WHITE PAPER OF THE COMMITTEE OF EXPERTS ON A DATA PROTECTION FRAMEWORK FOR INDIA

FOREWORD

The Government of India has set up our Committee of Experts to study various issues relating to data protection in India, make specific suggestions on principles underlying a data protection bill and draft such a bill. The objective is to ñensure growth of the digital economy while keeping personal data of citizens secure and protected.ò

The issue of data protection is important both intrinsically and instrumentally. Intrinsically, a regime for data protection is synonymous with protection of informational privacy. As the Supreme Court observed in *Puttaswamy*,

> ñ*Informational privacy is a facet of the right to privacy. The dangers to privacy in an age of information can originate not only from the state but from non-state actors as well. We commend to the Union Government the need to examine and put into place a robust regime for data protection. The creation of such a regime requires a careful and sensitive balance between individual interests and legitimate concerns of the state.*ò

Instrumentally, a firm legal framework for data protection is the foundation on which data-driven innovation and entrepreneurship can flourish in India. Fostering such innovation and entrepreneurship is essential if India is to lead its citizens and the world into a digital future committed to empowerment, experiment and equal access.

A carefully formulated data protection law is necessary for fulfilling both these objectives. It is our Committeeôs view that the law we draft must be cognisant of international and comparative practices in this regard. Doing otherwise in our increasingly interconnected world would be naïve. At the same time, the law must be acutely aware of the views of Indians, particularly the common man and woman, perhaps new to data but with clear views on right and wrong, benefit and harm.

To serve these two purposes, a White Paper has been drafted to solicit public comments on what shape a data protection law must take. The White Paper outlines the issues that a majority of the members of the Committee feel require incorporation in a law, relevant experiences from other countries and concerns regarding their incorporation, certain provisional views based on an evaluation of the issues vis-à-vis the objectives of the exercise, and specific questions for the public. On the basis of the responses received, we will conduct public consultations with citizens and stakeholders shortly to hear all voices that wish and need to be heard on this subject.

Since the task of identifying key data protection issues, examining international best practices and recommending a draft bill is a task of considerable magnitude, this White Paper is necessarily lengthy. However, for the benefit of those who may not have either the time or the

inclination to peruse the contents of the White Paper fully, a concise summary is provided in Part V, containing the key principles and questions for public consultation.

Drafting a data protection law for India is a complex exercise. But as the scriptures say:

वादे वादे जायते त□वबोध:

[From each debate, there arises knowledge of the Ultimate Principle]

With your inputs and our collective aim of both protecting and empowering citizens, we are certain that the law that India drafts will not only serve our own, but will also be a model for the world to adopt.

Chairman

Justice B.N. Srikrishna

Members

Smt. Aruna Sundararajan

Dr. Ajay Bhushan Pandey

Dr. Ajay Kumar

Prof. Rajat Moona

Dr. Gulshan Rai

Prof. Rishikesha Krishnan

Dr. Arghya Sengupta

Smt. Rama Vedashree

Submission of responses to this White Paper may be made through the Web Form available at:
https://innovate.mygov.in/data-protection-in-india/

In case you wish to submit written comments/feedback, same may be sent to:

Shri Rakesh Maheshwari
Scientist G & Group Co-ordinator, Cyber laws
Ministry of Electronics and Information Technology (MeitY),
Electronics Niketan, 6, CGO Complex,
Lodhi Road, New Delhi- 110003.

Submission made through the Web Form is preferred.

The deadline for submission of responses is 31st January, 2018.

TABLE OF CONTENTS

Foreword ..... **i**

PART I **1**

Context-Setting **1**
1. A Digital India in a Digital World 1
2. Data Protection: Genesis and Rationale 4
(i) Data Protection and the Value of Privacy 4
(ii) The Evolution of Privacy Principles 6
3. Comparative Approaches to Data Protection 10
4. Data Protection in India 14
(i) Judicial Developments on Right to Privacy 14
(ii) Legislative Developments 16
(iii) The AP Shah Committee Report 22
5. Possible Approaches 22

PART II **24**

Scope And Exemptions **24**

Chapter 1: Territorial And Personal Scope **24**
1.1. Introduction 24
1.2. Issues 24
1.3. International Practices 25
1.4. Enforceability of provisions of laws 27
1.5. Provisional Views 28
1.6. Questions 28

Chapter 2: Other Issues of Scope **30**
2.1 Natural/Juristic Persons 30
2.2 Horizontality of Application (Public versus Private Sector) 31
2.3 Retrospective Application 31
2.4 Provisional Views 32
2.5 Questions 32

Chapter 3: What is personal data? **34**
3.1. Introduction 34
3.2. Issues and International Practices 34
(i) Information or data? 34
(ii) Information about/relating an individual 35
(iii) Identified or Identifiable Individual 36
(iv) Pseudonymisation and Anonymisation 37
(v) Personal Data and New Technologies 37
(vi) A layered approach? 38
3.3. Provisional Views 39
3.4. Questions 39

Chapter 4: Sensitive personal data **41**
4.1 Introduction 41
4.2 Issues and International Practices 41
4.3 Provisional Views 43
4.4 Questions 43

Chapter 5: What is Processing? **44**
5.1 Introduction 44
5.2 Issues and International Practices 44
(i) Processing of Personal Data 44
(ii) Automated means versus manual processing 45
5.3 Provisional Views 46
5.4 Questions 46

Chapter 6: Entities to be defined in the law: Data Controller and Processor **48**
6.1 Introduction 48
6.2 Issues and International Practices 48
6.3 Provisional Views 50
6.4 Questions 50

Chapter 7: Exemptions for Household purposes, journalistic and literary purposes and research **52**
7.1 Introduction 52
7.2 Specific Exemptions and International Practices 53
(i) Personal or household purpose 53
(ii) Journalistic/Artistic/Literary purposes 53
(iii) Research/historical and statistical purposes 54
(iv) Other categories of exemptions that have been incorporated by some jurisdictions 55
(v) Investigation and detection of crime 56
(vi) National security or security of State and other similar grounds 57
7.3 Provisional Views 59
7.4 Questions 59

Chapter 8: Cross-Border Flow of Data **62**
8.1 Introduction 62
8.2 Issues and International Practices 62
(i) Adequacy Test 63
(ii) Binding Corporate Rules 65
(iii) Model Contractual Clauses 65
(iv) Privacy Shield 66
8.3 Provisional Views 68
8.4 Questions 68

Chapter 9 : Data Localisation **69**
9.1 Introduction 69
9.2 Issues 69
(i) Protecting Rights of Data Subjects 69
(ii) Preventing Foreign Surveillance 69
(iii) Easy Access of Data in Support of Law Enforcement and National Security 69
9.3 Industry Perspective 70
(i) Expensive, Reduces Foreign Investments and it is difficult to distinguish data 70
(ii) Role of Data Transfers in Trade of Goods and Services 70
(iii) IT-BPO/BPM Industrial Growth 71
(iv) Industrialisation 4.0 and Internet of Things 71
(v) Digitisation of Product and Service Offerings 71
(vi) India as a Capital of Analytics Services 72
(vii) Cloud Services Brokerage 72
(viii) Global in-house centers (GICs) 72
(ix) Impact on Indian start-up eco system 72

(x) Impact on development of telecommunication sector 73
9.4 International Practices 73
9.5 Provisional Views 75
9.6 Questions 75

Chapter 10: Allied Laws 76

PART III 78

Grounds of Processing, Obligation on Entities and Individual Rights 78

Chapter 1: Consent 78
1.1 Introduction 78
1.2 Issues 79
(i) Lack of Meaningful and Informed Consent 79
(ii) Standards of consent 80
(iii) Consent Fatigue 80
(iv) Lack of Bargaining Power 81
1.3 International Practices 81
1.4 Provisional Views 83
1.5 Questions 83

Chapter 2: Child's Consent 85
2.1 Introduction 85
2.2 Issues 85
(i) Balancing the issue of children lacking the legal competence to provide valid consent to data processing activities with the fact that children continue to use a large number of online services 86
(ii) Difficulty in determining which websites and entities must comply with the additional data protection requirements to safeguard children 86
(iii) Difficulty in verifying the age of a child 87
2.3 International Practices 87
2.4 Provisional Views 89
2.5 Questions 90

Chapter 3: Notice 92
3.1 Introduction 92
3.2 Issues 92
(i) Notice complexity and difficulty in comprehension 93
(ii) Lack of Meaningful Choice 93
(iii) Notice Fatigue 94
(iv) Problems in Notice Design 94
3.3 International Practices 95
3.4 Provisional Views 97
3.5 Questions 98

Chapter 4: Other Grounds of Processing 99
4.1 Introduction 99
4.2 Issues 99
(i) Requirement to have additional grounds of processing, along with consent. 99
(ii) Lack of clarity with respect to certain grounds of processing, such as ñpublic interestò, ñvital interestò and ñlegitimate interestò 100
4.3 International Practices 100
(i) Performance of Contract 100
(ii) Legal Obligation 101

(iii) Vital Interest 101
(iv) Public interest task, or the exercise of official authority 101
(v) Legitimate Interest 102
4.4 Provisional Views 103
4.5 Questions 104

Chapter 5: Purpose Specification and Use Limitation 105
5.1 Introduction 105
(i) Purpose Specification Principle 105
(ii) The Use Limitation Principle 105
5.2 Issues 106
(i) Relevance of the Purpose Specification Principle in light of technological developments 106
(ii) Compatibility Assessment 106
(iii) Difficulty in specifying purpose in a simple manner 106
5.3 International Practices 107
5.4 Provisional Views 109
5.5 Questions 110

Chapter 6: Processing of Sensitive Personal Data 111
6.1 Introduction 111
6.2 Issues 112
(i) Definition of ñsensitive dataò as per the Sensitive Personal Data Rules 112
(ii) Need to further examine the rationale behind certain categories of personal data 112
(iii) Difficulty in determining the context of use which could make data sensitive 113
6.3 International Practices 113
6.4 Provisional Views 115
6.5 Questions 116

Chapter 7: Storage Limitation and Data Quality 117
7.1 Introduction 117
(i) Storage Limitation 117
(ii) Data Quality 117
7.2 Issues 117
(i) Implementation 117
(ii) Modern technology and processing 118
7.3 International Practices 118
(i) Storage Limitation 118
(ii) Data Quality 119
7.4 Provisional views 120
7.5 Questions 121

Chapter 8: Individual Participation Rights-1 122
8.1 Introduction 122
(i) Origin 122
8.2 Issues 123
(i) Costly implementation 123
(ii) Technical Challenges 124
(iii) Logic behind automated decisions 124
(iv) Limited exercise of rights 125
8.3 International Practices 125
8.4 Provisional Views 127
8.5 Questions 128

Chapter 9: Individual Participation Rights-2 129

9.1 Introduction 129
(i) The right to object to processing 129
(ii) The right to object to processing for the purpose of direct marketing 129
(iii) Right to not to be subject to a decision based solely on automated processing 130
(iv) Right to Restrict Processing 130
(v) Right to Data Portability 131
9.2 Issues 131
(i) Costly implementation 131
(ii) Inchoate nature of rights 132
(iii) Unsuitability for India 132
(iv) Overlap with sector-specific regulations 133
(v) Automated Decision Making 133
9.3 International Practices 133
9.4 Provisional Views 135
9.5 Questions 136

Chapter 10: Individual Participation Rights 3- Right to be forgotten 137
10.1 Introduction 137
10.2 Issues 138
(i) Conflict with freedom of speech 138
(ii) Compliance of Third Parties 139
10.3 International Practices 139
10.4 Provisional Views 141
10.5 Questions 141

PART IV 143

Regulation And Enforcement 143

Chapter 1: Enforcement Models 143
1.1 Introduction 143
1.2 Types of Enforcement Models 144
(i) ócommand and controlô regulation 144
(ii) Self-regulation 144
(iii) Co-regulation 145
1.3 Provisional Views 146
1.4 Questions 146

Chapter 2: Accountability and Enforcement Tools 147
Accountability 147
2.1 Introduction 147
2.2 Issues 149
2.3 International Practices 151
2.4 Provisional Views 155
2.5 Questions 155
Enforcement Tools 157
2.6 Introduction 157

A. Codes Of Practice 157
2.7 Issues 157
2.8 International Practices 158
2.9 Provisional Views 159
2.10 Questions 159

B. Personal Data Breach Notification 161

2.11 Issues and International Practices 161
2.12 Provisional Views 165
2.13 Questions 166

C. Categorisation Of Data Controllers 167
2.14 Issues 167
2.15 Additional Obligations on Data Controllers 167
2.16 Provisional Views 171
(i) Registration 172
(ii) Data protection impact assessment 172
(iii) Data audits 172
(iv) Data protection officer 172
2.17 Questions 172

D. Data Protection Authority 175
2.18 Issues 175
2.19 International Practices 175
2.20 Provisional Views 181
(i) Monitoring, enforcement and investigation 181
(ii) Awareness generation 181
(iii) Standard setting 181
2.21 Questions 182

Chapter 3: Adjudication Process 184
3.1 Introduction 184
3.2 Issues 184
3.3 International Practices 186
3.4 Provisional Views 188
3.5 Questions 189

Chapter 4: Remedies 191

A. Penalties 191
4.1 Issues 191
4.2 International Practices 191
4.3 Provisional Views 193
(i) Per day basis 194
(ii) Discretion of adjudicating body subject to a fixed upper limit 194
(iii) Discretion of adjudicating body subject to an upper limit linked to a variable parameter 194
4.4 Questions 195

B. Compensation 197
4.5 Issues 197
4.6 International Practices 198
4.7 Provisional Views 200
4.8 Questions 200

C. Offences 201
4.9 Issues 201
4.10 International Practices 202
4.11 Provisional Views 203
4.12 Questions 203

PART V 204

Summary 204

PART I
CONTEXT-SETTING

1. A Digital India in a Digital World

The 21st century has witnessed such an explosive rise in the number of ways in which we use information, that it is widely referred to as ótheinformation ageô. It is believed that by 2020, the global volume of digital data we create is expected to reach 44 zettabytes.[1] Much of that new information will consist of personal details relating to individuals, including information relating to the products they have purchased, the places they have travelled to and data which is produced from ñsmart devicesò connected to the Internet.

With the rapid development of technology, computers are able to process vast quantities of information in order to identify correlations and discover patterns in all fields of human activity. Enterprises around the world have realised the value of these databases and the technology for its proper mining and use is evolving every day. Proprietary algorithms are being developed to comb this data for trends, patterns and hidden nuances by businesses.[2] Many of these activities are beneficial to individuals, allowing their problems to be addressed with greater accuracy.[3] For instance, the analysis of very large and complex sets of data is done today through Big Data analytics. Employing such analytics enables organisations and governments to gain remarkable insights into areas such as health, food security, intelligent transport systems, energy efficiency and urban planning.[4] This is nothing short of a digital revolution.

This digital revolution has permeated India as well. Recognising its significance, and that it promises to bring large disruptions in almost all sectors of society, the Government of India has envisaged and implemented the ñDigital Indiaò initiative. This initiative involves the incorporation of digitisation in governance; healthcare and educational services; cashless economy and digital transactions; transparency in bureaucracy; fair and quick distribution of

[1] ó The Digital Universe of Opportunities: Rich Data and the Increasing Values of the Internet of Thingsô, EMC Digital Universe with Research and Analysis by IDC (April 2014), available at:https://www.emc.com/leadership/digital-universe/2014iview/executive-summary.htm, (last accessed 4 November 2017).

[2] ó Big data: Changing the Way Businesses Operate and Competeô, Ernst & Young (April 2014), available at:http://www.ey.com/Publication/vwLUAssets/EY_-_Big_data:_changing_the_way_businesses_operate/%24FILE/EY-Insights-on-GRC-Big-data.pdf, (last accessed November 20, 2017).

[3] Roger Parloff, ó Why Deep Learning is Suddenly Changing your Lifeô, Fortune Magazine (28 September 2016), available at: http://fortune.com/ai-artificial-intelligence-deep-machine-learning/, (last accessed 3 November 2017).

[4] European Commission, ó European Data Protection Reform and Big Data: Factsheetô, (2016), available at: http://ec.europa.eu/justice/data-protection/files/data-protection-big-data_factsheet_web_en.pdf, (last accessed 4 November 2017).

welfare schemes etc to empower citizens.[5] With nearly 450 million Internet users and a growth rate of 7-8%, India is well on the path to becoming a digital economy, which has a large market for global players.[6] This digital economy is expected to generate new market growth opportunities and jobs in the coming 40-50 years.[7]

While the transition to a digital economy is underway, the processing of personal data has already become ubiquitous in both the public and private sector. Data is valuable *per se* and more so, when it is shared, leading to creation of considerable efficiency. The reality of the digital environment today, is that almost every single activity undertaken by an individual involves some sort of data transaction or the other. The Internet has given birth to entirely new markets: those dealing in the collection, organisation, and processing of personal information, whether directly, or as a critical component of their business model.[8] As has been noted by the Supreme Court in *Puttaswamy*[9]:

> ñ*'Uber', the world's largest taxi company, owns no vehicles. 'Facebook', the world's most popular media owner, creates no content. 'Alibaba', the most valuable retailer, has no inventory. And 'Airbnb', the world's largest accommodation provider, owns no real estate.*ò[10]

Something as simple as hailing a taxi now involves the use of a mobile application which collects and uses various types of data, such as the userôs financial information, her real-time location, and information concerning her previous trips. Data is fundamentally transforming the way individuals do business, how they communicate, and how they make their decisions. Businesses are now building vast databases of consumer preferences and behaviour. Information can be compressed, sorted, manipulated, discovered and interpreted as never before, and can thus be more easily transformed into useful knowledge.[11] The low costs of storing and processing information and the ease of data collection has resulted in the prevalence of long-term storage of information as well as collection of increasingly minute details about an individual which allows an extensive user profile to be created.[12] Such

---

[5] Press Information Bureau, ôDigital India ï A programme to transform India into digital empowered society and knowledge economyô (20 August 2014), available at http://pib.nic.in/newsite/PrintRelease.aspx?relid=108926 (last accessed 16 November 2017).

[6] Arushi Chopra, ôNumber of Internet users in India could cross 450 million by June: reportô, LiveMint (2 March 2017), available at: http://www.livemint.com/Industry/QWzIOYEsfQJknXhC3HiuVI/Number-of-Internet-users-in-India-could-cross-450-million-by.html, (last accessed 5 November 2017).

[7] Ranjan Guha, ôDigital Evolution in Indiaô, Business Today (29 August 2017), available at: http://www.businesstoday.in/opinion/columns/digital-evolution-in-india/story/259227.html, (last accessed 4 November 2017).

[8] Ryan Moshell, ôAnd then there was one: The outlook for a self-regulatory United States amidst a global trend towards comprehensive data protection frameworkô, 37 Texas Tech Law Review 357 (2005).

[9] *Justice K.S. Puttaswamy (Retd.) v. Union of India & Ors.* 2017 (10) SCALE 1.

[10] Tom Goodwin, ôThe Battle is for Customer Interfaceô, TechCrunch (3 March 2015), available at: https://techcrunch.com/2015/03/03/in-the-age-of-disintermediation-the-battle-is-all-for-the-customer-interface/ (last accessed 14 November 2017) cited in *Justice K.S. Puttaswamy (Retd.) v. Union of India & Ors.* 2017 (10) SCALE 1, Per S.K. Kaul, J. at paragraph 17.

[11] Helen Nissenbaum, ôPrivacy in Context-Technology, Policy, and the Integrity of Social Lifeô, 36, (Stanford University Press, 2010).

[12] Joel Reidenberg, ôResolving Conflicting International Data Privacy Rules in Cyberspaceô, 52 Stanford Law Review 1315 (1999).

information can then be used to create customised user profiles, based on their past online behaviour, which has the benefit of reducing the time required to complete a transaction. For instance, e-commerce websites track previous purchases, use algorithms to predict what sorts of items a user is likely to buy, thereby reducing the time spent on each purchase.[13]

There are a large number of benefits to be gained by collecting and analysing personal data from individuals. Pooled datasets allow quicker detection of trends and accurate targeting. For instance, in the healthcare sector, by collecting and analysing large data sets of individualôs health records and previous hospital visits, health care providers could make diagnostic predictions and treatment suggestions;[14] an individualôs personal locational data could be used for monitoring traffic and improving driving conditions on the road;[15] banks can use Big Data techniques to improve fraud detection;[16] insurers can make the process of applying for insurance easier by using valuable knowledge gleaned from pooled datasets.[17]

At the same time, the state processes personal data for a plethora of purposes, and is arguably its largest processor. In India, the state uses personal data for purposes such as the targeted delivery of social welfare benefits, effective planning and implementation of government schemes, counter-terrorism operations, etc. Such collection and use of data is usually backed by law, though in the context of counter-terrorism and intelligence gathering, it appears not to be the case.[18]

Thus both the public and the private sector are collecting and using personal data at an unprecedented scale and for multifarious purposes. While data can be put to beneficial use, the unregulated and arbitrary use of data, especially personal data, has raised concerns regarding the privacy and autonomy of an individual. Some of the concerns relate to

---

[13] For an illustrative example, see Greg Linden *et al.*, ôAmazon.com Recommendations: Item to Item Collaborative Filteringô, University of Maryland: Department of Computer Science, available at: https://www.cs.umd.edu/~samir/498/Amazon-Recommendations.pdf (last accessed 5 November 2017).

