques (Prohibition of Sex Selection) Act, 1994
12. The Mental Health Act, 1987

Information Technology and Telecommunications Sector

13. The Indian Telegraph Act, 1885
14. The Telecom Regulatory Authority of India Act, 1997
    Information Technology Act, 2000, including, but not limited to the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, Information Technology (Intermediaries Guidelines) Rules, 2011 and the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009

Miscellaneous

15. The Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016 including Regulations made under the Act including but not limited to Aadhaar (Data Security) Regulations, 2016, Aadhaar (Sharing of Information) Regulations, 2016.
16. Census Act, 1948
17. Collection of Statistics Act, 2008
18. Consumer Protection Act, 1986
19. Persons with Disabilities (Equal Opportunities, Protection of Rights and Full Participation) Act, 1995
20. Right of Children to Free and Compulsory Education Act, 2009
21. Right to Information Act, 2005

Therefore, comments are invited from stakeholders on how each of these above laws, or any other relevant law not listed above, may need to be reconciled with the obligations for data processing introduced under the new data protection law.

[390] IRDAI Circular on Submission of Insurance Data of IRDA to Insurance Information Bureau of India (IIB) dated 20 June 2013, available at: https://iib.gov.in/IIB/circulars/Mandate%20for%20Insurance%20data.pdf (last accessed 13 November 2017).

[391] IRDAI Guidelines on Information and Cyber Security for Insurers dated 7 April 2017, available at: https://www.irdai.gov.in/ADMINCMS/cms/Uploadedfiles/07.04.2017-Guidelines%20on%20Information%20and%20Cyber%20Security%20for%20insurers.pdf (last accessed 13 November 2017).