[14] Clemens Suter-Crazzolara, ôBig Data And The Journey To Personalized Medicineô, Forbes (17 November 2015), available at: https://www.forbes.com/sites/sap/2015/11/17/big-data-and-the-journey-to-personalized-medicine/#7865d751b0ee, (last accessed 20 November 2017).

[15] Matthew Sparks, ôGPS Big Data: making cities safer for cyclistsô, The Telegraph (9 May 2014), available at: http://www.telegraph.co.uk/technology/news/10818956/GPS-big-data-making-cities-safer-for-cyclists.html, (last accessed 5 November 2017).

[16] Jacomo Corbo *et al.*, ôApplying analytics in financial institutionsô fight against fraud', McKinsey and Company (April 2017), available at:https://www.mckinsey.com/business-functions/mckinsey-analytics/our-insights/applying-analytics-in-financial-institutions-fight-against-fraud, (last accessed 5 November 2017).

[17] Information Commissionerôs Office (UK), ôBig Data, Artificial Intelligence, Machine Learning and Data Protectionô, available at: https://ico.org.uk/for-organisations/guide-to-data-protection/big-data/ (last accessed 31 October 2017).

[18] Press Information Bureau, ôHome minister proposes radical restructuring of security architectureô, Ministry of Home Affairs, Government of India (23 December 2009), available at http://pib.nic.in/newsite/erelease.aspx?relid=56395 (last accessed 5 November 2017); Press Information Bureau, ôCentralised System to Monitor Communicationsô, Ministry of Communications, Government of India (26 November 2009), available at http://pib.nic.in/newsite/PrintRelease.aspx?relid=54679 (last accessed 16 November 2017); Udbhav Tiwari, ôThe Design and Technology behind Indiaôs Surveillance Programmeô, Centre for Internet & Society, India (20 January 2017), available at https://cis-india.org/internet-governance/blog/the-design-technology-behind-india2019s-surveillance-programmes (last accessed 16 November 2017).

centralisation of databases, profiling of individuals, increased surveillance and a consequent erosion of individual autonomy. This was also the subject matter of the landmark judgement of the Supreme Court in *Puttaswamy,* which recognised the right to privacy as a fundamental right.[19] The Supreme Court stated that the ñright to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 of the Constitution and as a part of the freedoms guaranteed by Part III of the Constitutionò.[20] Further, it went on to recognise informational privacy as a facet of the right to privacy and directed the Union Government to put in place a robust data protection regime to ensure protection against the dangers posed to an individualôs privacy by state and non-state actors in the information age.[21]

In this light, in order to harness the benefits of the digital economy and mitigate the harms consequent to it, formulating a data protection law is the need of the hour for India.

2. Data Protection: Genesis and Rationale

(i) Data Protection and the Value of Privacy

Data protection principles are designed to protect the personal information of individuals by restricting how such information can be collected, used and disclosed.[22] As a legal right, it has developed in many jurisdictions because of the emergence of a wide range of issues related to personal information being processed through ñautomatedò means.[23] In order to understand these issues, it is important to examine how the usage of personal information is an important activity in society as it not only reaps many benefits but is also capable of causing considerable harm. The need for data protection thus arises out of the need to prevent such harms, and hinges on the question of who should be permitted to use personal information and how.

It is crucial to understand this concept in relation with privacy, as privacy can have different meanings based on the context. Three broad types of privacy have been identified: the privacy pertaining to physical spaces, bodies and things (spatial privacy); the privacy of certain significant self-defining choices (decisional privacy); and the privacy of personal information (informational privacy).[24] The concept of data protection is primarily linked with the idea of informational privacy,[25] though given the deeply pervasive nature of technology, its impact on decisional privacy and spatial privacy is also discernible. Though privacy is popularly associated with seclusion or secrecy, as a legal right, it is understood as a question of control over personal information.

---

[19] 2017 (10) SCALE 1.
[20] 2017 (10) SCALE 1.
[21] 2017 (10) SCALE 1.
[22] Lee Bygrave, ódData Protection Law: Approaching Its Rationale, Logic, and Limitsô 2 (Kluwer Law International: The Hague/London/New York, 2002).
[23] *See* definition of óprocessingô under Article 4 (2) of the EU General Data Protection Regulation, 2016 (Regulation (EU) 2016/679).
[24] Jerry Kang, ódInformation Privacy in Cyberspace Transactionsô, 50 Stanford Law Review 1193, 1202-03 (April 1998).
[25] Maria Tzanou, ódData protection as a fundamental right next to privacy? óReconstructingô a not so new right,ô3 (2) International Data Privacy Law 88 (1 May 2013).

Privacy is a complex concept that has been difficult to define. In many circumstances, the harms that arise from violations of privacy are difficult to identify because very often they are intangible. Despite its amorphous nature, there are a number of reasons why protecting privacy is considered valuable. The protection of privacy permits individuals to plan and carry out their lives without unnecessary intrusion.[26] Informational privacy is often understood as the freedom of individuals ñto determine for themselves when, how, and to what extent information about them is communicated to othersò[27] and this freedom allows for individuals to protect themselves from harm. However, not all information about an individual is necessarily private and deserving of protection. It is for a legal framework to determine where affording such freedom is appropriate and where it is not.

Certain aspects related to an individual are considered especially central to their identity, such as their bodies, their sexuality, or their ability to develop their own distinct personalities.[28] Privacy is also valued where it legitimately protects an individualôs reputation. Disclosure of certain kinds of inflammatory and sensitive information, even where the information is true, unfairly results in the stereotyping and pre-judging of individual.[29] In some circumstances, information about an individual (such as their race, religion, caste etc.) can be used to discriminate against them. There are also some actions of the state which may threaten an individualôs privacy. For instance, surveillance activities by government or private organisations can disrupt peace of mind and create chilling effects by making people conform to societal expectations.[30]

However, it is not possible to conclusively demarcate all the aspects requiring protection in this manner as the relevant concerns arise in varying contexts. Privacy does not arise only in some special, unchanging space like the home or the family but also in various situations including in public spaces. Different norms of privacy can exist in different spheres of life.[31] For example, an individual may be willing to disclose certain things to a doctor or psychologist that she would not even tell her spouse or friends. Rules of data protection and privacy are designed in such a way that they allow individuals the freedom to determine how their personal information will be collected, used and disclosed. This is because individuals themselves are best equipped to understand how they will be benefited or harmed in the many unique contexts which involve their personal information.

Privacy laws are not identical in form to any other existing fields of law like property, copyright or tort law, though there are some similarities.[32] For example, laws on defamation

---

[26] *Time, Inc. v. Hill*, 385 U.S. 374, 413 (1967) (Fortas, J., dissenting); *Doe v. Bolton*, 410 U.S. 179, 213 (1973) (Douglas, J., concurring)

[27] Alan Westin, ôPrivacy and Freedomô, 7, (Atheneum, 1967).

[28] Stanley I. Benn, ôPrivacy, Freedom, and Respect for Persons,ô in ôNomos XIII: Privacyô, 26 (J. Ronald Pennock and J.W. Chapman *eds*., 1971).

[29] Jeffrey Rosen, ôThe Unwanted Gaze: The Destruction of Privacy in Americaô(Random House, 2000).

[30] Neil M. Richards, ôThe Dangers of Surveillance,ô 126 (7) Harvard Law Review 1934, 1950 (20 May 2013).

[31] Helen Nissenbaum, ôPrivacy as Contextual Integrityô, 79 Washington Law Review 119 (2004).

[32] Daniel Solove, ôConceptualizing Privacyô, 90 (4) California Law Review 1088-89, 1100-02, 1112-13, 1130-31, (July 2002).

generally prohibit disclosure of personal information only if it is false. Privacy, on the other hand, would even protect against disclosure of truthful personal information.[33] The source and application of privacy has not been confined to constitutional law, criminal procedure or evidentiary rules. Defining appropriate rules as to how personal information should be distributed thus requires *sui generis* concepts and tools. One important aspect that arises in the unique framework of privacy is the method by which we identify harms. These can be subjective or objective.[34] A subjective harm is one where an individual has not actually suffered any tangible loss but anticipates such loss after personal information is collected. The uncertainty, anxiety and fear of potential observation are the identified harms in this situation. On the other hand, objective harms are separately identified when the use of oneôs personal information actually results in some damage, whether through loss of reputation or through some other change in the treatment of the individual by society. Data protection must account for both these kinds of harms which arise as a result of unregulated collection and use of personal information.

(ii) The Evolution of Privacy Principles

The 1970s witnessed increasing use of automated data systems containing personal information about individuals.[35] To address concerns surrounding this, the Government of the United States appointed an Advisory Committee in the Department of Health, Education and Welfare (HEW Committee) to examine the various legal and technological issues raised vis-a-vis increasingly automated processing of data. The HEW Committee went on to issue a landmark report titled ó*Records, Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems',* which recommended that the United States Congress develop a Code of Fair Information Practices based on Fair Information Practices Principles (FIPPS).[36] The FIPPS are a set of principles which prescribe how data should be handled, stored and managed to maintain fairness, privacy and security in a rapidly growing global technology environment.[37] FIPPS are now deemed to be the bedrock of modern data protection laws across the world.[38]

---

[33] Samuel Warren and Louis Brandeis, ôThe Right to Privacy,ô 4(5) Harvard Law Review 193 (15 December 1890).
[34] Ryan M. Calo, ôThe Boundaries of Privacy Harmô, 86 Indiana Law Journal 1131, 1142-43 (2011).
[35] Robert Gellman, ôFair Information Practices: A Brief Historyô (April 10, 2017), available at: https://bobgellman.com/rg-docs/rg-FIPshistory.pdf (last accessed 31 October 2017).
[36] Fred H. Cate, ôFailure of Fair Information Principlesô, in óConsumer Protection in the Age of Information Economyô, (Jane K. Winn *ed.*, Routledge, 2006).
[37] Pam Dixon, óA brief introduction to fair information practice principlesô, World Privacy Forum (2006), available at: https://www.worldprivacyforum.org/2008/01/report-a-brief-introduction-to-fair-information-practices/ (last accessed 31 October 2017).
[38] The FIPPS are as follows:

1. There must be no personal-data record-keeping systems whose very existence is secret.
2. There must be a way for an individual, to find out what information about him is in a record and how it is used.
3. There must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent.
4. There must be a way for an individual to correct or amend a record of identifiable information about him.

The FIPPS were soon followed by the Organisation for Economic Cooperation and Development Privacy Guidelines (OECD Guidelines) in the 1980s.[39] The OECD Guidelines were significantly inspired by the FIPPS and were intended to provide a framework for harmonising national privacy legislations amongst OECD members, while upholding human rights, and preventing interruptions in international flows of data.[40] The OECD Guidelines are deemed to be the first internationally agreed upon statement of core information privacy principles and have considerably influenced data protection frameworks around the world.[41]

The OECD Guidelines have inspired multiple data protection frameworks such as the European Directive 95/46/EC on the processing of personal data and the free movement of such data (Data Protection Directive), the 2004 Asia-Pacific Economic Cooperation Framework (APEC Framework) as well as data protection legislations such as the Australiaôs Privacy Act, 1988 (Privacy Act), New Zealandôs Privacy Act, 1993 and Japanôs Protection of Personal Information Act, 2003.[42] However, despite the popularity that traditional privacy principles have enjoyed, they have come under considerable scrutiny in recent times.[43]

It has been argued that traditional privacy principles may not be well-suited to address the challenges posed by the dramatic increase in the volume and use of personal data, advances in computing, and global flows of data. As a consequence of these concerns, an expert group was constituted to revise and modernise the OECD Guidelines. The OECD Guidelines as updated in 2013 (2013 OECD Guidelines) are the product of this attempt. While the 2013 OECD Guidelines keep the core privacy principles such as collection limitation, data quality and purpose specification etc. intact, several new elements to strengthen data safeguards have been introduced. These include: privacy management programs to enhance accountability of the data controller,[44] data security breach notification[45] which oblige data controllers to

---

5. Any organisation creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data.

[39] OECD, ôOECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Dataô (2013), available at: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (last accessed 31 October 2017).

[40] OECD, ôOECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Dataô (2013), available at: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (last accessed 31 October 2017).

[41] OECD, ôThirty Years After: The OECD Privacy Guidelinesô (2011), available at: http://www.oecd.org/sti/ieconomy/49710223.pdf (last accessed 31 October 2017).

[42] OECD, ôOECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Dataô (2013), available at: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (last accessed 31 October 2017).

[43] Fred H. Cate, ôFailure of Fair Information Principlesô, in ôConsumer Protection in the Age of Information Economyô (Jane K. Winn *ed.*, Routledge, 2006).

[44] Privacy management programmes are intended be integrated in the governance structure of a data controller and establish appropriate internal oversight mechanisms to ensure data is safeguarded (Organisation for Economic Co-operation and Development, ôThirty Years After: The OECD Privacy Guidelinesô (2011), available at: http://www.oecd.org/sti/ieconomy/49710223.pdf (last accessed 31 October 2017).

inform individuals/authorities of a security breach and establishment and maintenance of privacy enforcement authorities.[46] Further cross-border flows of data[47] and international cooperation to improve global interoperability of privacy frameworks have been recognised as essential for a global data economy.[48]

The 2013 OECD Guidelines have been criticised as being fundamentally incompatible with modern technologies and Big Data analytics which have revolutionised how data is collected and processed.[49] Presently, corporations possess data that has been generated or collected from a wide variety of sources. Such data may include financial data, employee data and customer data. It may be relevant to note that at the time when these guidelines originated, data processing, including collection activities were more linear and easier to define. However, now the situation has changed with data being collected and used in ways not envisaged at the time these principles were developed. We have, as a consequence, been ushered into the era of modern technologies and Big Data analytics. While Big Data does not have a precise definition, it can be understood as essentially involving gathering large quantities of data and applying innovative technology (such as predictive analysis) to them to extract knowledge.[50] Big Data is usually characterised by 3 Vs, namely ówolumeô as in massive datasets, ówelocityô which relates to real time data, and ówarietyô which relates to different sources of data.[51] Other technological developments such as artificial intelligence,[52] machine learning[53], the Internet of Things[54] are all part of the Big Data ecosystem and their use is becoming increasingly commonplace.

---

[45] OECD, ôThirty Years After: The OECD Privacy Guidelinesô (2011), available at: http://www.oecd.org/sti/ieconomy/49710223.pdf (last accessed 31 October 2017).

[46] OECD, ôThirty Years After: The OECD Privacy Guidelinesô (2011), available at: http://www.oecd.org/sti/ieconomy/49710223.pdf (last accessed 31 October 2017).

[47] OECD, ôThirty Years After: The OECD Privacy Guidelinesô (2011), available at: http://www.oecd.org/sti/ieconomy/49710223.pdf (last accessed 31 October 2017).

[48] OECD, ôThirty Years After: The OECD Privacy Guidelinesô (2011), available at: http://www.oecd.org/sti/ieconomy/49710223.pdf (last accessed 31 October 2017).

[49] Jordi Soria-Comas and Josep Domingo-Ferrer, ôBig Data Privacy: Challenges to Privacy Principles and Modelsô, 1(1) Data Science and Engineering (March 2016), available at: https://link.springer.com/article/10.1007/s41019-015-0001-x (last accessed 31 October 2017).

[50] Kate Crawford and Jason Schultz, ôBig Data And Due Process: Towards A Framework To Redress Predictive Privacy Harmsô, 55(1) Boston College Law Review 93 (2014).

[51] Information Commissionerôs Office (UK), ôBig Data, Artificial Intelligence, Machine Learning and Data Protectionô, available at: https://ico.org.uk/for-organisations/guide-to-data-protection/big-data/ (last accessed 31 October 2017).

[52] Artificial Intelligence pertains to ógiving computers behaviours which would be thought intelligence in human beingsô. *See* The Society for the Study of Artificial Intelligence and Simulation of Behaviour, 'What is Artificial Intelligence', available at: http://www.aisb.org.uk/public-engagement/what-is-ai, (last accessed 3 November 2017); *See generally* Information Commissionerôs Office (UK), ôBig Data, Artificial Intelligence, Machine Learning and Data Protectionô, available at: https://ico.org.uk/for-organisations/guide-to-data-protection/big-data/ (last accessed 31 October 2017).

[53] Machine Learning is defined as: óthe set of techniques that allow computers to think by creating mathematical algorithms based on accumulated dataô. *See* Deb Miller Landau, óArtificial Intelligence and Machine Learning: How Computers Learnô, IQ Intel (17 August 2016), available at: https://iq.intel.com/artificial-intelligence-and-machine-learning/,(last accessed 3 November 2017).

[54] óThe concept of the Internet of Things or IoT refers to an infrastructure in which billions of sensors embedded in common, everyday devices ï óthingsô as such, or things linked to other objects or individuals ï are designed to record, process, store and transfer data and, as they are associated with unique identifiers, interact with other devices or systems using networking capabilities.ô *See* Article 29 Data Protection Working Party Opinion, óOpinion 8/2014 on the on Recent Developments on the Internet of Thingsô, European Commission (16

In light of these developments, the biggest challenge in regulating emerging technologies such as Big Data, artificial intelligence and the Internet of Things, lies in the fact that they may operate outside the framework of traditional privacy principles. These principles, as they were originally envisaged, were designed to protect a single static data set.[55] Thus, it was possible to limit the collection of data to satisfy a particular purpose. However, this limited activity may no longer hold true with respect to current data processing activities. For instance, given that Big Data involves the processing of large data sets, usually the source of such data may not be directly from the individual, and consent may not be as relevant. Further, data may be generated as a by-product of a transaction or obtained by a service provider in return for a free service (such as free email accounts, social networks etc.) or obtained as a consequence of accessing a service (such as use of GPS navigation), and it may not be possible to specify the purpose for which personal data is collected at the time of collection.[56]

The advent of such technologies has also expanded the very definition of personal data. For instance, analysing meta-data such as a set of predictive or aggregated findings, or by combining previously discrete sets of data, Big Data has radically expanded the range of personally identifiable data.[57] Data which is viewed as non-personal information can now be combined with other data sets to create personally identifiable information. An example of this is how anonymised Netflix data on ranking of films could be easily combined with other data sets such as timestamps with public information from the Internet Movie Database (IMDb) to de-anonymise the original data set and reveal personal movie choices.[58] Similarly, Big Data relies on accumulation of large volumes of data to extract knowledge from them, making it difficult to apply the principle of data minimisation.[59] Additionally, technologies such as the Internet of Things relies on continuous collection of personal information from the users of ñsmart devicesò, which may then be interpreted to provide unique services.[60] Therefore, in such instances as well, it may be difficult to adhere to the traditional privacy principles of consent, collection and use limitation. Given the dynamic pace of development

---

September 2014), available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf, (last accessed 3 November 2017).

[55] Jordi Soria-Comas and Josep Domingo-Ferrer, óBig Data Privacy: Challenges to Privacy Principles and Modelsô, 1(1) Data Science and Engineering (March 2016), available at: https://link.springer.com/article/10.1007/s41019-015-0001-x (last accessed 31 October 2017).

[56] Kate Crawford and Jason Schultz, óBig Data And Due Process: Towards A Framework To Redress Predictive Privacy Harmsô, 55(1) Boston College Law Review 93 (2014).

[57] Kate Crawford and Jason Schultz, óBig Data And Due Process: Towards A Framework To Redress Predictive Privacy Harmsô, 55(1) Boston College Law Review 93 (2014).

[58] Bruce Schneier, óWhy ñanonymousô data sometimes isnôtô, Wired (12 December 2017), available at: https://www.wired.com/2007/12/why-anonymous-data-sometimes-isnt/ (last accessed 1 November 2017).

[59] Jordi Soria-Comas and Josep Domingo-Ferrer, óBig Data Privacy: Challenges to Privacy Principles and Modelsô, 1(1) Data Science and Engineering (March 2016), available at: https://link.springer.com/article/10.1007/s41019-015-0001-x (last accessed 31 October 2017).

[60] Article 29 Data Protection Working Party Opinion, óOpinion 8/2014 on the on Recent Developments on the Internet of Thingsô, European Commission (16 September 2014), available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf, (last accessed 3 November 2017).

of emerging technologies, alternatives to traditional privacy principles have thus been suggested that require careful scrutiny.[61]

Since technologies such as Big Data, the Internet of Things and Artificial Intelligence are here to stay and hold out the promise of welfare and innovation, India will have to develop a data protection law which can successfully address the issues relating to these technologies, so as to ensure a balance between innovation and privacy. Whether this involves a reiteration of traditional privacy principles, an alternative approach based on newer *ex ante* forms of regulation or a hybrid model, will have to be determined carefully.

3. Comparative Approaches to Data Protection

In determining, Indiaôs approach to data protection, it will be instructive to look at practices followed in other jurisdictions, particularly recent models that have emerged. A perusal of foreign jurisdictions demonstrates that there are two distinct models in the field of data protection. The European Union or EU model and others similar to it, provide for a comprehensive data protection law couched in the rights based approach; and the American marketplace model has sector specific data protection laws. This is because of the distinct conceptual basis for privacy in each jurisdiction.[62] The two approaches towards data protection are discussed briefly below:[63]

European Union

In EU, the right to privacy is a fundamental right which seeks to protect an individualôs dignity.[64] The European Charter of Fundamental Rights (EU Charter) recognises the right to privacy as well as the right to protection of personal data, in Article 7[65] and Article 8,[66] respectively. The first principal EU legal instrument on data protection was the Data Protection Directive.[67] The Data Protection Directive has been significantly inspired by the

---

[61] Jordi Soria-Comas and Josep Domingo-Ferrer, ôBig Data Privacy: Challenges to Privacy Principles and Modelsô, 1(1) Data Science and Engineering (March 2016), available at: https://link.springer.com/article/10.1007/s41019-015-0001-x (last accessed 31 October 2017).

[62] Avner Levin and Mary Jo Nicholson, ôPrivacy Law in the United States, the EU and Canada: The Allure of the Middle Groundô, 2(2) University of Ottawa Law & Technology Journal, 357 (2005).

[63] In this part, the regulatory approach towards data protection will be discussed ï specific practices will be discussed in detail under the section *International Practices* in the White Paper.

[64] Avner Levin and Mary Jo Nicholson, ôPrivacy Law in the United States, the EU and Canada: The Allure of the Middle Groundô, 2(2) University of Ottawa Law & Technology Journal, 357 (2005).

[65] Respect for private and family life - Everyone has the right to respect for his or her private and family life, home and communications

[66] Protection of personal data -

1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.

[67] The European Union Agency for Fundamental Rights (FRA), the Council of Europe and the Registry of the European Court of Human Rights, ôHandbook on European Data Protection Lawô (2014), available at: http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf, (last accessed 4 November 2017).

OECD Guidelines,[68] and sought to achieve a uniformly high level of data protection in the EU by harmonising data protection legislations in order to ensure that free flow of data was not impeded.[69] The Data Protection Directive was eventually adopted as national legislations by EU Member States. Given that it was a non-binding instrument, it left some room for interpretation.[70] The rapidly changing data landscape led the EU to update its regulatory environment on data protection.[71] The product of this process is the EU General Data Protection Regulation of 2016 (EU GDPR). The EU GDPR is considered to be one of the most stringent data protection laws in the world[72] and being a regulation, it will become immediately enforceable as law in all Member States. However, given the ambitious changes it envisages, Member States have been given two years (till 25 May 2018) to align their laws to the EU GDPR.

The EU GDPR is a comprehensive data protection framework which applies to processing of personal data by any means, and to processing activities carried out by both the Government as well as the private entities, although there are certain exemptions such as national security, defence, public security, etc.[73] Similarly, it continues to recognise and enforce the core data protection principles recognised in the OECD Guidelines.[74] The EU GDPR follows a rights based approach towards data protection, and places the individual at the centre of the law. As a consequence, it imposes extensive control over the processing of personal data both at the time of, and after the data has been collected.[75] Further, collection of certain forms of personal data, known as sensitive personal data (such as racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning health and sex life) is prohibited subject to certain exceptions.[76] Thus, for processing to be lawful and fair, the entity collecting personal data must comply with an extensive range of principles such as that of purpose specification,[77] data minimisation,[78] data quality,[79] security safeguards,[80] etc.

---

[68] OECD, ‘OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data’ (2013), available at: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (last accessed 31 October 2017).

[69] 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).

[70] The EU GDPR, ‘How did we get here?’, available at http://www.eugdpr.org/how-did-we-get-here-.html (last accessed 4 November 2017.)

[71] The EU GDPR, ‘How did we get here?’, available at http://www.eugdpr.org/how-did-we-get-here-.html (last accessed 4 November 2017).

[72] DLA Piper, ‘EU General Data Protection Regulation’ available at https://www.dlapiper.com/en/asiapacific/focus/eu-data-protection-regulation/home (last accessed 5 November 2017).

[73] Article 23, EU GDPR.

[74] OECD, ‘OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data’ (2013), available at: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (last accessed 31 October 2017).

[75] Avner Levin and Mary Jo Nicholson, ‘Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground’, 2(2) University of Ottawa Law & Technology Journal, 357 (2005).

[76] Article 9, EU GDPR

[77] Article 5(1)(b), EU GDPR.

[78] Article 5(1)(c), EU GDPR.

Further, an individual continues to exercise extensive control over her data post collection. This is enabled by a gamut of individual participation rights guaranteed under the law. These includes: the right to confirm if data about oneself is being collected[81], the right to access data[82], the right to rectification of data[83], the right to data portability[84], the right to restrict processing[85], the right to erasure[86], the right to object to processing[87], the right to object to processing for the purpose of direct marketing[88], the right to object to automated decisions[89].

The EU model also envisages an independent supervising authority (a regulator) who is armed with an array of functions and powers.[90] Primarily, this body is responsible for monitoring and enforcing compliance with the law and for ensuring the protection of the fundamental rights in relation to processing and facilitating the free flow of data.[91] Significant powers of imposing penalties are vested in the regulator to ensure effective compliance.

The EU model appears to be the preferred mode in several countries who have adopted data protection legislations recently.[92] A variation of this law, which may be described as a co-regulatory model, was earlier adopted in Australia in the form of the Privacy Act and in Canada in the form of the Personal Information Protection and Electronic Documents Act, 2000 (PIPEDA). In both Australia and Canada, co-regulatory hybrid models involve the cooperation of industry and government.[93]

United States

On the contrary, in the US, privacy protection is essentially a ñliberty protectionò i.e. protection of the personal space from government.[94] Thus, the American understanding of the ñright to be let aloneò has come to represent a desire for as little government intrusion as possible. [95] While there is no provision in the US Constitution that explicitly grants a right to privacy, the right in a limited form is reflected in the Fourth Amendment to the US

[79] Article 5(1)(d), EU GDPR.
[80] Article 5(1)(f), EU GDPR.
[81] Article 15(1), EU GDPR.
[82] Article 15, EU GDPR.
[83] Article 16, EU GDPR.
[84] Article 20, EU GDPR
[85] Article 19, EU GDPR.
[86] Article 18, EU GDPR.
[87] Article 21, EU GDPR.
[88] Article 21(2), EU GDPR.
[89] Article 22, EU GDPR.
[90] Articles 4(21) and 51, EU GDPR.
[91] Section 51, EU GDPR.
[92] *See* for example, South African Law Reform Commission, óPrivacy and Data Protectionô Discussion Paper 109, Project 124 (October 2005), available at: http://www.justice.gov.za/salrc/dpapers/dp109.pdf; (last accessed 2 November 2017).
[93] Ryan Moshell, óAnd then there was one: The outlook for a self-regulatory United States amidst a global trend towards comprehensive data protection frameworkô, 37 Texas Tech Law Review 357 (2005).
[94] Avner Levin and Mary Jo Nicholson, óPrivacy Law in the United States, the EU and Canada: The Allure of the Middle Groundô, 2(2) University of Ottawa Law & Technology Journal, 357 (2005).
[95] Avner Levin and Mary Jo Nicholson, óPrivacy Law in the United States, the EU and Canada: The Allure of the Middle Groundô, 2(2) University of Ottawa Law & Technology Journal, 357 (2005).

Constitution ï the right against unreasonable searches and seizures. US courts however, have collectively recognised a right to privacy by piecing together the limited privacy protections reflected in the First, Fourth, Fifth and Fourteenth Amendments to the US Constitution.[96]

In addition to the distinction in the conceptual basis of privacy, the US approach towards privacy and data protection varies from the EU in multiple respects. First, unlike the EU, there is no comprehensive set of privacy rights/principles that collectively address the use, collection and disclosure of data in the US. [97] Instead, there is limited sector specific regulation.[98]

Second, the approach towards data protection varies for the public and private sector. The activities and powers of the Government *vis-à-vis* personal information are well defined and addressed by broad, sweeping legislations[99] such as the Privacy Act, 1974 which is based on the FIPPS (governing collection of data by the federal government); the Electronic Communications Privacy Act, 1986; the Right to Financial Privacy Act, 1978, etc. For the private sector, which is not governed by these legislations, certain sector-specific norms exist. These include: The Federal Trade Commission Act (FTC Act), The Financial Services Modernization Act (Gramm-Leach-Bliley Act or the GLB Act), The Health Insurance Portability and Accountability Act (HIPAA), and the Children's Online Privacy Protection Act (COPPA) etc. In addition, States have their own data protection laws.

As far as private sector regulation is concerned, the core of data protection practice in the US is notice and consent. The Federal Trade Commission (FTC), is a bipartisan federal agency with the dual mission to protect consumers and promote competition[100] which has the responsibility to ensure consumer privacy enforcement. It does this by bringing enforcement actions against companies which violate consumer privacy, including activities like failing to comply with posted privacy principles and unauthorised disclosure of personal data. The FTC has described notice to be ñmost fundamental principleò,[101] and has focused all of its privacy related efforts on getting websites to post privacy policies and its enforcement efforts in holding websites accountable when they fail to adhere to them.[102]

Further, US statutes and regulations have also tended to focus on ñnotice and consentò. For instance, Title V of the GLB Act has only three substantive restrictions on processing of

[96] *Roe v. Wade* 410 U.S. 113 (1973) and *Griswold v. Connecticut* 381 U.S. 479 (1965). See Ryan Moshell, óAnd then there was one: The outlook for a self-regulatory United States amidst a global trend towards comprehensive data protection frameworkô, 37 Texas Tech Law Review (2005).
[97] Joel R Reidenberg, óData Protection in the Private Sector in the United Statesô 3 International Yearbook of Law Computers and Technology (1993).
[98] Ryan Moshell, óAnd then there was one: The outlook for a self-regulatory United States amidst a global trend towards comprehensive data protection frameworkô, 37 Texas Tech Law Review 357 (2005).
[99] Ryan Moshell, óAnd then there was one: The outlook for a self-regulatory United States amidst a global trend towards comprehensive data protection frameworkô, 37 Texas Tech Law Review (2005).
[100] FTC, ówhat we doô, available at https://www.ftc.gov/about-ftc/what-we-do (last accessed 4 November 2017)
[101] Martha K. Landesberg *et al.,* óPrivacy Online: A Report to Congressô, FTC (June, 1998) available at: https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf (last accessed 4 November 2017).
[102] Fred H. Cate, óFailure of Fair Information Principlesô, in óConsumer Protection in the Age of Information Economyô, (Jane K. Winn *ed.*, Routledge, 2006).

personal information and instead emphasises on procedural requirements, specifically, the need for institutions to ñclearly and conspicuouslyò provide consumers with notice pertaining to its disclosure practices and an opportunity to opt out of such disclosure.[103] Another example is the rules pertaining to privacy of personal health information under the HIPAA. The HIPAA essentially envisages three types of notice and consent requirements.[104] Such emphasis on notice and consent is the *status quo* of data protection laws in the US.

The US approach to data protection thus has two discernible trendsð stringent norms for government processing of personal information; and notice and choice based models for private sector data processing. This dichotomy can largely be said to be a consequence of the *laissez faire* culture of the US markets,[105] as opposed to the rights-centric culture of the EU.

4. Data Protection in India

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

(i) Judicial Developments on Right to Privacy

The Supreme Court in *Puttaswamy* overruled its previous judgments of *M.P. Sharma v. Satish Chandra* (*M.P. Sharma*)[106] and *Kharak Singh v. State of Uttar Pradesh* (*Kharak Singh*)[107] which appeared to observe that there was no fundamental right to privacy enshrined in the Constitution of India. By doing so, it upheld several precedents following *Kharak Singh,* which had recognised a right to privacy flowing from Article 21 of the Constitution of India.[108]

The Supreme Court in *M.P. Sharma* examined whether the constitutionality of search and seizure of documents pursuant to a FIR would violate the right to privacy. A majority decision by an eight-judge Constitution bench observed that the right to privacy was not a fundamental right under the Constitution.

Subsequently, in *Kharak Singh,* the issue at hand was whether regular surveillance by police authorities amounted to an infringement of constitutionally guaranteed fundamental rights. A Constitution bench of six judges analysed this issue in the backdrop of the validity of the regulations governing the Uttar Pradesh police which legalised secret picketing, domiciliary

---

[103] Fred H. Cate, ófFailure of Fair Information Principlesô, in ófConsumer Protection in the Age of Information Economyô, (Jane K. Winn *ed.*, Routledge, 2006).
[104] Fred H. Cate, ófFailure of Fair Information Principlesô, in ófConsumer Protection in the Age of Information Economyô, (Jane K. Winn *ed.*, Routledge, 2006).
[105] Ryan Moshell, ófAnd then there was one: The outlook for a self-regulatory United States amidst a global trend towards comprehensive data protection frameworkô, 37 Texas Tech Law Review 357 (2005).
[106] *M.P. Sharma v. Satish Chandra*, (1954) SCR 1077.
[107] *Kharak Singh v. State of Uttar Pradesh*, (1964) 1 SCR 332.
[108] For illustrative examples see, *Gobind v. State of Madhya Pradesh*, (1975) 2 SCC 148; *R. Rajagopal v. State of Tamil Nadu*, (1994) 6 SCC 632; *People's Union for Civil Liberties v. Union of India*, (1997) 1 SCC 301.

visits at night and regular surveillance., The Supreme Court struck down night-time domiciliary visits by the police as violative of órdered libertyô.[109] Further, the Supreme Court held that Article 21 of the Constitution of India is the repository of residuary personal rights and it recognised the common law right to privacy. However, the Court observed that privacy is not a guaranteed fundamental right. It must be noted though, dissenting judge, Justice Subba Rao, opined that even though the right to privacy was not expressly recognised as a fundamental right, it was an essential ingredient of personal liberty under Article 21 and thus fundamental.

Following this approach of Justice Subba Rao, the nine-judge bench of the Supreme Court in *Puttaswamy* recognised the right to privacy as an intrinsic part of the fundamental right to life and personal liberty under Article 21 of the Constitution of India in particular, and in all fundamental rights in Part III which protect freedoms in general, and overruled the aforementioned judgments to this extent.[110] Notably, it was held that the Constitution of India must evolve with the circumstances of time to meet the challenges thrown up in a democratic order governed by the rule of law and that the meaning of the Constitution of India cannot be frozen on the perspectives present when it was adopted.

The right to privacy was grounded in rights to freedom under both Article 21 and Article 19 of the Constitution of India encompassing freedom of the body as well as the mind. It was held that ñprivacy facilitates freedom and is intrinsic to the exercise of libertyò[111] and examples of the freedoms enshrined under Article 25, Article 26 and Article 28(3) of the Constitution of India were given to show how the right to privacy was necessary to exercise all the aforementioned rights.[112] The approach of the Supreme Court in *Kharak Singh* and *A.K. Gopalan v. State of Madras*[113] of putting the freedoms given under Part III of the Constitution of India under distinct compartments was also rejected. Instead, it was held that that these rights are overlapping and the restriction of one freedom affects the other, as was also held previously in the *Maneka*[114] and *Cooper*[115] judgments.[116] Therefore, a law restricting a freedom under Article 21 of the Constitution of India would also have to meet the reasonableness requirements under Article 19 and Article 14 of the Constitution of India.[117]

The Supreme Court acknowledged that the concept of the right to privacy, as seen from jurisprudence in India and abroad has evolved from the basic right to be let alone, to a range of negative and poistive rights. Thus it now includes óthe right to abort a foetus; rights as to procreation, contraception, general family relationships, child rearing, education, data

[109] *Kharak Singh v. State of Uttar Pradesh*, (1964) 1 SCR 332. Also discussed: Per S.A. Bobde, J. at paragraph 6; Per Chelameswar, J. at paragraph 9; Per D.Y. Chandrachud, J. at paragraph 27.
[110] Per S.A. Bobde, J. at paragraph 6; Per Chelameswar, J. at paragraph 9; Per D.Y. Chandrachud, J. at paragraph 27.
[111] Per D.Y. Chandrachud, J. at paragraph 169.
[112] Per S.A. Bobde, J. at paragraph 32.
[113] *A.K. Gopalan v. State of Madras,* AIR 1950 SC 27
[114] *Maneka Gandhi v. Union of India*, (1978) 1 SCC 248.
[115] *Rustom Cavasji Cooper v. Union of India*, (1970) 1 SCC 248.
[116] Per D.Y. Chandrachud, J. at paragraph 164; per S.A. Bobde at Paragraph 7.
[117] Per D.Y. Chandrachud, J. at paragraph 165.

protection, etc.ô[118] The Court recognised óinformational privacyô as an important aspect of the right to privacy that can be claimed against state and non-state actors. The right to informational privacy allows an individual to protect information about herself and prevent it from being disseminated.[119] Further, the Court recognised that the right to privacy is not absolute and may be subject to reasonable restrictions. In order to limit discretion of State in such matters, the Court has laid down a test to limit the possibility of the State clamping down on the right ï the action must be sanctioned by law, it must be necessary to fulfil a legitimate aim of the State, the extent of the State interference must be óproportionate to the need for such interferenceô, there must be procedural safeguards to prevent the State from abusing its power.[120] It has expressly recognised ñprotecting national security, preventing and investigating crime, encouraging innovation and the spread of knowledge, and preventing the dissipation of social welfare benefitsò[121] as certain legitimate aims of the State.

(ii) Legislative Developments

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

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

The SPDI Rules have been issued under Section 43A of the IT Act. Section 43A, relates to ñCompensation for Failure to Protect Dataò and enables the enactment of ñreasonable security practices and proceduresò for the protection of sensitive personal data. The SPDI Rules incorporate, to a limited extent, the OECD Guidelines, specifically: collection limitation, purpose specification, use limitation and individual participation.

The SPDI Rules mandate certain requirements for the collection of information,[122] and insist that it be done only for a lawful purpose connected with the function of the organisation.[123] In addition, every organisation is required to have a detailed privacy policy.[124] The SPDI Rules also set out instructions for the period of time information can be retained,[125] and gives individuals the right to correct their information.[126] Disclosure is not permitted without consent of the provider of the individual, or unless such disclosure is contractually permitted

[118] Per R.F. Nariman, J. at paragraph 42.
[119] Per D.Y. Chandrachud, J. at paragraph 142.
[120] Per S.K. Kaul, J., paragraph 71.
[121] Per D.Y. Chandrachud, at paragraph 185.
[122] Rule 5(1), SPDI Rules.
[123] Rule 5(2), SPDI Rules.
[124] Rule 4, SPDI Rules.
[125] Rule 5(4), SPDI Rules.
[126] Rule 5(6), SPDI Rules.

or necessary for legal compliance.[127] When it comes to sharing information with Government agencies, then the consent of the provider is not required and such information can be shared for purposes such as verification of identity, prevention, detection and investigation including of cyber incidents, prosecution, and punishment of offences.[128]

The SPDI Rules apply only to corporate entities[129] and leaves the government and government bodies outside its ambit; the rules are restricted to ósensitive personal dataô, which includes attributes like sexual orientation, medical records and history, biometric information etc.,[130] and not to the larger category of personal data. Further, the Cyber Appellate Tribunal (CyAT) which hears appeals under the IT Act has issued its last order in 2011. The absence of an effective enforcement machinery therefore raises concerns about the implementation of the SPDI Rules. It is thus necessary to make a comprehensive law to adequately protect personal data in all its dimensions and to ensure an effective enforcement machinery for the same.

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

The Aadhaar Act enables the Government to collect identity information from citizens[131] including their biometrics, issue a unique identification number or an Aadhaar Number on the basis of such biometric information[132], and thereafter provide targeted delivery of subsidies, benefits and services to them.[133] The Aadhaar Act also provides for Aadhaar based authentication services wherein a requesting entity (government/public and private entities/agencies) can request the Unique Identification Authority of India (UIDAI) to verify/validate the correctness of the identity information submitted by individuals to be able to extend services to them.[134] The requesting entity is required to obtain the consent of the individual before obtaining her identity information for the purpose of authentication and must use her identity information only for the purpose of authentication.[135]

The Aadhaar Act establishes an authority, namely, the UIDAI, which is responsible for the administration of the said Act.[136] It also establishes a Central Identities Data Repository (CIDR)[137] which is a database holding Aadhaar Numbers and corresponding demographic and biometric information.[138] Under the Aadhaar Act, collection, storage and use of personal data is a precondition for the receipt of a subsidy, benefit or service.[139] Though the Aadhaar

[127] Rule 6, SPDI Rules.
[128] Rule 6(1), SPDI Rules.
[129] Section 43-A, IT Act.
[130] Rule 3, SPDI Rules.
[131] Section 30, Aadhaar Act.
[132] Section 3, Aadhaar Act.
[133] Section 7, Aadhaar Act.
[134] Section 8, Aadhaar Act.
[135] Section 8(2), Aadhaar Act.
[136] Section 11, Aadhaar Act.
[137] Section 10, Aadhaar Act.
[138] Section 2(h), Aadhaar Act.
[139] Section 7, Aadhaar Act.

Act does not *per se* make application for an Aadhaar Number mandatory (it is specifically provided as an ‘entitlement’ under Section 3) except for availing of certain benefits, subsidies and services funded from the Consolidated Fund of India, in practice, taking of Aadhaar Number is becoming mandatory for availing most services through a range of cognate laws.[140]

The Aadhaar Act and its regulations recognise various data protection principles, to ensure the security of information and privacy of Aadhaar Number holders. First, there is an obligation on the UIDAI to ensure security and confidentiality of the identity information and authentication records of individuals which includes taking all necessary steps to protect such information against unlawful access, use or disclosure, and accidental or intentional destruction, loss or damage.[141] Further, the Aadhaar Act prohibits the sharing of core biometric information, and the use of it for a purpose other than the generation of Aadhaar Numbers and authentication.[142] The sharing of information other than core biometric information is permissible under certain conditions. The Aadhaar Act also permits an individual to make a request to the UIDAI to provide her access to her identity information (excluding her core biometric information)[143] and her authentication records.[144] She can also seek rectification of her demographic data if it changes/is incorrect, and her biometric information if it is lost or changes.[145] Finally, the UIDAI will have no knowledge of the purpose of any authentication.[146]

Data protection norms for personal information collected under the Aadhaar Act are also found in the Aadhaar (Data Security) Regulations, 2016 (Aadhaar Security Regulations). The Aadhaar Security Regulations impose an obligation on the UIDAI to have a security policy which sets out the technical and organisational measures which will be adopted by it to keep information secure.[147]

Despite its attempt to incorporate various data protection principles, Aadhaar has come under considerable public criticism. First, though seemingly voluntary, possession of Aadhaar has become mandatory in practice, and has been viewed by many as coercive collection of personal data by the State.[148] Concerns have also been raised *vis-a-vis* the provision on

---

[140] Komal Gupta and Suranjana Roy, ‘Aadhaar to be mandatory for mobile phone verification’, LiveMint (25 March 2017) available at http://www.livemint.com/Industry/wyGskI48Ak73ETJ5XW0diK/Aadhaar-now-a-must-for-all-mobile-phone-connections-after-ta.html (last accessed 5 November 2017); ‘PTI, ‘Linking Aadhaar number to bank accounts mandatory: RBI’, Business Line, (21 October 2017), available at: http://www.thehindubusinessline.com/money-and-banking/linking-aadhaar-with-bank-account-is-mandatory-rbi/article9917776.ece (last accessed 5 November 2017).

[141] Section 28, Aadhaar Act.

[142] Section 29, Aadhaar Act.

[143] Section 28(5), Aadhaar Act.

[144] Section 32(2), Aadhaar Act.

[145] Section 31, Aadhaar Act.

[146] Section 32, Aadhaar Act.

[147] Regulation 3, Aadhaar Security Regulations.

[148] Reetika Khera, ‘The Different Ways in Which Aadhaar Infringes on Privacy’, The Wire (19 July 2017), available at https://thewire.in/159092/privacy-aadhaar-supreme-court/ (last accessed 16 November 2017); Reetika Khera, ‘No Good Will Come from Linking Aadhaar to Mid-Day Meals’, The Wire (24 March 2017), available at https://thewire.in/118555/aadhaar-mid-day-meals/ (last accessed 16 November 2017).

Aadhaar based authentication which permits collection information about an individual every time an authentication request is made to the UIDAI.[149] Finally, despite an obligation to adopt adequate security safeguards, no database is 100% secure.[150] In light of this, the interplay between any proposed data protection framework and the existing Aadhaar framework will have to be analysed.

c. Financial Sector

Financial information, being a highly sensitive category of information, necessitates an adequate data protection regime for its protection. The primary legal instruments that address data protection in the financial sector include: the Credit Information Companies (Regulation) Act, 2005 (CIC Act), the Credit Information Companies Regulation, 2006 (CIC Regulations) and circulars issued by the Reserve Bank of India (RBI). Further, the SPDI Rules recognise financial information such as credit card, debit card and other payment instrument details as sensitive personal data, thus to that extent regulating their use, collection and disclosure.[151]

i. CIC Act

In the financial sector, provisions scattered across various statutes provide for an obligation to maintain customer confidentiality and adherence to data protection norms. However, the CIC Act, along with the CIC Regulations, is perhaps the legislation with the most comprehensive provisions on data protection in the financial sector.

The CIC Act primarily applies to credit information companies (CICs) and recognises them as collectors of information.[152] The CIC Act imposes an obligation on CICs to adhere to privacy principles at the stage of collection, use and disclosure of credit information[153], and requires them to ensure that credit information held by them is accurate, complete and protected against loss or unauthorised use, access and disclosure.[154] Similarly, the CIC Regulations impose an obligation on CICs to ensure data security and secrecy. It also requires them to adhere to a large number of recognised data protection principles such as: data collection limitation, data use limitation, data accuracy, data retention and access and modification.[155]

ii. RBI Circulars

[149] Jean Dreze, ôHello Aadhaar, Goodbye Privacyô, The Wire (24 March, 2017) available at https://thewire.in/118655/hello-aadhaar-goodbye-privacy/ (last accessed 5 November 2017)
[150] Subhashis Banerjee *et al.,* A Computer Science Perspective: Privacy and Security of Aadhaar, 52(37) Economic & Political Weekly (16 September 2017).
[151] Section 3(ii), SPDI Rules.
[152] Regulation 2(b), CIC Regulations.
[153] Section 20, CIC Act.
[154] Section 19, CIC Act.
[155] Chapter VI, Privacy Principles, CIC Regulations.

The Know Your Customer (KYC) norms limit the categories of information that banks and financial institutions can seek from their customers.[156] Once such information is collected, there is an obligation on banks to keep it confidential.[157] Further, multiple instruments such as the Master Circular on Credit Card, Debit Card and Rupee Denominated Co-branded Prepaid Card Operations of Banks and Credit Card issuing NBFCs,[158] the Master Circular on Customer Services, 2009[159] and the Code of Banks Commitment to Customers[160] etc. all provide for privacy and customer confidentiality obligations that have to be adhered to by various entities in the financial sector.

d. Telecom Sector

There are multiple laws that operate in the telecom sector such as the Indian Telegraph Act, 1885 (Telegraph Act), the Indian Wireless Telegraphy Act, 1933, the Telecom Regulatory Authority of India Act, 1997 (TRAI Act) and various regulations issued thereunder. However, data protection norms in the telecom sector are primarily dictated by the Unified License Agreement (ULA) issued to Telecom Service Providers (TSP) by the Department of Telecommunications (DoT).

The format in which, and the types of information that are to be collected from the individual is prescribed by the DoT.[161] A TSP has an obligation to take necessary steps to safeguard the privacy and confidentiality of the information of individuals to whom it provides a service and from whom it has acquired such information by the virtue of the service provided.[162]

Further, the TSP is obliged to maintain all commercial, call detail records, exchange detail records and IP detail records for at least one year for scrutiny by the DoT.[163]As far as security safeguards are concerned, there are multiple obligations prescribed for the TSP which includes inducting only those network elements into its telecom network which have been

---

[156] 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).

[157] RBI Master Circular on Customer Service in UCBs dated 1 July 2015, available at: https://www.rbi.org.in/scripts/BS_ViewMasCirculardetails.aspx?id=9863, (last accessed November 5, 2017).

[158] 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).

[159] 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).

[160] Code of Bankôs Commitment to Customers, ôSection 5- Privacy and Confidentialityô, Banking Codes and Standards Board of India (June 2014), available at: https://www.dbs.com/in/iwov-resources/pdf/codeofbanks-aug091.pdf (last accessed 3 November 2017).

[161] Clause 39.17, Unified License Agreement.

[162] Clause 37.2, Unified License Agreement.

[163] Clause 39.20, Unified License Agreement.

tested as per the contemporary Indian or International Security Standards,[164] amongst others.[165] Finally, customer information can be disclosed only if the individual has consented to such disclosure and the disclosure is in accordance with the terms of consent.[166] In addition, the TSP has to make efforts to comply with the Telegraph Act which imposes an obligation on it to facilitate the Government to carry out ôinterceptionô of messages in case of emergencies - a privacy intrusion justified largely in the name of national security. There are some procedural safeguards built into this process of interception.[167]

Further, the Telecom Regulatory Authority of India (TRAI) has framed the Telecom Commercial Communication Preference Regulations, 2010 (TRAI Regulations) to deal with unsolicited commercial communications.[168] The TRAI Regulations envisage the setting up of Customer Preference Registration Facility[169] by telecom service providers through which customers could choose to not receive commercial communications. However, these regulations are limited to messages and other communication through phones, and would would not cover an email application or advertisements appearing on browsers.

e. Health Sector

Despite the inherently sensitive nature of health information, the legal framework on data protection in the health sector appears to be inadequate. The Clinical Establishments (Central Government) Rules, 2012 (Clinical Establishments Rules) requires clinical establishments to maintain and provide Electronic Medical Records/Electronic Health Records, thus mandating the storage of health information in an electronic format.[170] The SPDI Rules recognise health information as constituting ôsensitive personal dataô and thus regulates its collection, use and disclosure. However, as already mentioned the SPDI Rules apply only to the private sector thus leaving the whole of the public health sector outside its ambit.

The Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations, 2002 (IMC Code) issued under the Indian Medical Council Act, 1956 mandate physician-patient confidentiality unless the disclosure of the patientôs information is required by law, or if there is a serious and identified risk to an individual/community, or the disease is a notifiable one.[171] Interestingly, at the same time the IMC Code requires that the patient, her relatives and responsible friends have knowledge of the patient's condition so as to serve her best interests[172] thus allowing for disclosure without the consent of the patient. Further, physicians are encouraged to computerise medical records, maintain them for a period of three years and provide access to them to the patient upon her request.[173] However, the limited privacy

[164] Clause 39.7, Unified License Agreement.
[165] Clause 39, Unified License Agreement.
[166] Clause 37.2, Unified License Agreement.
[167] Rule 419-A, Telegraph Act.
[168] Regulation 2(i), TRAI Regulations.
[169] Regulation 3, TRAI Regulations.
[170] Rule 9(iv), Clinical Establishments Rules.
[171] Section 2.2., IMC Code.
[172] Section 2.3. IMC Code.
[173] Section 1.3.2, IMC Code.

safeguards and absence of an enforcement mechanism renders the IMC Code largely inadequate to address the concerns surrounding health information.

These existing laws and regulations will have to be analysed and changes, if any, concomitant with the introduction of a new data protection framework, suggested.

(iii) The AP Shah Committee Report

In 2012, a Group of Experts on Privacy was constituted by the erstwhile Planning Commisison under the Chairmanship of Justice AP Shah (Justice AP Shah Committee). The report of the Justice AP Shah Committee recommended a detailed framework that serves as the conceptual foundation for a privacy law in India, considering multiple dimensions of privacy. After a detailed deliberative and consultative exercise, it proposed a set of nine National Privacy Principles to be followed, broadly derived from the OECD Guidelines.[174] It also proposed a co-regulatory form of enforcement with privacy commissioners set up by statute along with self-regulatory organisations.[175] The principles recommended by the Justice AP Shah Committee as well as the model of enforcement deserve close scrutiny insofar as they relate to question of data protection.

5. Possible Approaches

As discussed above, the analysis of the data protection models followed by the EU and the US sets out two basic approaches: the EU model is a rights based one, where protection of personal data is equated with protecting the fundamental right to privacy. The EU model has been criticised however, for being excessively stringent, and imposing many obligations on the organisations processing data. At the other end of the spectrum is the US approach, which focuses on protecting the individual from excessive State regulation. The US model recognises the value of data *vis-a-vis* encouraging innovation, and therefore allows collection of personal information as long as the individual is informed of such collection and use. However it has been viewed as inadequate in key respects. Several hybrid models also exist. These approaches must be kept in mind alongside the recognition of the right to privacy by the Supreme Court of India and legislative and other developments which have already taken place in India.

At the same time, one must be mindful of the need to encourage innovation, recognised by the Supreme Court of India, in its decision holding privacy to be fundamental, yet limited by reasonable restrictions. In addition, Indiaôs potential to lead the world into a digital economy making use of its existing strengths in information technology, demographic dividend, and its need for empowerment based on data-driven access to services and benefits for the common

[174] The nine principles set out by the Justice AP Shah Committee are as follows:
Principle 1: Notice; Principle 2: Choice and Consent; Principle 3: Collection Limitation; Principle 4: Purpose Limitation; Principle 5: Access and Correction; Principle 6: Disclosure of Information; Principle 7: Security; Principle 8: Openness; Principle 9: Accountability
Report of the Justice AP Shah Committee, 21-27 (October 16, 2012).
[175] Report of the Justice AP Shah Committee, 5 (October 16, 2012).

man and woman must be kept in mind. Factoring in these diverse objectives, a nuanced approach towards data protection will have to be followed in India. It is to understand what these nuances are that this White Paper has been drafted for public consultation and comments.

This White Paper has been divided into three substantive parts:

Part II- Scope and Exemptions;
Part III- Grounds of Processing, Obligation on Entities and Individual Rights; and
Part IV- Regulation and Enforcement.

Each Part contains several Chapters comprising brief notes on every aspect that we envisage will form a part of a data protection law. Each note, in turn, sets out the key issues that need to be considered, international practices relevant in this regard, provisional views of the Committee based on its research and deliberations and questions for public consultation. For easy reference, a summary is provided at the end of the paper in Part V listing all questions for public consultation. The purpose of this exercise is to ascertain the views of key stakeholders and the general public on each of these aspects. It must be emphasised that this format for consultation has been followed based on the need to ensure targeted consultation with stakeholders. The provisional views of the Committee are meant to provoke discussion and debate and do not represent its final views in any manner. Further, the questions suggested for discussion are carefully formulated and would serve their purpose if careful and precise and answers are provided.

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] ñS.S. Lotusò (*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, Brownlieôs Principles of International Lawô, 456 (Oxford, 8th Ed, 2008).
[178] Crawford, Brownlieôs Principles of International Law, 457 (Oxford, 8th Ed, 2008).
[179] Crawford, Brownlieôs Principles of International Law, 458 (Oxford, 8th Ed, 2008),.
[180] Dan Jerker B. Svantesson, óExtraterritoriality in the context of Data Privacy Regulationô, 7(1) Masaryk University Journal of Law and Technology 87 (2012); Christopher Kuner, óExtraterritoriality and Regulation of International Data Transfers in EU Data Protection Lawô, 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, ôAgainst Data Exceptionalismõ, 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: ôIf Article 25 of Directive 95/46 were interpreted to mean that there is ótransfer [of data] to a third countryõ 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.õ

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

[184] Dan Jerker B Svantesson, ôA Layered Approach To The Extraterritoriality Of Data Privacy Lawsõ, 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 ñcarries on business in Australiaò 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, óExtraterritoriality in the context of Data Privacy Regulationô, 7(1) Masaryk University Journal of Law and Technology 87 (2012).
[186] óNew Rules, Wider Reach: The Extraterritorial Scope of the GDPRô, 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, óAPP Guidelines- Key Conceptsô (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, óAPP Guidelines- Key Conceptsô (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, ôAgainst Data Exceptionalismõ, 68(4) Stanford Law Review 729, 748 (April 2016).
[195] Dan Jerker B. Svantesson, ôExtraterritoriality in the context of Data Privacy Regulationõ, 7(1) Masaryk University Journal of Law and Technology 87,138 (2012).
[196] Dan Jerker B. Svantesson, ôExtraterritoriality in the context of Data Privacy Regulationõ, 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, ôData protection in Indonesia: Overviewõ, 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 ónatural personsô as the definition of ópersonal dataô 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 companyôs 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: óEveryone has the right to recognition everywhere as a person before the law.ô

[200] Article 29 Data Protection Working Party, óOpinion 4/2007 on the Concept of Personal Dataô, 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, ôPrivacy and Data Protectionô 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, ôPrivacy and Data Protectionô 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 individualôs 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, ôReport of the Special Rapporteur on the right to privacyõ, 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 ñ*All processing of personal information must within one year after the commencement of this section be made to conform to this Act*.ò 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, ôPOPI - is South Africa keeping up with international trends?ô 84(44) De Rebus (May 2014) , available at: http://www.saflii.org/za/journals/DEREBUS/2014/84.html, (last accessed 28 October 2017).
[207] ôCompliance with the Personal Information Protection and Electronic Documents Actô, Aylesworth LLP, available at: http://documents.jdsupra.com/4217f03e-a265-4711-a230-103d2a5f3140.pdf, (last accessed 28 October 2017).
[208] ôCompliance with the Personal Information Protection and Electronic Documents Actô, 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. ôInformationô 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 ñinformationò 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 ñsensitive personal information or sensitive personal dataò.[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: ôDataô, Oxford Dictionaries, available at: https://en.oxforddictionaries.com/definition/data, (last accessed 1 November 2017).

[211] Definition of information, can be found at: ôInformationô, 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 ñdataò or ñinformationò 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 ñinformationò. 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, ñOpinion 4/2007 on the Concept of Personal Dataò, 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 ñrobustnessò 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, ôHandbook on European Data Protection Lawô (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, ôPrivacy Expert Group Report on the Review of the 1980 OECD Privacy Guidelinesô, 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, ôBroken Promises of Privacy: Responding to the surprising failure of Privacyô, 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 personôs 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 ñPersonally Identifiable Informationò (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, ôPrivacy Expert Group Report on the Review of the 1980 OECD Privacy Guidelinesô, 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, ôRegulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security and Consentô, 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, ôThe PII Problem: Privacy and a New Concept of Personally Identifiable Informationô, 86 NYU Law Quarterly Review 1814 (2011).

that the information is not in the ñpublic domain.ò 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. Californiaôs 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 ópersonal dataô or ópersonal informationôbe used?

   Alternatives:

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

> *ñSexual 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.ò*

Thus, apart from the harm of intrusion of oneôs 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 ñsensitiveò 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, ñAdvice paper on Special Categories of Data (ñsensitive dataò)ò, 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, ñGuidance note on Special Categories of Dataò, available at: https://ico.org.uk/for-organisations/guide-to-data-protection/key-definitions/, (last accessed 2 November 2017), ñThe 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.ò

[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, ôProtecting Personal Information: A Guide for Businessô (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, ôThe Privacy Act: Some Important Definitionsô, 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 ñprocessingò. 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 óprocessingô 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 termsð 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.

ófiling systemô.[254] A ófiling systemô has been defined as óany structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.ô[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 ñdata controller.ò 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 ñthird partyò 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* ódefinition of data controllerô in OECD, óOECD Guidelines Concerning the Protection of Privacy and Transborder Flows of Personal Dataô (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, óOpinion 01/2010 on the Concepts of óControllerô and óProcessorôö, 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 ôholdsô 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, ó Opinion 01/2010 on the Concepts of ó Controllerô and ó Processorôö, 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, ó Australian businesses and the EU General Data Protection Regulationô (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 ódata controllerô. The competence to determine the purpose and means of processing may be the test for determining who is a ódata controllerô.

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 ódata controllerô or should it additionally define ódata processorõ?

   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 ódata controllerô (entity that determines the purpose of collection of information) and attribute primary responsibility for privacy to it.
   c. Use the two concepts of ódata controllerôand ódata processorô(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, óChapter 11: Obligations of processors ï Unlocking the EU General Data Protection Regulationõ, 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 ï (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 ópublishing powerô 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 individualôs 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 ójournalistic purposesô and ójournalistô 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 Justiceï 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 colleaguesô 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 ï ôProposals for Amendments regarding exemption for personal or household activities (EU)ô, 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 ï ôProposals for Amendments regarding exemption for personal or household activities (EU)ô, 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 ónecessary to reconcile the right to the protection of personal data with the freedom of expression and information.ö[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 ójournalistô, ójournalisticô, óartisticô, óliteraryô 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 Commissionerôs Office (UK) Guidance, óData Protection and Journalism: A Guide for the Mediaô (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 Commissionerôs Office (UK) Guidance, óData Protection and Journalism: A Guide for the Mediaô (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 óFor 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)ô.

[281] Section 32, UK DPA.

[282] Section 7, POPI Act.

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

[284] Singapore exempts ónews organisationsô from seeking consent for collection of personal data strictly for ónews activitiesô. They are not exempted from other principles. *See* Graham Greenleaf, óAsian Data Privacy Laws: Trade & Human Rights Perspectivesô, 481 (Oxford University Press, 2016).

[285] South Korea provides a general exemption for personal data that is collected for óuse for reporting by the press,ô *see* Graham Greenleaf, óAsian Data Privacy Laws: Trade & Human Rights Perspectivesô, 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 ôhistorical, statistical or research activity.ô 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 ôresearchô 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) <u>Other categories of exemptions that have been incorporated by some jurisdictions</u>

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 ónecessary or desirable for the purpose of any investigation, inquiry, trial or other proceeding under this Code.ô Section 93 of the CrPC empowers the Court to issue a ósearch warrantô to compel individuals to produce the necessary documents or things in certain circumstances.

Further, the PMLA provides powers of search and seizure to a ôDirector or any other officer not below the rank of Deputy Director.ô[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 ówhich would impede the process of investigation or apprehension or prosecution of offendersô is exempted from disclosure under the Right to Information Act, 2005 (RTI Act).[302] This refers to information about ótargets of investigationô or an óaccusedô. 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 ï óprevention or detection of crimeô; or óapprehension or prosecution of offendersô; or óassessment 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] ôRecordsô 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.ô 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 ó 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.ô[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 ñan offence against the Stateò, 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 individualôs 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 ódetermination has passed on to the data processors themselves.ô[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, óExemptions to the European Union Personal Data Privacy Directive: Will They Swallow the Directive?ô, 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 ñhear applications for and grant orders approving electronic surveillance anywhere within the United Statesò 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 ñforeign intelligence purposesò 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 ñinternational terrorism or clandestine intelligence activitiesò.

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 ódomesticô or óhousehold purposeô 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 ójournalistô and ójournalistic purposeô 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 óliteraryô or óartisticô 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 óprevention of crimeô 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 ódata Nationalismô[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, óBinding Corporate Rules for Cross-Border Data Transferô 3(2) Rutgers Journal of Law & Urban Policy 154, 171 (2006).
[317] Coalition of Services Industries, óCross-Border Data Flowsô, 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, ódata Nationalismô, 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, ódata Nationalismô, 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, óExploring Data-Driven Innovation as a New Source of Growth: Mapping The Policy Issues Raised By "Big Dataô, 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, óThe Internet, Cross-Border Data Flows and International Tradeô, 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 óadequate levelô 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 Jerseyô, 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, óOpinion 11/2011 on the level of protection of personal data in New Zealandô, 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, óOpinion 6/2010 on the level of protection of personal data in the Eastern Republic of Uruguayô, 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, óOverview on Binding Corporate Rulesô, 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, óOverview on Binding Corporate Rulesô, 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, óFrequently Asked Questions Relating to Transfers of Personal Data From The EU/EEA To Third Countriesô, 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, óModel Contracts for the Transfer of Personal Data to Third Countriesô, 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 ôresponsible partyô 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 ôresponsible partyôcan 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, ôFact-Sheet: Overview of EU-US Privacy Shield Frameworkô (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, ôChapter 8: APP 8 ð Cross-border disclosure of personal informationô (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 ñprovide a comparable level of protection while the information is being processed by the third party.ò

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 ð 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, óPersonal Information Transferred Across Bordersô (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, óPersonal Information Transferred Across Bordersô (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, óPersonal Information Transferred Across Bordersô (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, óPersonal Information Transferred Across Bordersô (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, óGlobal Data Privacy Directoryô (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. œEuropean Union Data Protection Directive: Adequacy of Data Protection in Singapore,ô 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 USô 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, ôThe Growth Of Data Localization Post-Snowden: Analysis And Recommendations For U.S. Policymakers And Business Leadersõ, The Hague Institute for Global Justice, Conference on the Future of Cyber Governance 2014, 5 (1 May 2014) as cited in Erica Fraser, ôData Localisation and the Balkanisation of the Internetõ, 13(3) SCRIPTed 359 (December 2016).
[362] Anupam Chander and Uyên P. Lê, ôBreaking the Web: Data Localisation vs. the Global Internetõ UC Davis Legal Studies Research Paper No. 378, (April 2014).
[363] Andrew Keane Woods, ôAgainst Data Exceptionalismõ, 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

ñCross border data transferò is a broad concept, which involves international cooperation in ñdata processingò, 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.,* ôData Localisation in Russia: A self-imposed sanctionõ, 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), ôData Protection Regulations and International Data Flows: Implications for Trade and Developmentsõ (2016), available at: http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf ,(last accessed 12 October 2017).

[366] Neha Mishra, ôData Localisation Laws in a Digital World- Data Protection or Data Protectionism?õ, 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.,* ôThe Economic Importance of Getting Data Protection Right: Protecting Privacy, Transmitting Data, Moving Commerceõ, 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 Indiaôs 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 Indiaôs GDP in 2015ï16.[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 ñsmart factory,ò 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, ôRole of BPO and its Impact on Indian Economyô, 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 ñsmartò 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, óCyber-Physical Systemsô (2017), available at: https://www.nist.gov/el/cyber-physical-systems, (last accessed 30 October 2017).

[371] Bernard Marr, ôWhat Everyone Must Know About Industry 4.0ô, 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. GICsô ability to create cost savings for an enterprise while tapping Indiaôs 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, ôCloud Services Brokerage: A Must-Have for Most Organizationsô, 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.,* ôGlobal In-house Centers in Indiaô, 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 countryôs 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 citizenôs 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, ôData Localisation and the Balkanisation of the Internetô, 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 Peopleôs Congress of the Peopleôs 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, ôIndonesia: New Regulation on Personal Data Protectionô (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).

PART III
GROUNDS OF PROCESSING, OBLIGATION ON ENTITIES AND INDIVIDUAL RIGHTS

CHAPTER 1: CONSENT

1.1 Introduction

Consent forms the foundation of data protection law in many jurisdictions. There is great value in using consent as a validating mechanism for data processing. It satisfies two needs. First, consent is intuitively considered as the most appropriate method to ensure the protection of an individualôs autonomy.[392] Allowing an individual to have autonomy over her personal information allows her to enjoy ñinformational privacyò. Informational privacy may be broadly understood as the individualôs ability to exercise control over the manner in which her information may be collected and used.[393] Second, consent provides a ñmorally transformativeò value as it justifies conduct, which might otherwise be considered wrongful.[394] For instance, seeking consent is what differentiates entering someoneôs house with permission, from trespass.

Recently, the *Puttaswamy* judgment, held that the right to privacy would encompass the right to informational privacy, which recognises that an individual should have control over the use and dissemination of information that is personal to her.[395] Unauthorised use of personal information would lead to an infringement of this right.

Consent has largely been considered to be an efficient means of protecting an individualôs information.[396] Operationalising consent is done through the mechanism of ñnotice and choiceò. Through this, the individual is put in charge of the collection and use of her personal information. This is believed to be a more flexible, inexpensive and easily enforceable mechanism of protecting personal data of individuals, rather than strict regulation over how individualsô data may be used.[397] Seeking consent allows the individual to be responsible for managing her own information, thereby resulting in ñprivacy self-managementò[398].

---

[392] ñIn democratic societies, there is a fundamental belief in the uniqueness of the individual, in his basic dignity and worthé and in the need to maintain social processes that safeguard his sacred individuality.ò *See:* Alan Westin, ôPrivacy and Freedomô, (Atheneum, 1967).

[393] Adam Moore, ôToward Informational Privacy Rightsô, 44 San Diego Law Review 809 (2007).

[394] John Kleinig, ôThe Nature of Consentô in ôThe Ethics of Consent- Theory and Practiceô, 4 (Alan Wertheimer and Franklin Miller (*eds*.), Oxford University Press, 2009).

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

[396] Joel R. Reidenberg *et al*., ôPrivacy Harms and the Effectiveness of the Notice and Choice Frameworkô, 11 Journal of Law and Policy for the Information Society, 485, 489, (2015).

[397] Ryan M. Calo, ôAgainst Notice Skepticism in Privacy (and Elsewhere)ô, 87(3) Notre Dame Law Review 1027 (2012), available at: http://scholarship.law.nd.edu/cgi/viewcontent.cgi?article=1020&context=ndlr, (last accessed 21 October 2017).

[398] Privacy self-management has its origins in the Fair Information Practices (FIPPs), which were created in the 1970s in order to address concerns about the increasing digitisation of data. These principles also helped shape the OECD Privacy Guidelines. *See* Daniel Solove, ôPrivacy Self-management and the Consent Dilemmaô, 126 Harvard Law Review 1880, 1881, (2013).

Another advantage of relying on consent to protect personal information is that it takes into account varying privacy principles. An individual may often be best placed to determine how much of her personal information she is willing to exchange in return for the goods and services offered by an organisation. For example, an individual buying a book online may be happy to allow the online store to track and record her shopping choices and to be informed of new releases in her genres of interest; another may not. The information regarding the purposes for which the online store could collect information could be provided to the individual by way of a privacy notice. In an ideal situation, the individual would read the privacy notice, become aware of the information collection practices of the organisation, and then make the decision whether or not she wishes to complete the online transaction. Here, consent could arguably be a more effective means of protecting personal data than the law stepping in and prohibiting the use of a customerôs personal data for promotional material. *Qua* the individual, this might be an efficient solution provided the uses of such information are within the bounds of reasonableness. But its systemic impact requires greater scrutiny.

1.2 Issues

Although consent continues to play a critical role in data protection law, several issues with the practical operation of consent have been observed over the years. These are described below:

(i) Lack of Meaningful and Informed Consent

Although the purpose of consent is to enable individuals to self-manage their privacy and ensure autonomy, this is often difficult to achieve in practice. Privacy self-management assumes that an informed and rational individual is capable of making appropriate decisions about her data collection and use. Needless to say, this is a questionable assumption.

Consent and notice go hand in hand. An individual can make an informed choice regarding the collection and use of her personal information, only on the basis of information that she receives from an organisation. Most individuals do not read privacy notices, and, if they do, are unable to comprehend the information contained in them. This may be because of certain flaws within the notice itself (which will be discussed in Part III, Chapter 3 of the White Paper). In certain situations, individuals do read the privacy notice, but they lack sufficient expertise to assess the consequences of agreeing to a particular use of their information.[399] This is particularly true in areas of rapidly changing technology where it might be difficult for an individual to continually educate herself about the advances in technology and consequently their impact on her privacy. Finally, even if individuals manage to read and understand the information contained in the notice, they will be able to make an informed choice only about the immediate use of their information. They may not be able to make an

[399] CGAP, Dalberg and Dvara Research, ôPrivacy on the Lineô (November 2017), available at: https://dalberg.com/our-ideas/privacy-line, (last accessed 18 November 2017).

informed choice regarding the possible future uses of their information, and the harms that may arise as a result. All these factors contribute towards decreasing the value of consent.[400]

This issue is especially relevant with respect to the growing use of data aggregation techniques. Individuals may be able to foresee an immediate harm caused by misuse of their personal information, however, it is highly unlikely that they will be able to predict future uses of their information, which takes place after combining it with other data sets.

Further, many organisations use notices as a means to disclaim their liability instead of actually using this opportunity to inform the individual about the organisationsô data use practices. The presence or absence of a notice may be a first step for regulators to determine whether an organisation is compliant with data protection laws in that country. Therefore, in order to make their privacy notice as comprehensive as possible, and avoid liability, organisations treat notices as legal documents and use legalese and technical terms that the individual may not understand.[401] This is a commonly noticed phenomenon.

(ii) Standards of consent

While recognising the importance of consent as a foundational concept, there may be a need for having different standards of consent for different transactions. A ñone-size fits allò model may not be sufficient. It may not be necessary to obtain óexpressô consent for certain routine transactions, if these activities do not involve processing sensitive personal information. For routine, low-risk transactions, an individualôs implied consent may be sufficient. If a data controller wishes to collect and use sensitive information, the misuse of which is likely to cause great harm to an individual, then the express consent of the individual may be required.[402] Therefore, there may be a need to explore and accommodate standards of consent within the data protection law and align it with different types of information.

(iii) Consent Fatigue

Consent as it was originally intended, is likely to suffice in an environment where there are limited reasons for collecting information and only a few uses to which it could be put. This would make it relatively easy for an individual to keep track of her information being collected, and to what purposes it is being put to use.[403] At present, data processing has become a largely routine activity and individuals are flooded with notices seeking permission to process data. Given the number of requests and the effort required to scrutinise each one,

---

[400] Daniel Solove, ôPrivacy Self-management and the Consent Dilemmaô, 126 Harvard Law Review 1880, 1881, (2013).
[401] Fred H. Cate, ôFailure of Fair Information Principlesô, in óConsumer Protection in the Age of Information Economyô, (Jane K. Winn *ed.*, Routledge, 2006).
[402] Article 29 Data Protection Working Party, óOpinion 15/2011 on the Definition of Consentô, European Commission (13 July 2011), available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf, (last accessed 24 October 2017).
[403] Rahul Matthan, ôBeyond Consent: A New Paradigm for Data Protection- Discussion Document 2017-03ô, Takshashila Institution, (19 July 2017), available at: http://takshashila.org.in/wp-content/uploads/2017/07/TDD-Beyond-Consent-Data-Protection-RM-2017-03.pdf, (last accessed 24 October 2017).

individuals may find it impossible to give meaningful consent. Many of these notices are written in complex language, and add to the difficulty. According to a study published in 2008, if everyone took the time to read each one of the privacy notices which came her way, the national opportunity cost of the time spent on reading privacy policies in the US alone, would have exceeded USD 781 billion.[404]

(iv) Lack of Bargaining Power

Some scholars believe that consent forms for collection of personal information often amount to ñcontracts of adhesionò, where the terms of the notice only provide a ñtake it or leave it optionò. Therefore, the individual has no opportunity to negotiate the terms of the notice, which she is agreeing to. If she does not agree, she has no option but to forego the service offered by the data controller.[405] This does not genuinely vest the individual with meaningful autonomy to negotiate over contractual terms. In the context of data collected by the government there is often not even a choice that is available. Consent, on this account, is thus circumscribed by the limited nature of choice available to the individual.

1.3 International Practices

European Union

Consent forms the primary basis for collection, use, and disclosure of personal information, in certain jurisdictions, such as Canada. Other jurisdictions recognise that relying only on consent may not be sufficient. For instance, the EU GDPR provides that there are six grounds on the basis of which personal information can be processed.[406] These include: consent, performance of contract, compliance with a legal obligation, protection of vital interest, public interest, and legitimate interest pursued by the controller.[407]

In order to ensure that the consent given by an individual is valid, the EU GDPR mandates that the consent must be freely given, specific, informed and unambiguous for processing of personal data. Consent has to be expressed by a ñstatement or by clear affirmative actionò. The EU GDPR recognises that there must be an increased standard for consent, when it comes to processing of sensitive data. It requires that consent in such situations must be ñexplicitò. However, at present, the manner in which ñexplicitò consent will be translated into actual practice is not clear.

---

[404] Aleecia M. McDonald and Lorrie Faith Cranor, ôThe Cost of Reading Privacy Policiesõ, I/S: A Journal of Law and Policy for the Information Society (2008), available at: http://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf, (last accessed 24 October 2017).

[405] Arthur Leff, ôContract as a Thingõ, 19 American University Law Review 131 (1 January 1970), available at: http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=3809&context=fss_papers, (last accessed 24 October 2017).

[406] Regulation EU 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

[407] Article 6(1)(a), EU GDPR provides with respect to consent that:
ñ*Processing shall be lawful only if and to the extent that at least one of the following applies- the data subject has given consent to the processing of his or her personal data for one or more specific purposes.*ò

United Kingdom

The UK DPA also requires the data subject to provide consent for the processing of her personal data.[408] The UK DPA follows the EU GDPR approach by making consent only one of the six grounds for lawful processing.

South Africa

The POPI Act also recognises that processing of personal data should only takes place with the consent of the data subject. It follows the EU GDPR and the UK DPA approach by making consent one of the other grounds for lawful processing of personal data.[409]

Canada

Under Canadaôs PIPEDA, organisations are required to obtain an individualôs valid consent to lawfully collect, use and disclose personal information in the course of commercial activity.[410] Recognising the need to have different standards of consent, the 2015 amendment to PIPEDA (through the Digital Privacy Act) provides that the form of consent required depends on the circumstances and the type of information being collected.[411] While express consent is necessary for sensitive information, implied consent is sufficient for non-sensitive information.[412] The Digital Privacy Act introduced a ñgraduated consent standardò or a ñsliding-scaleò for obtaining valid consent. The Digital Privacy Act stipulates that an individualôs consent will be valid only if an individual could reasonably expect to understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which she has consented.[413]

Australia

Under the Privacy Act, consent is not directly a pre-requisite for collecting personal information. The only requirement prior to collecting personal information is that the information should be reasonably necessary for the agencyôs (government body) or the organisationôs (private entity) activities. The APPs set out that personal information should be collected directly from the individual unless the individual has consented to collection from other sources, or if it is authorised by law.[414] The bar is significantly higher for the collection of sensitive information as the individualôs consent is required in addition to the condition

[408] Section 4, read with Schedule 1 (Principle 1), Schedule 2 (Condition 1) and Schedule III (Condition 1) of the UK DPA.
[409] Section 11(1)(a)-(f), POPI Act.
[410] Principle 4.3, Schedule 1, PIPEDA.
[411] Principle 4.3.4, Schedule 1, PIPEDA.
[412] Principle 4.3.6, Schedule 1, PIPEDA.
[413] Dan Cooper, ôHighlights of the Canada Digital Privacy Actô, Covington & Burling LLP (24 June 2015), available at: https://www.insideprivacy.com/international/canada/highlights-of-the-canada-digital-privacy-act-2015/, (last accessed 24 October 2017).
[414] APP 3.6, Privacy Act.

that the collection is reasonably necessary for the entityôs functions. Under the Privacy Act, consent can mean either express consent or implied consent.

United States

In the US, privacy is protected by a patchwork of laws at the state and federal levels. Many are sector specific. Data protection practices are carried out largely on the basis of consent and notice. For example, legislations such as the GLB Act,[415] which governs the financial services industry, places certain obligations on financial institutions to seek the consent of consumer prior to collecting non-public financial institution and does not permit the disclosure of any non-public financial information to a third party in the absence of the consumerôs consent (obtained by way of notice).[416] Similarly HIPAA, which regulates medical information, requires that written consent of the data subject is required before disclosing medical information.[417]

1.4 Provisional Views

1. The importance of consent in data protection law is widely recognised. Keeping in mind the importance of consent, it is proposed that consent of individuals should be one of the grounds for collection and use of personal data. However, at the same time is it recognised that consent is being used as a means to disclaim liability. In the context of data collected and processed by the government, the individual often has no choice but to provide her data. Thus the validity of consent will have to be carefully determined.

2. In order for the consent to be valid, it should be freely given, informed and specific to the processing of personal data by way of a well-designed notice (discussed in Part III, Chapter 3 of the White Paper).

3. All transactions may not warrant the same standards of consent. Therefore, there may be a need to explore and accommodate standards of consent within the data protection law and align it with different types of information. Additionally, the standards for implied consent may need to be evolved in order to ensure that adequate information is provided to the individual giving her consent.

1.5 Questions

1. What are your views on relying on consent as a primary ground for processing personal data?

   Alternatives:

[415] 15 U.S.C. Sections 6801-6827.
[416] Section 502, GLB Act.
[417] 42 U.S.C. Section 1301.

a. Consent will be the primary ground for processing.
b. Consent will be treated at par with other grounds for processing.
c. Consent may not be a ground for processing.

2. What should be the conditions for valid consent? Should specific requirements such as ónambiguousô, ófreely givenô etc. as in the EU GDPR be imposed? Would mandating such requirements be excessively onerous?

3. How can consent fatigue and multiplicity of notices be avoided? Are there any legal or technology-driven solutions to this?

4. Should different standards for consent be set out in law? Or should data controllers be allowed to make context-specific determinations?

5. Would having very stringent conditions for obtaining valid consent be detrimental to day-to-day business activities? How can this be avoided?

6. Are there any other views regarding consent which have not been explored above?

CHAPTER 2: CHILD'S CONSENT

2.1 Introduction

It is estimated that globally, one in three Internet users is a child under the age of 18.[418] Although Internet-use among children is very common and children are becoming more familiar with technology, they are viewed as being more vulnerable than adults online. They may be more easily misled, given their lack of awareness with respect to the long-term consequences of their actions online.[419] Therefore, children represent a vulnerable group, which may benefit from receiving a heightened level of protection with respect to their personal information.[420]

Keeping in mind their vulnerability and increased exposure to risks online, there has been a call to take into consideration the rights of children in the ñdigital ageò. To this effect, the United Nations Convention on the Rights of the Child (UN CRC) recognises childrenôs rights to protection, including a specific protection against arbitrary or unlawful interference with childrenôs privacy and unlawful attacks on their honour and reputation.[421] Previously, most informational privacy laws were designed for everyone, without a special focus on protecting the processing of childrenôs personal information. However, studies conducted across the EU and the US have highlighted instances of personal data misuse and reputational damage (such as hacking social media accounts, creation of fake accounts and impersonation), which are affecting children.[422] Studies show that children also face difficulties while navigating privacy settings.[423] Additional issues relating to inadequate, non-child-tailored privacy policies, excessive collection of personal data from children and frequent disclosure of childrenôs data to third parties were also revealed.[424] Therefore, several jurisdictions have recognised the need to introduce data protection measures that are specifically applicable to the processing of childrenôs personal information.

2.2 Issues

[418] Sonia Livingstone *et al.*, óOne in Three: Internet Governance and Childrenôs Rightsô, Global Commission on Internet Governance Paper Series No. 22 (November 2015), available at: https://www.cigionline.org/sites/default/files/no22_2.pdf, (last accessed 28 October 2017).
[419] Milda Macenaite and Eleni Kosta, óConsent for Processing Childrenôs personal data in the EU: Following in US footsteps?ô, 26(2) Information & Communications Technology Law Journal (2017), available at: http://www.tandfonline.com/doi/full/10.1080/13600834.2017.1321096, (last accessed 28 October 2017).
[420] óChildrenôs data protection and parental consent: A best practice analysis to inform the EU data protection reformô, Advertising Education Forum (October 2013), available at: http://www.aeforum.org/gallery/5248813.pdf, (last accessed 28 October 2017) *citing:* Giovanna Mascheroni and Kjartan Olaffson, 'Risks and Opportunitiesô, Net Children Go Mobile (Second edn, Milano Educatt 2014).
[421] Article 16, United Nations Convention on the Rights of the Child.
[422] Milda Macenaite and Eleni Kosta, óConsent for Processing Childrenôs personal data in the EU: Following in US footsteps?ô, 26(2) Information & Communications Technology Law Journal (2017), available at: http://www.tandfonline.com/doi/full/10.1080/13600834.2017.1321096, (last accessed 28 October 2017).
[423] Sonia Livingstone *et al.*, óOne in Three: Internet Governance and Childrenôs Rightsô, Global Commission on Internet Governance Paper Series No. 22 (November 2015), available at: https://www.cigionline.org/sites/default/files/no22_2.pdf, (last accessed 28 October 2017).
[424] Global Privacy Enforcement Network, óSweep-Childrenôs Privacyô (2015), available at: http://194.242.234.211/documents/10160/0/GPEN+Privacy+Sweep+2015.pdf, (last accessed 28 October 2017).

(i) Balancing the issue of children lacking the legal competence to provide valid consent to data processing activities with the fact that children continue to use a large number of online services

Under the Indian Contract Act, 1872, a person is considered competent to contract as long as she is no longer a minor (above the age of 18). However, it may not be possible to prevent children from accessing any online service on this basis. As discussed above, children use many online services, access websites, and have social media accounts. Prior to using these services, the child will have to consent to the terms of use and notice of the websites. Websites attempt to circumvent this issue by seeking the parentôs consent on behalf of the child if the child is below the age of 18. However, other countries recognise that relying solely on parental consent for all children below the age of majority might have a chilling effect on the childôs opportunity to freely use the Internet as a medium of self-expression, growth and education. It also does not take into account that as a child becomes older, she gains the maturity and capacity to understand the purposes for which her information may be used, and so should not be solely reliant on a parentôs consent. The UK developed a test to gauge the capacity of a child to understand the consequences of what she is agreeing to in the absence of a parentôs consent, with respect to medical decisions.[425] Perhaps there is a need to develop a similar test in order to develop an alternative model for childôs consent generally with respect to data processing, though the form that the test will take in Indiaôs context.

(ii) Difficulty in determining which websites and entities must comply with the additional data protection requirements to safeguard children

The intention behind creating a specific protection regime for services which process childrenôs personal data is clear. However, it is difficult to pinpoint the exact type of entity to which it must apply. If additional data protection safeguards for children are only applicable to websites catering to children, as it is in the US, then this scope may be too narrow. This is because children also commonly access websites such as Facebook, which is technically not a ñchildrenôs websiteò. If the intended application is only towards commercial websites, or websites which support online transactions, as it is in the EU, which also collect information relating to a child, then this classification may also be flawed as many ónon-commercialô websites collect large amounts of data relating to children and generate revenue by way of their advertisements, tracking use patterns and so on. Therefore, it may be difficult to draw a line as to which websites will need to comply with additional child data protection requirements.

Additionally, specific standards need to be established for other non-website based collection of data about children. Schools and other educational institutions are getting increasingly digitised often deploying cloud based services and software as a service modules to manage their operations. These entities need clear guidance as to the manner in which they need to manage the information that they are storing with regard to children including regulations on

[425] Gilick Competence Test: *Gilick v. West Norfolk and Wisbech Area Health Authority and Department of Health and Social* Security [1984] Q.B. 581.

the cloud service provider as to storage, processing and transfer. The government also collects data about children as part of its various functions but does not follow any differential processing practices with regard to this data.

(iii) Difficulty in verifying the age of a child

It is very difficult to verify the age of a child using an online service.[426] Most of these transactions lack face-to-face value and the website operator or controller may find it difficult to verify the identity of its users. [427] Although there are some guidelines as to how such verification can be done, most of these procedures are unreliable and easily circumvented. Seeking to obtain parental consent may also be difficult to operationalise in practice.

2.3 International Practices

There are differing jurisdictional approaches with respect to determining when a child can be considered competent to act on her own behalf as a data subject under data protection law. Countries such as the US, South Africa and the EU prescribe a certain age, below which data processing activities can take place only with the consent of the parent. Countries such as Australia and the UK follow a subjective approach, based on the childôs understanding of the processing of information.

United States

COPPA is one of the first pieces of legislation designed to specifically protect the privacy of minors online. COPPA puts parents in control of what information commercial websites collect from children below the age of 13 online. [428] COPPA requires online services directed towards children to obtain verifiable parental consent before collecting personal information.[429] The FTC has provided guidance on certain measures to verify parental consent.[430]

European Union

The EU GDPR[431] explicitly recognises that children need more protection than adults, as they ñmay be less aware of risks, consequences, safeguards and their rights in relation to the processing of personal dataò, especially online.[432] In situations where processing of personal

[426] Article 29 Data Protection Working Party, ówOpinion 15/2011 on the Definition of Consentô, European Commission (13 July 2011), available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf, (last accessed 24 October 2017).
[427] Milda Macenaite and Eleni Kosta, ówConsent for Processing Childrenôs personal data in the EU: Following in US footsteps?ô, 26(2) Information & Communications Technology Law Journal (2017), available at: http://www.tandfonline.com/doi/full/10.1080/13600834.2017.1321096, (last accessed 28 October 2017).
[428] 15 USC 6501-6505, COPPA.
[429] Section 312.3, COPPA.
[430] Section 312.5 (b), COPPA.
[431] Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.
[432] Recital 38, EU GDPR.

data of children takes place on the basis of consent, the EU GDPR has established a parental consent requirement on websites, which offer ñinformation society servicesò[433] directly to children under the age of 16.[434] Lack of harmonised general rules on childrenôs data processing and consent, led to individual EU Member States to nationally set age-limits for children, at which parental consent would be required. For instance, the data protection law in Spain provides that data pertaining to data subjects over the age of 14 may be processed with their consent.[435]

South Africa

The POPI Act prohibits the processing of personal information of a child, unless certain special conditions allowing such processing apply.[436] These include where a competent person has earlier consented to such processing; where processing may be necessary for the establishment of a legal claim; where it is necessary to carry out a public interest task and so on. The POPI Act clarifies that any person who is below the age of 18, and who is not legally competent to take a decision on her behalf, is considered a child.

Australia

The Privacy Act provides that, in order for consent to be valid, an individual must have the capacity to consent. An organisation can presume that every individual has the capacity to consent, unless there is something to suggest otherwise, for instance, if the data being collected is that of a child. The Privacy Act does not specify a certain minimum age, after which an individual can make her own privacy decisions. If an organisation is handling the personal information of an individual under the age of 18 and knows this, the organisation must determine on a case-by-case whether that individual has the capacity to provide consent.[437] If the organisation is unable to gauge the capacity of the individual on a case-by-case basis, then it is presumed that an individual has the capacity to do so.[438]

Canada

---

[433] An Information Society Service is defined as ñany service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services.ò Article 1(1)(b) of Directive 2015/1535 of the European Parliament and of the Council.

[434] Article 8, EU GDPR.

[435] Article 13, Data Protection Act (Law 15/1999 on the protection of personal data).

[436] Sections 34 and 35, POPI Act.

[437] The APP guidelines state:
'As a general principle, an individual under the age of 18 has the capacity to consent when they have sufficient understanding and maturity to understand what is being proposed. In some circumstances, it may be appropriate for a parent/guardian to consent on behalf of a younger person.' OAIC, óAustralian Privacy Principles Guidelines: Privacy Act 1988ô (February 2014), available at: https://www.oaic.gov.au/images/documents/privacy/applying-privacy-law/app-guidelines/APP-guidelines-combined-set-v1.pdf, (last accessed 28 October 2017).

[438] OAIC, óProtection of Childrenôs Privacy in Focusô (11 May 2015), available at: https://www.oaic.gov.au/media-and-speeches/media-releases/protection-of-children-s-privacy-in-focus, (last accessed 28 October 2017).

The PIPEDA does not specifically deal with the issue of obtaining childôs consent. However, the Guidelines on Privacy and Online Behavioural Advertising recognise that it is difficult to ensure meaningful consent from children with respect to online behavioural practices, and organisations should avoid using tracking websites that are aimed at children.[439] Additionally, the Guidelines for Online Consent provide that organisations should recognise and adapt to special considerations in managing the personal information of children and youth. It recognises that the ability of children and youth to provide meaningful consent for the sharing of their personal information online depends on their cognitive and emotional development.[440]

United Kingdom

The UK DPA also does not explicitly refer to the age of consent of a child. However, the Information Commissionerôs Office (ICO) has provided some guidelines stating that processing must always be fair and lawful. Therefore, it is important to ensure that the individuals from whom data is being collected understand the reasons for which it is being collected. Therefore, with respect to children, the ICO suggests that it is a good practice to ensure that data is collected in a manner in which the audience (the child) is likely to understand, and that the amount and nature of data being collected from a child be proportional to her level of understanding.[441] In a recently reported development, Parliament is expected to take a view on banning usage of Facebook and Twitter by children under 13 years of age, contained in a bill that has been moved before it.[442]

2.4 Provisional Views

1. From studies relating to Internet use among children, it has been observed that children are generally recognised as a vulnerable group, and merit a higher standard of protection due to their relatively limited ability to adequately assess online privacy risks and consequently manage their privacy.

2. One solution to this could be to seek parental authorisation or consent when data controllers process personal data relating to children. This may also be a solution to the conundrum that children do not have the capacity to enter into a valid contract. Many jurisdictions recognise that solely relying on parentsô consent would have a chilling effect on the use of the Internet by children. Therefore, these jurisdictions have created

[439] Office of the Privacy Commissioner of Canada, ôGuidelines on Privacy and Online Behavioural Advertisingô (December 2011), available at: https://www.priv.gc.ca/en/privacy-topics/advertising-and-marketing/behaviouraltargeted-advertising/gl_ba_1112/, (last accessed 28 October 2017).
[440] Office of the Privacy Commissioner of Canada, ôGuidelines for Online Consentô (May 2014), available at: https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_oc_201405/, (last accessed 28 October 2017).
[441] ICO, ôPersonal Information Online: Code of Practiceô (July 2010), available at: https://ico.org.uk/media/for-organisations/documents/1591/personal_information_online_cop.pdf, (last accessed 28 October 2017).
[442] Edward Malnick, ôPeers issue warning over legislation banning children from joining Facebook and Twitter until they are 13ô, Telegraph (4 November 2017), available at: http://www.telegraph.co.uk/news/2017/11/04/children-will-banned-joiningfacebookand-twitter-13under-legislation/ (last accessed 15 November 2017).

an age-limit, below which a parentôs consent is necessary, in order to protect very young children from privacy harms. Similarly, a variable age limit can be drawn (not necessarily 18- which is the generally accepted age of majority in India) below which parental consent is to be mandatory. Methods for effectively ensuring parental consent must be considered, either for certain categories of services or through certain processes that may be onerous for the child to circumvent.

3. In addition, or in the alternative, perhaps distinct provisions could be carved out within the data protection law, which prohibit the processing of childrenôs personal data for potentially harmful purposes, such as profiling, marketing and tracking. Additionally separate rules could be established for the manner in which schools and other educational institutions that collect personal information about children as part of their regular activities need to collect and process this data. Similarly, regulations should be prescribed as to the manner in which the government collects and processes data about children.

2.5 Questions

1. What are your views regarding the protection of a childôs personal data?

2. Should the data protection law have a provision specifically tailored towards protecting childrenôs personal data?

3. Should the law prescribe a certain age-bar, above which a child is considered to be capable of providing valid consent? If so, what would the cut-off age be?

4. Should the data protection law follow the South African approach and prohibit the processing of any personal data relating to a child, as long as she is below the age of 18, subject to narrow exceptions?

5. Should the data protection law follow the Australian approach, and the data controller be given the responsibility to determine whether the individual has the capacity to provide consent, on a case by case basis? Would this requirement be too onerous on the data controller? Would relying on the data controller to make this judgment sufficiently protect the child from the harm that could come from improper processing?

6. If a subjective test is used in determining whether a child is capable of providing valid consent, who would be responsible for conducting this test?

   Alternatives:

   a. The data protection authority
   b. The entity which collects the information
   c. This can be obviated by seeking parental consent

7. How can the requirement for parental consent be operationalised in practice? What are the safeguards which would be required?

8. Would a purpose-based restriction on the collection of personal data of a child be effective? For example, forbidding the collection of childrenôs data for marketing, advertising and tracking purposes?

9. Should general websites, i.e. those that are not directed towards providing services to a child, be exempt from having additional safeguards protecting the collection, use and disclosure of childrenôs data? What is the criteria for determining whether a website is intended for children or a general website?

10. Should data controllers have a higher onus of responsibility to demonstrate that they have obtained appropriate consent with respect to a child who is using their services? How will they have ñactual knowledgeò of such use?

11. Are there any alternative views on the manner in which the personal data of children may be protected at the time of processing?

CHAPTER 3: NOTICE

3.1 Introduction

The role of consent in data protection law has been discussed in detail in Part III, Chapter 1 of the White Paper. Consent is operationalised through the mechanism of ñnotice and choiceò. The underlying philosophy is that consent through notice puts the individual in charge of the collection and subsequent use of her personal information.[443] The notice is a presentation of terms of the agreement by the data controller, whereas the choice is an action by the individual signifying the acceptance of the terms (such as when an individual clicks the ñI agreeò button on a website). Notice purports to respect the basic autonomy of the individual by arming her with relevant information and placing the ultimate decision of whether or not her personal information is to be used or not, in her hands.[444]

Notice and choice are popular data protection measures as they are more flexible, inexpensive to implement, and easier to enforce.[445] For instance, where the services offered by a data controller are very diverse; a regulator may not be able to analyse in-depth, the likelihood of harms it may cause to an individual. However, where the data controllerôs data policies are available through a notice, it performs the function of informing the individual, who can then determine for herself whether or not signing-up for the service is an acceptable trade-off for her personal information.

In India, several organisations have proactively taken privacy initiatives by adopting several global best practices in the matter of obtaining consent through privacy notices, even without a legal requirement to do so. However, when the concept of a privacy notice itself is in question, such steps will have to be reassessed. Particularly, in a country as vast as India, with large sections to the citizenry being unable to comprehend the contents of such notices, it would, at the very least, be necessary to take further steps to improve existing practices in this regard.

3.2 Issues

The concepts of notice and choice were first introduced at a time when computerised databases were just beginning to be used widely. There were only a few ways in which organisations could collect and use individualôs information. Data use and transfers had not become as ubiquitous as they are now. Therefore, although the use of the notice and choice

[443] Ryan M. Calo, óAgainst Notice Skepticism in Privacy (and Elsewhere)ô, 87(3) Notre Dame Law Review 1027, 1049 (2012), available at: http://scholarship.law.nd.edu/cgi/viewcontent.cgi?article=1020&context=ndlr, (last accessed 21 October 2017).
[444] Ryan M. Calo, óAgainst Notice Skepticism in Privacy (and Elsewhere)ô, 87(3) Notre Dame Law Review 1027, 1049 (2012), available at: http://scholarship.law.nd.edu/cgi/viewcontent.cgi?article=1020&context=ndlr, (last accessed 21 October 2017).
[445] Ryan M. Calo, óAgainst Notice Skepticism in Privacy (and Elsewhere)ô, 87(3) Notre Dame Law Review 1027, 1048 (2012), available at: http://scholarship.law.nd.edu/cgi/viewcontent.cgi?article=1020&context=ndlr, (last accessed 21 October 2017).

mechanism still continues to play a critical role in data protection, several issues have arisen over the years. These include:

(i) Notice complexity and difficulty in comprehension

The notice and choice mechanism is often criticised for leaving users uniformed (or misinformed) as people rarely see, read or understand privacy policies.[446] In several instances, data controllers serve privacy notices in order to demonstrate their compliance with existing data protection laws and serve as an indemnity against liability, rather than to genuinely inform users about their data practices. In such circumstances, the notice often takes the shape of very detailed and complicated documents, replete with legal jargon that is difficult for ordinary users to understand.[447] Therefore, understanding such notices presents certain cognitive problems that act as a hurdle to privacy-self management.

At the first instance, individuals may not even bother to read privacy notices.[448] When individuals do manage to read the privacy notices, they are often so complicated, that individuals may not be able to understand what is written in them. If individuals do manage to read and understand privacy notices, they may lack sufficient specialised knowledge relating to the manner in which their personal data will actually be used, which prevents them from making an informed choice. And finally, even if they do succeed in doing all the above, the individuals may lack the ability to adequately assess the consequences of agreeing to certain uses and disclosures of their personal information.[449] This leads to the problem of skewed decision making.[450]

(ii) Lack of Meaningful Choice

Most privacy notices inform individuals about the data practices of the data controller; however, they do not offer much in the way of a real choice to the users. Using a website or a mobile application is interpreted as having provided consent to the data controllerôs data practices. This is also the case in the context of data collected and processed by the government where, more often than not no notice is provided. If individuals wish to avail the services being offered, they do not have much choice beyond accepting the terms of the notice in its entirety. Some mobile applications and website developers do attempt to break

[446] Daniel Solove, óPrivacy Self-management and the Consent Dilemmaô, 126 Harvard Law Review 1880, 1885, (2013).
[447] Florian Schaub *et al*., óA Design Space for Effective Privacy Noticesô, USENIX Association, Symposium of Usable Privacy and Security (2015), available at: https://www.usenix.org/system/files/conference/soups2015/soups15-paper-schaub.pdf, (last accessed 22 October 2017).
[448] Fred H, Cate, óFailure of Fair Information Principlesô, in óConsumer Protection in the Age of Information Economyô, 343, 361-62, (Jane K. Winn *ed.*, Routledge, 2006) *citing* Helen Nissenbaum, óPrivacy in Context-Technology, Policy and the Integrity of Social Lifeô (Stanford University Press, 2010). (discussing a study that only about 20% people read privacy notices ñmost of the timeò).
[449] Daniel Solove, óPrivacy Self-management and the Consent Dilemmaô, 126 Harvard Law Review 1880, 1886, (2013).
[450] Daniel Solove, óPrivacy Self-management and the Consent Dilemmaô, 126 Harvard Law Review 1880, 1887, (2013).

down consent by providing individuals to opt-out of certain data use practices (such as receiving marketing communications or not permitting a particular use of their information), however, this is still relatively uncommon. Consent notices are usually an all-or-nothing package with no modulations ordinarily permitted.

(iii) Notice Fatigue

Some critics of the notice and choice mechanism claim that this system is impractical. There are too many notices to keep track of, considering that an ordinary user visits hundreds of websites in one day.[451] Expecting an individual to read all of these notices is likely to be an extremely time consuming exercise. An individual may be able to manage their privacy quite well if only a few entities are involved. However, this is usually not the case, and keeping track of all the notices encountered by an individual contributes to the individualôs burden.[452]

Additionally, as discussed in the section on consent, even if an individual is able to make a rational decision about sharing a particular piece of information at one time, she may not be able to predict how this information will be combined with other pieces of information in the future. This is an especially relevant problem with the advent of data mining and predictive analytics.[453]

(iv) Problems in Notice Design

Some scholars believe that the reason for the failure of an effective notice is due to problems in its design. Long and text-heavy notices may not be the most efficient means of conveying relevant information to individuals. In many instances, the notice is not designed keeping the intended audience in mind, which may be a regulator, or the consumer. Notices, which are designed keeping the regulator in mind, may prove difficult for an ordinary user to navigate.

Collection and use of an individualôs information is no longer limited to websites and mobile applications. A host of ñsmart devicesò, such as fitness trackers, video game systems and speakers collect userôs information on a continuous basis. Ordinarily, the privacy notices of such devices are decoupled from the device itself and are posted on the data controllerôs websites. This may not be the most effective way of informing the user of the devices data collection and use policies. Keeping the above in mind, there may be a need to develop better notice design or to question whether the use of notices is in fact the correct solution to the problem.

---

[451] *See generally*: Aleecia M. McDonald and Lorrie Cranor, ôThe Cost of Reading Privacy Policiesô, 4(3) I/S: A Journal of Law and Policy for the Information Society 544 (2008), available at: http://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf, (last accessed 22 October 2017).

[452] Joel R. Reidenberg *et al.*, ôPrivacy Harms and the Effectiveness of the Notice and Choice Frameworkô, 11(2) Journal of Law and Policy for the Information Society, 486, 492 (2015), available at: https://kb.osu.edu/dspace/bitstream/handle/1811/75473/ISJLP_V11N2_485.pdf?sequence=1, (last accessed 22 October 2017).

[453] Daniel Solove, ôPrivacy Self-management and the Consent Dilemmaô, 126 Harvard Law Review 1880, 1886, (2013).

3.3 International Practices

Despite certain flaws, the mechanism of notice and choice continue to be widely used across many jurisdictions. These jurisdictions have attempted to address some of these flaws through the practices described below:

European Union

The EU GDPR does not use the term ñnoticeò *per se.*[454] It provides that a data controller must demonstrate that the data subject has consented to the processing of her information.[455] This is done by ensuring that a ñrequest for consentò (which could be understood to mean a notice), is presented in a manner clearly distinguishable from other matters in a concise, intelligible and easily accessible form- using clear and plain language.[456] These provisions are intended to ensure that the notice conveys necessary information in an easily comprehensible manner, which is clear to the data subject. The EU GDPRôs notice requirements are prescriptive in nature, and contain details regarding the types of information, which must be provided to the data subject, including the identity of the data controller, purpose of processing, intended recipients of the data, among others. It attempts to make choice more meaningful by indicating when delivery of the notice will be most effective, and additional safeguards, which are to be followed when the information is not collected directly from the data subject.[457]

United Kingdom

UK DPA, provides that personal data must be processed fairly and lawfully.[458] The ICO has issued some guidelines as to what this means. Being transparent and providing accessible information to individuals about how their data will be used is critical. Transparency through a privacy notice is an important part of fair processing. The ICO recognises that individualsô expectations of privacy have changed and very often using a single notice to convey the necessary information will not be an effective approach to convey necessary information. It has provided samples of what a good privacy notice and a bad privacy notice would look like.[459] It recognises that use of innovative techniques, such as multi-layered notices are helpful in conveying relevant information to users in a clear and accessible manner. Where individuals have a choice, with respect to deciding whether their information can be used, the privacy notice should give individuals the opportunity to exercise that choice.[460]

---

[454] Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.
[455] Article 7(1), EU GDPR.
[456] Article 7(2), EU GDPR.
[457] Articles 12, 13 and 14, EU GDPR.
[458] Schedule I, Part I, Paragraph 1, UK DPA.
[459] ICO, ó Good and Bad Examples of Privacy Noticesô, available at: https://ico.org.uk/media/for-organisations/documents/1625136/good-and-bad-examples-of-privacy-notices.pdf, (last accessed 23 October 2017).
[460] ICO, ó Privacy Notices, Transparency and Controlô, available at: https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/, (last accessed 23 October 2017).

South Africa

The POPI Act provides very detailed prescriptions as to what information must included in the notice at the time of collection of personal data from the individual. It mandates that the data controller must take all steps which are reasonably practicable to ensure that all necessary information is provided to the individual, including the type of information being collected, the purpose for which information is being collected, to whom the information will be disclosed, and so on.[461]

Canada

PIPEDA provides that purposes for which personal information is collected must be identified by the collecting organisation at or before the time the information is collected. It goes on to say that the identified purposes should be specified either orally or in writing, at the time that the information is collected.[462] The Privacy Commissioner has issued certain guidelines for online consent, which require that organisations must be fully transparent about their privacy practices and disclose what information they are collecting, what it will be used for and with whom it will be shared.[463] The guidelines attempt to address difficulties relating to notice readability, comprehension and access, by providing that it must contain clear explanations, language at an appropriate reader level, informing users in advance if an organisation intends to change its data use, etc.

Australia

The APPs, which form part of the Privacy Act suggest that all entities must have a ñclearly expressed and up to dateò privacy policy regarding how personal information is managed by the entity. The policy should also specify what types of information the entity collects and holds, the purposes for which it is collected, and how this information will be used and disclosed. The privacy policy must also be available free of charge and in whatever form as may be considered appropriate.[464] Further, the APPs also require that any entity, which collects personal information about an individual, must take reasonable steps to notify the information about the information collected as soon as possible, and to ensure that the individual is aware that such information is being collected.[465]

United States

The privacy laws in the US are sector-specific. Several of these laws mandate the form and substance of what information a privacy notice must contain. For instance, in order to ensure easy accessibility of the notice, laws such as California Online Privacy Protection Act, 2003

[461] Section 18, POPI Act.
[462] Principle 2, Paragraph 4.2.3, PIPEDA.
[463] Office of the Privacy Commissioner of Canada, ó Guidelines for Online Consentô (May 2014), available at: https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_oc_201405/, (last accessed 23 October 2017).
[464] Paragraphs 1.3, 1.4 and 1.5, APP 1, Privacy Act.
[465] Paragraph 5.1 and 5.2, APP 5, Privacy Act.

(CALOPPA)[466] and the GLB Act require that websites and financial institution post ñclear and conspicuousò privacy notices. In order to ensure their visibility, and to draw user attention, the hyperlinks to the notices must be in a contrasting colour and font. To ensure that users understand the organisationsô data use practices, these legislations make it mandatory for the notice to contain certain types of information, such as the identity of the data controller, the categories of personal information collected, whether this information will be shared with third parties, and so on. The GLB Act goes one step further, through its Privacy Rule, provides samples of model notices, which organisations can rely while creating their own notices. The Privacy Rule further specifies the language, which must be used while preparing a notice, and warns against the use of unnecessarily complicated legal jargon.

From the above, it is clear that despite its flaws, notice and choice continue to play a central role in many data protection laws. Some jurisdictions have attempted to address issues relating to notice complexity and incomprehensibility by requiring that unnecessarily complicated language not be used. The data protection laws of some jurisdictions also prescribe requirements regarding the form and substance of a notice. Despite these measures, countries are still struggling with issues relating to flaws in notice design and notice fatigue. Codes of practice and guidelines issued by a data protection authority provide some clarity on how notice can be made more effective.

3.4 Provisional Views

1. Mandatory notice is a popular form of privacy self-management, which plays a role in most data protection laws. Notice is important as it operationalises consent.

2. The law may contain requirements regarding the form and substance of the notice.

3. The data protection authority could play an important role by issuing guidelines and codes of practice that could provide guidance to organisations on the best way to design notices, so that it conveys relevant information in the most effective manner to individuals. This may include giving advice on how to redesign notices, making them multi-layered and context specific, informing them of the importance that timing plays while providing notices, etc. This may be further bolstered by sectoral regulators as well.

4. Privacy Impact Assessment or other enforcement tools may take into account the effectiveness of notices issued by organisations.

5. In order to address issues relating to notice fatigue, assigning every organisation may be assigned a ñdata trust scoreò (similar to a credit score), based on their data use policy.

[466] California Online Privacy Protection Act, Education Foundation: Consumer Federation of California, available at: https://consumercal.org/about-cfc/cfc-education-foundation/california-online-privacy-protection-act-caloppa-3/, (last accessed 26 October 2017).

6. Similarly, having a ócconsent dashboardô could help individuals easily view which organisations have been provided with consent to process personal information and how that information has been used.

3.5 Questions

1. Should the law rely on the notice and choice mechanism for operationalising consent?

2. How can notices be made more comprehensible to individuals? Should government data controllers be obliged to post notices as to the manner in which they process personal data?

3. Should the effectiveness of notice be evaluated by incorporating mechanisms such as privacy impact assessments into the law?

4. Should the data protection law contain prescriptive provisions as to what information a privacy notice must contain and what it should look like?

   Alternatives:

   a. No form based requirement pertaining to a privacy notice should be prescribed by law.
   b. Form based requirements may be prescribed by sectoral regulators or by the data protection authority in consultation with sectoral regulators.

5. How can data controllers be incentivized to develop effective notices?

   Alternatives:

   a. Assigning a ódata trust scoreô.
   b. Providing limited safe harbor from enforcement if certain conditions are met.

   If a ódata trust scoreôis assigned, then who should be the body responsible for providing the score?

6. Would a consent dashboard be a feasible solution in order to allow individuals to easily gauge which data controllers have obtained their consent and where their personal data resides? Who would regulate the consent dashboard? Would it be maintained by a third party, or by a government entity?

7. Are there any other alternatives for making notice more effective, other than the ones considered above?

CHAPTER 4: OTHER GROUNDS OF PROCESSING

4.1 Introduction

Lawfulness of processing is a core principle under data protection law.[467] The OECD Guidelines recognise lawfulness of processing under the collection limitation principle, which provides that collection of personal data must be limited, and any such collection should be done only by lawful and fair means, and where appropriate, with the consent of the concerned individual.[468] Although consent forms the foundation of data protection law, it may not be sufficient to rely on consent for all processing activities. With regard to processing by the government, consent is rarely an option as data is required to be provided by law. Some jurisdictions have realised that there may be a need to carve out other grounds, under which processing activities can take place, irrespective of the consent of the individual, and still be considered lawful.[469] For instance, an employer may need to collect the personal data of its employees for processing pension payments. If such processing is routine, then obtaining consent prior to every such transaction would lead to multiplicity of notices and therefore, to consent fatigue. Identifying certain other grounds under which personal data could be lawfully processed would allow sufficient flexibility within the data protection law for such activities.

4.2 Issues

(i) Requirement to have additional grounds of processing, along with consent.

The importance of consent in legitimising data processing activities has been discussed in Part III, Chapter 1 of the White Paper, above. Over the years, several shortcomings in the consent model have been identified, including that of consent fatigue. Relying solely on consent may not be sufficient to accommodate the various types of data processing activities that take place on a day-to-day basis. In some situations, seeking consent prior to a data processing activity would not be possible, or it may defeat the purpose of the processing. For instance, where law enforcement officials need to apprehend a criminal, seeking the consent of the criminal prior to processing would defeat the purpose of the investigation. In other situations, the government may need to process the personal information of citizens in the performance of some of their legislative functions, and it may not be possible to seek consent.

---

[467] Article 5 and Recital 39, EU GDPR set out that any processing of personal information should be lawful and fair. It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data will be processed.

[468] OECD, ‘OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data’ (2013), available at: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (last accessed 31 October 2017).

[469] Article 29 Data Protection Working Party, ‘Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC’, European Commission (9 April 2014), available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf, (last accessed 28 October 2017).

Therefore, there may be a need to designate certain ñlawfulò grounds under which data can be processed, even in the absence of consent.

(ii) Lack of clarity with respect to certain grounds of processing, such as ñpublic interestò, ñvital interestò and ñlegitimate interestò.

Certain grounds of lawful processing, such as consent and performance of contract may be intuitively considered necessary for data processing. However, other grounds such as ñpublic interestò, ñvital interestò and ñlegitimate interestò, as lawful grounds of processing may not provide sufficient clarity as to what the intended scope of these grounds are. These grounds originated in the EU, and the Working Party opinion give some clarity as to how these grounds should be interpreted.[470] However, in the absence of interpretative guidelines, it may not be possible to import these grounds to the Indian context without some modification. Whether these six grounds of processing, as provided under the EU GDPR, are sufficient, or whether there is a need to include other grounds of processing, more suitable to the Indiaôs specific data processing activities may also need to be examined.

4.3 International Practices

European Union

The EU GDPR[471] provides that personal data may be lawfully processed based on the data subjectôs consent, or on the basis of five other grounds. These five grounds are: (i) performance of a contract with the data subject; (ii) compliance with a legal obligation imposed on the controller; (iii) protection of vital interests of the data subject; (iv) performance of a task carried out in the public interest; and (v) legitimate interests pursued by the controller, subject to an additional balancing test against the data subjectôs rights and interests.[472] A EU Working Party opinion clarifies that there does not appear to be any legal distinction among these grounds, and there is no indication that these grounds must be applied in any particular order, or that any one ground is more important than the other. [473]

Each of the five additional grounds of processing is described in detail below:

(i) Performance of Contract

[470] Article 29 Data Protection Working Party, ôOpinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/ECõ, European Commission (9 April 2014), available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf, (last accessed 28 October 2017).
[471] Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.
[472] Article 7(a)-(f), EU GDPR.
[473] Article 29 Data Protection Working Party, ôOpinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/ECõ, European Commission (9 April 2014), available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf, (last accessed 28 October 2017).

This ground covers two types of scenarios. First, where processing is necessary for the performance of a contract to which the data subject is a party. This is a strictly interpreted provision and does not cover situations where processing is not genuinely necessary for the performance of a contract, and is unilaterally imposed by the entity processing information. Therefore, a determination of the precise rationale of the contract, its substance and fundamental objective is essential.[474]

Second, this ground is also intended to cover any processing activity, which could take place prior to entering a contract. This includes pre-contractual relations, where the steps are taken at the initiative of the individual. For example, if an individual requests an insurance quote from a car-insurance company, the insurer would be justified in processing the individualôs personal data in order to provide this service.[475]

(ii) Legal Obligation

For this ground to be applicable, processing of personal information must be necessary for compliance with a legal obligation, or a mandatory requirement under law.[476] For instance, if a bank were required to report suspicious transactions under anti-money laundering laws, this situation would be covered under this ground.

(iii) Vital Interest

This ground may be used only in very limited circumstances, such as where there is a there is a threat to the life or health of the individual. The Recitals to the EU GDPR clarifies that this ground must only be used to protect an interest essential to the life of the individual.[477] However, there is no clarity on what constitutes a threat to life, whether the threat must be immediate, and what the scope of this ground should be.

(iv) Public interest task, or the exercise of official authority

The ground dealing with public interest covers two situations. First, where the entity collecting the information has official authority, and processing is essential for exercising this authority. Second, where the controller does not have the authority, but a third party who has

[474] Article 29 Data Protection Working Party, ôOpinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/ECõ, European Commission (9 April 2014), available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf, (last accessed 28 October 2017).
[475] Article 29 Data Protection Working Party, ôOpinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/ECõ, European Commission (9 April 2014), available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf, (last accessed 28 October 2017).
[476] Article 29 Data Protection Working Party, ôOpinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/ECõ, European Commission (9 April 2014), available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf, (last accessed 28 October 2017).
[477] Recital 31, EU GDPR.

the authority requests the disclosure.[478] For instance, an authorised public authority investigating a crime can request a bank to disclose information regarding suspicious financial transactions.

(v) Legitimate Interest

This last ground is intended to act as a residuary ground, for processing activities, which are not covered by any of the other grounds. This ground, as envisaged under the EU GDPR demands the carrying out of a balancing test between the legitimate interests of the data collecting entity and the interests or fundamental rights and freedoms of the data subject on the other. This balancing test is complex and involves weighing multiple factors. For instance, the data controller would have to examine the nature of the information being processed, the manner in which it may be processed, the reasonable expectations of the individual with respect to how the data may be processed and disclosed, and finally the balance of power between the individual and the data controller.[479]

United Kingdom

The UK DPA largely follows the EU GDPR approach, described above, except for the ñpublic interest groundò and the ñlegitimate interestò ground. As the EU GDPRôs ground on public interest does not provide much clarity on what intended function is, the UK DPA has divided the public interest ground into specific heads, such as processing which is necessary for the administration of justice; the exercise of the functions of the Parliament; exercise of functions by the Crown; and in the exercise of any function exercised in public interest.[480] The UK DPA also recognises that a data controller may have a legitimate reason to process information, which none of the other grounds cover.

South Africa

The POPI Act largely follows the UK DPAôs approach with respect to the grounds under which data may be processed.[481]

Canada

Under PIPEDA, consent is the primary basis for collecting data and does not recognise additional grounds of processing like the EU GDPR. However, the PIPEDA does recognise

[478] Article 29 Data Protection Working Party, ôOpinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/ECõ, European Commission (9 April 2014), available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf, (last accessed 28 October 2017).
[479] Article 29 Data Protection Working Party, ôOpinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/ECõ, European Commission (9 April 2014), available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf, (last accessed 28 October 2017).
[480] Schedule 2, UK DPA.
[481] Section 11 (1) (a)-(f), POPI Act.

that there may be certain situations where it may not be possible to obtain consent at the time of collecting information. These include diverse situations such as collection for the purpose of a legal investigation, where it is required for the purpose of an emergency, if it required for purposes of research, if it is necessary for the collection of a debt, etc.[482]

Australia

The Privacy Act relies on consent as the primary ground for collection, use and disclosure of personal information. The APPs provide that an entity covered under the Privacy Act, must only collect personal information which is ñreasonably necessaryò for one or more of the entityôs functions or activities. Determining whether a particular collection of personal information is permitted, involves a two-step process: identifying the entityôs functions or activities-different criteria apply for ascertaining functions and activities of organisations; determining whether the collection of personal information is reasonably necessary.[483]

United States

The US has a number of sector-specific legislations. By and large, data protection legislations in the US operate on the notice and choice model. Collection of information for any purpose is permitted, as long as the individual is informed by way of a clear and easily understandable notice, and is given the opportunity to opt-out of the processing activity, where required. For instance, under the GLB Act, a financial institution can disclose a customerôs information to a non-affiliated third party as long as they notify the consumer about this process and inform the consumer about their right to opt-out of such a disclosure.[484]

4.4 Provisional Views

1. Consent continues to play a very important role in data processing activities. It may not be possible to seek consent of the individual, prior to collection and use of her information in all circumstances, particularly when information is used for various purposes for which they might not have been originally intended. There may be a need to have certain legally recognised grounds to permit processing of personal data in these circumstances.

2. Grounds such as performance of contract; and necessity for compliance with law appear to be intuitively necessary, and have been adopted, as is, by jurisdictions.

3. Other grounds such as the public interest ground finds mention within the EU GDPR; however lack of specificity as to what it comprises, has led to countries such as the UK to modify it to fit the particular administrative, judicial and legislative requirements of each country. For instance, other grounds of processing could include collection of

[482] Sections 7(2), (3), (4) and (5), PIPEDA.
[483] APP 3.1 and 3.2, Privacy Act.
[484] GLB Act, 15 U.S.C. Section 6801-6827.

information in the event that it has been ordered by a court of law; where a public authority needs to collect data necessary to the exercise of the functions of the legislature, such as the drafting of new laws. Adaptations suitable for India will have to be explored.

4. There may also be a need of a ground which permits the collection of information in situations of emergency where it may not be possible to seek consent from the affected individual.

5. The ñlegitimate interestò ground under the EU GDPR appears to be subjective and difficult to enforce. It places a heavy burden on the data controller who must carry out the balancing test weighing its interests against that of the rights of the individual. Despite this, there may be a need to have a residuary ground under which processing activities could take place, as it is not possible for the law to foresee and provide for all situations, which may warrant the processing of information without seeking consent of the individual. This residuary ground would be intended for the benefot of the individual. As an alternative, the data protection authority could designate certain activities as lawful, and provide guidelines for the use of these grounds and the data controller would be permitted to collect information under these grounds.

4.5 Questions

1. What are your views on including other grounds under which processing may be done?

2. What grounds of processing are necessary other than consent?

3. Should the data protection authority determine residuary grounds of collection and their lawfulness on a case-by-case basis? On what basis shall such determination take place?

   Alternatives:

   a. No residuary grounds need to be provided.
   b. The data protection authority should lay down ólawful purposesô by means of a notification.
   c. On a case-by-case basis, applications may be made to the data protection authority for determining lawfulness.
   d. Determination of lawfulness may be done by the data controller subject to certain safeguards in the law.

4. Are there any alternative methods to be considered with respect to processing personal data without relying on consent?

CHAPTER 5: PURPOSE SPECIFICATION AND USE LIMITATION

5.1 Introduction

(i) Purpose Specification Principle

Purpose Specification is an essential first step in applying data protection laws and designing safeguards for the collection, use and disclosure of personal data.[485] The principle of purpose limitation is designed to establish the boundaries within which personal data collected for a given purpose may be processed and may be put to further use. As described in the OECD Guidelines[486], the principle has two components: the data must be collected for a specified purpose and once the data is collected, it must not be processed further in a manner which is incompatible with the purpose for collection. Each subsequent use must be specified at the time of change of purpose. For instance, if a clothing store collects an individualôs address for the purpose of delivering goods she has ordered, and later uses this information to send her promotional material, this would not be permitted; as such use is incompatible with the original purpose. This principle is closely linked to the Use Limitation principle (described below) and the Data Quality Principle (described in Part III, Chapter 7 of the White Paper). Specifying the purpose of collection and ensuring that further use is in line with the purpose of collection contributes to transparency, legal certainty and predictability in the data collection process. This principle also gives an individual control over her data by allowing her to set limits on how her personal information will be used. It also ensures that collection is lawful and fair, and prevents further use that may be unexpected, inappropriate or otherwise objectionable. [487]

(ii) The Use Limitation Principle

The Use Limitation principle provides that personal data should not be disclosed, made available or otherwise used for purposes other than those specified. It provides two exceptions where this does not apply, i.e. where the individual has permitted the use; and when such use or disclosure occurs with the authority of law. The intention of providing these two exceptions is to allow some level of flexibility of use within processing activities.[488] The underlying logic of the use limitation and purpose specification principles is that of data

[485] Article 29 Data Protection Working Party, ówOpinion 03/2013 on purpose limitationô, European Commission (2 April 2013) available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf, (last accessed 24 October 2017).
[486] OECD, ówOECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Dataô (2013), available at: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (last accessed 31 October 2017).
[487] Article 29 Data Protection Working Party, ówOpinion 03/2013 on purpose limitationô, European Commission (2 April 2013) available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf, (last accessed 24 October 2017).
[488] OECD, ówOECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Dataô (2013), available at: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (last accessed 31 October 2017).

minimisation, or the practice of limiting the collection of personal information to that which is necessary to accomplish a specified purpose.[489]

5.2 Issues

(i) Relevance of the Purpose Specification Principle in light of technological developments

The advent of newer technologies such as Big Data, data analytics and the Internet of Things may challenge the relevance of the purpose limitation principle, as it currently exists. Various applications of these technologies have demonstrated that many potentially valuable and innovative uses of data develop outside of the scope of the purpose specified at the time of data collection. Data may be repurposed and used in an entirely different manner, which has nothing to do with the original purpose.[490] Similarly, the Internet of Things functions by collecting and storing a large amount of data first, which is then analysed to translate into an immensely beneficial service the purpose of which was not even conceptualised at the time of collection.[491] However, it could be argued that even for such services, the purposes that the services may be put to could be envisaged and set out for the data subject to review. If the purposes get changed in the future, the data subject may be notified as and when such amendments are made.

(ii) Compatibility Assessment

Assessing whether a particular use of information is compatible with the original purpose is difficult. Data is often multi-functional and it may not be possible to definitively determine whether a particular use of data falls within a permitted purpose. On the other hand, if a more subjective compatibility test is prescribed, this would involve weighing factors such as the nexus between the original use and the current use; the context in which the information was collected, whether the use was reasonable; the nature of information collected and the impact of further processing. This may prove burdensome to the data controller, or to the data protection authority, depending on who must assess compatibility. This leads to another issue of who is responsible for determining compatibility.

(iii) Difficulty in specifying purpose in a simple manner

The purpose specification principle is intended to ensure that the purpose for which information is collected is clear and specific. In actual practice, personal data could be

[489] Bernard Marr, ôWhy Data Minimisation is an important concept in the age of Big Dataô, Forbes (16 March 2016), available at: https://www.forbes.com/sites/bernardmarr/2016/03/16/why-data-minimization-is-an-important-concept-in-the-age-of-big-data/#58dbc0aa1da4, (last accessed 24 October 2017).

[490] Omer Tene and Jules Polonetsky, ôBig Data for All: Privacy and User Control in the Age of Analyticsô, 11(5) Northwestern Journal of Technology and Intellectual Property 239 (2013), available at: http://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1191&context=njtip, (last accessed 24 October 2017).

[491] Office of the Privacy Commissioner of Canada, ôDiscussion Paper on Consent and Privacyô (May 2016), available at: https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2016/consent_201605/#heading-0-0-7, (last accessed 20 November 2017).

collected for more than one purpose, which are distinct but related in some degree. Privacy notices attempt to work around this difficulty by using terms such as ñimproving user experienceò, ñIT-security purposesò and so on. These are vaguely worded and the individual may not understand the exact purpose for which her information is being used. Companies may also use vague purposes deliberately to allow for the data to be put to significantly higher and varied uses than the data subject is likely to think of. On the other hand, providing a detailed description full of legal terms may prove counter-productive as it adds to the complexity of the notice, and makes it difficult for the individual to read and understand.[492]

5.3 International Practices

European Union

The principle of purpose specification as envisaged under the EU GDPR requires that the data controller must only collect data for specified, explicit and legitimate purposes, and once the data is collected, it must not be processed further in a manner that is incompatible with the original purpose. [493] It provides an exemption for further use, as long as it is for scientific, historical or statistical research purposes, as they are not considered to be incompatible purposes. The intention behind using terms such as ñspecified, explicit and limitedò is to ensure that the entity collecting the personal information carefully considers what purposes the information will be used for, and to avoid the excessive collection of information which may not be necessary, adequate or relevant for the purpose which is intended to be satisfied.[494] The EU GDPR does not separately provide for the use limitation principle; it is folded into the purpose specification principle.

United Kingdom

Under the UK DPA, personal data is allowed to be obtained only for one or more specified and lawful purposes and must not be further processed in any manner incompatible with that purpose. [495]Additionally, the UK DPA also provides that the personal data collected should be adequate, relevant and not excessive in relation to the purpose for which it is processed. The ICO guidelines provide that compatibility of subsequent use depends on whether the intended use can be considered lawful under the UK DPA. The purpose specification principle ensures that organisations are open about their reasons for obtaining personal data and that what they do with the information is in line with the reasonable expectations of the concerned individuals.

---

[492] Article 29 Data Protection Working Party, ópinion 03/2013 on purpose limitationô, European Commission (2 April 2013) available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf, (last accessed 24 October 2017).
[493] Article 29 Data Protection Working Party, ópinion 03/2013 on purpose limitationô, European Commission (2 April 2013) available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf, (last accessed 24 October 2017).
[494] Article 29 Data Protection Working Party, ópinion 03/2013 on purpose limitationô, European Commission (2 April 2013) available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf, (last accessed 24 October 2017).
[495] Paragraphs 2 and 3, Schedule 1, UK DPA.

South Africa

The POPI Act specifies that personal information must be collected for a specific, explicitly defined and lawful purpose related to the activity of the collecting party.[496] With respect to further processing of personal information, it must be compatible with the purposes for which it was collected. The test for compatibility would take into account factors such as the nature of the information collected, the consequences of the intended processing to the data subject, etc. This Act also specifies certain conditions under which further processing of information will not be considered incompatible.[497]

Australia

Under the Privacy Act, consent is not required for the collection of personal information. However, the collection of personal information must be *reasonably connected* to the activity of the collecting entity. The APPs provide that an entity under the Privacy Act can only use or disclose personal information for a purpose for which it was collected (known as the primary purpose), or for a secondary purpose if an exception applies. These exceptions include: (i) where the individual has consented to a secondary use[498]; (ii) the individual reasonably expects the entity to use or disclose her personal information for the secondary purpose, which must be related to the primary purpose[499]; (iii) if the secondary use/disclosure is required or authorised by law[500]; (iv) if there is a permitted general situation which exists in relation to the secondary use or disclosure, such as permitted situations relating to enforcement activities.[501]

The reasonableness test relies on whether a reasonable person who is properly informed, would expect such a use of personal data in the circumstances. This is a question of fact in each individual case and it is the responsibility of the entity to justify its conduct. For example, an employee of a company would reasonably expect it to use her bank account information in order to process salary payments.[502] However, she would not reasonably expect the company to disclose her salary statement to an advertising company.

The OAIC has recognised the incompatibility of purpose limitation and use specification with current developments in Big Data analytics, a consultation draft published in 2016 suggests that privacy impact assessments (described in the chapter on notice, above) be carried out to

[496] Section 13, POPI Act.
[497] Sections 14 and 15, POPI Act.
[498] APP 6.1(a), Privacy Act.
[499] APP 6.2 (a), Privacy Act.
[500] APP 6.2(b), Privacy Act.
[501] APPs 6.2(e) and 6.3, Privacy Act.
[502] OAIC, ôChapter 6: Australian Privacy Principle 6 ð Use or disclosure of personal informationõ (February 2014), available at: https://www.oaic.gov.au/resources/agencies-and-organisations/app-guidelines/chapter-6-app-guidelines-v1.pdf, (last accessed 23 October 2017).

enable data controllers to understand data flows within their system, understand potential data risks, and implementing safeguards which would mitigate those data risks.[503]

Canada

PIPEDA provides that an organisation may collect, use or disclose personal information only for purposes that a reasonable person would consider appropriate in the circumstances.[504] It also provides certain conditions under which an organisation may use an individualôs personal information without her knowledge or consent. These include: (i) if the organisation reasonably believes that the information is necessary in investigating a crime; (ii) if it is necessary to protect the health and safety of an individual; (iii) if the information was produced by the individual in the course of her employment and the use of this information is consistent with the purposes for which the information was produced[505]; (iv) if the information is used for research purposes, as long as the confidentiality of the information is protected.[506]

The Privacy Commissioner has also recognised that the purpose limitation and use specification principles may not be adequately equipped to address data collection and use issues with respect to Big Data and the Internet of Things. Their discussion paper concludes that a systemic approach to privacy protection must be explored, which may involve a range of policy, technical, regulatory and legal solutions.[507]

5.4 Provisional Views

1. The current regime of purpose specification and use limitation is designed to ensure that individuals retain control over the manner in which their personal data is collected, used and disclosed. This is a valuable objective.

2. Standards may have to be developed to provide guidance to data controllers about the meaning of data minimisation in the context of their data collection and use.

3. In light of recent developments in data flow practices and new technologies, data may be multi-functional and being required to specify each use in an exact manner within a privacy notice may prove to be burdensome. Using layered privacy notices, which provide hyperlinks to more information on data use practices, which can be accessed as

[503] OAIC, ôGuide to Big Data and the Australian Privacy Principles- Consultation Draftõ, 6-7 (May 2016), available at: https://www.oaic.gov.au/resources/engage-with-us/consultations/guide-to-big-data-and-the-australian-privacy-principles/consultation-draft-guide-to-big-data-and-the-australian-privacy-principles.pdf, (last accessed 23 October 2017).
[504] Division 1, Section 5(3), PIPEDA.
[505] Section 7(2)(b.2), PIPEDA.
[506] Section 7(2)(c), PIPEDA.
[507] Office of the Privacy Commissioner of Canada, ôDiscussion Paper on Consent and Privacyõ (May 2016), available at: https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2016/consent_201605/#heading-0-0-7, (last accessed 27 October 2017).

required, could mitigate this situation. Further, incompatible purposes, irrespective of how beneficial they may be to the user may not be permitted for further processing.

4. The use limitation principle may need to be modified on the basis of a contextual understanding of purposes and uses. This is captured by the reasonableness standard, i.e. a subsequent use is permitted as long as a reasonable individual could reasonably expect such use. This may be further developed by sectoral regulators.

5.5 Questions

1. What are your views on the relevance of purpose specification and use limitation principles?

2. How can the purpose specification and use limitation principles be modified to accommodate the advent of new technologies?

3. What is the test to determine whether a subsequent use of data is reasonably related to/ compatible with the initial purpose? Who is to make such determination?

4. What should the role of sectoral regulators be in the process of explicating standards for compliance with the law in relation to purpose specification and use limitation?

   Alternatives:

   a. The sectoral regulators may not be given any role and standards may be determined by the data protection authority.
   b. Additional/ higher standards may be prescribed by sectoral regulators over and above baseline standards prescribed by such data protection authority.
   c. No baseline standards will be prescribed by the authority; the determination of standards is to be left to sectoral regulators.

5. Are there any other considerations with respect to purpose specification and use limitation principles which have not been explored above?

CHAPTER 6: PROCESSING OF SENSITIVE PERSONAL DATA

6.1 Introduction

Data protection law deals with the protection of personal data of an individual. Personal data is understood as information relating to an identified or identifiable natural person. An identified person is one who can be identified directly or indirectly, with reference to one or more factors, which are specific to her physical, physiological, mental, economic, cultural or social identity.[508] Some of these identifying factors play an important role in forming an integral part of the individualôs personality and being. They refer to certain characteristics that define oneôs essence as a human being and contribute to the individualôs dignity, integrity, personal autonomy and independence.[509] These may include aspects such as individualôs religious beliefs and sexuality.

It may be intuitively understood that an individual would consider it important to protect information relating to such core aspects of her being from being used or disclosed in a manner likely to cause harm to her. In order to prevent harm, it may be necessary to categorise the types of information, which form an integral part of an individualôs identity. The harms arise, of course, because information of the individual becomes available to others through a wide range of activities, collectively termed ñdata processingò.[510] The aspect of informational privacy, which allows the individual to determine the manner and purpose their personal information should be used, becomes particularly important with respect to these types of information. For instance, in some circumstances, disclosure of such information, is more likely to lead to discrimination, ridicule and reputational harm, especially where oneôs beliefs and choices form part of the minority view in society. This in turn would cause greater harm to the person in the form of loss of dignity and personhood.[511] Disclosure of certain types of inflammatory and sensitive information, even where the information is true, could result in the stereotyping and pre-judging of persons, which may affect their ability to fully develop their personality.[512]

In order to guard against such harms, some jurisdictions recognise the necessity for certain pre-identified categories within the scope of personal data to grant individuals extra protection against misuse of these types of information, by prohibiting the collection, use and disclosure of this information without the explicit consent of the individual, or only for

[508] Article 4(1), EU GDPR.
[509] Edward J. Bloustein, ôPrivacy as an Aspect of Human Dignity- An Answer to Dean Prosserô, 36 New York University Law Review 962 (1964).
[510] Data Processing can be understood as ñany operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destructionò, Article 4(2), EU GDPR.
[511] Edward J. Bloustein, ôPrivacy as an Aspect of Human Dignity- An Answer to Dean Prosserô, 36 New York University Law Review 962 (1964).
[512] Robert C Post, ôThree Concepts of Privacyô 89 Texas Law Review 2087 (2001), *citing* Jeffrey Rosen, ôThe Unwanted Gaze: The Destruction of Privacy in Americaô (2000).

specific purposes and under special conditions.[513] Such types of data are termed ñsensitiveò, and may include religious beliefs, physical or mental health, sexual orientation, biometric and genetic data, racial or ethnic origin and health information.

6.2 Issues

(i) Definition of ñsensitive dataò as per the Sensitive Personal Data Rules

The SPDI Rules, framed under Section 43A of the IT Act place certain obligations on individuals holding data in electronic form. The SPDI Rules seek to introduce internationally accepted privacy principles, such as collection limitation, purpose specification, use limitation and consent in the handling of ñsensitive personal informationò.[514] However, it may not be possible to rely entirely on this definition from the perspective of possibility of abuse and misuse.[515] Information relating to caste and religious beliefs of an individual would also need to be examined, as they are especially relevant to the Indian context. There are other issues relating to the scope of the SPDI Rules as they only applied to ñbody corporatesò and not to other private and government entities, which may process sensitive personal data.

(ii) Need to further examine the rationale behind certain categories of personal data

As discussed, certain types of information have been identified as sensitive because there is a greater likelihood of harm caused to the individual if there is unauthorised collection, use and disclosure of this information. In order to understand the rationale behind identifying certain categories of information as sensitive, there may be a need to assess the harms, which are likely to arise. In understanding harms, two categories are evident: intrinsic harms- for instance, the harms caused by the disclosure of health information may be intrinsic, as a user may not want her health information to be widely shared. Other harms are instrumental- e.g. Sharing medical records could lead to discrimination, utilisation of this information by pharmaceutical companies to send unwanted marketing information to these individuals etc. On the other hand, payment instrument details are sensitive not necessarily because any intrinsic harm is caused by disclosure of say, a credit card number, but rather because damage

[513] Article 29 Data Protection Working Party, óAdvice paper on special categories of data (ñsensitive dataò)ô, European Commission (4 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 29 October 2017).

[514] Rule 3, SPDI Rules defines ósensitive personal data or informationô to include: password; financial information such as bank account or credit card or debit card or other payment instrument details; physical, physiological and mental health condition; sexual orientation; medical records and history; biometric information; any detail relating to the above provided to the organisation for providing service; and any of the information received under the above by the organisation for processing, stored or processed under lawful contract or otherwise.

[515] Bhairav Acharya, óComments on the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011ô, The Center for Internet & Society (CIS) (31 March 2013), available at: https://cis-india.org/internet-governance/blog/comments-on-the-it-reasonable-security-practices-and-procedures-and-sensitive-personal-data-or-information-rules-2011, (last accessed 29 October 2017).

may instrumentally be caused if the data is not adequately secured is significant. Understanding which categories of data be considered sensitive is a critical task.

(iii) Difficulty in determining the context of use which could make data sensitive

Although it may be possible to identify certain types of information, the processing of which is more likely to cause harm to an individual; very often this is dependent not only on the nature of the individual, but also on the context in which it is used. For instance, there may be certain types of information, which are not classified under the law, but it could become sensitive because of its potential impact on individuals if this data is compromised in any manner. This could include unique identification numbers, passport numbers, and computer passwords. The sensitivity of the data could also develop based on its combination with other types of information. For example, an email address taken in isolation, is not sensitive. However, if it is combined with a password, then it could become sensitive as it opens access to many other websites and systems, which may expose the individual to harms such as cyber-attacks and phishing frauds.[516] It is also possible that personal or even non-personal data, when processed using big data analytics could be transformed into sensitive personal data. Therefore, there may be a need to create safeguards which will prevent misuse of personal information in these contexts of use.

6.3 International Practices

European Union

The EU GDPR[517] provides separate rules for processing of ñspecial categories of dataò, which are listed as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data, biometric data, or data relating to the health, sex life and sexual orientation of an individual. The EU GDPR provides that in general, processing of such information is prohibited, except with the explicit consent of the data subject and where processing is permitted in certain specified situations as identified within the law.[518]

United Kingdom

Under UK DPA, ñsensitive personal dataò includes those types of information identified in the EU GDPR. It also includes information relating to the commission of an offence and proceedings relating to an offence.[519] The ICO guidelines recognise that information relating

[516] Lokke Moerel, ówGDPR Conundrums: Processing Special Categories of Dataô, IAPP (12 September 2016), available at: https://iapp.org/news/a/gdpr-conundrums-processing-special-categories-of-data/#, (last accessed 30 October 2017).
[517] Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.
[518] Articles 9 (1) and 9(2)(a)-(j), EU GDPR.
[519] Section 2, UK DPA.

to these matters could be used in a discriminatory way, and is likely to be of a private nature, there is a need to treat them with a greater degree of care than other personal data.[520]

South Africa

The POPI Act prohibits the processing of ñspecial categoriesò of personal data. The definition of sensitive personal information under POPI Act is the same as that under the UK DPA. Processing of such information is prohibited unless the data controller obtains the consent of the individual, or if the processing is carried out on the basis of one of the permitted grounds of processing, which are very similar to those within the UK DPA.[521]

Australia

The Privacy Act has defined largely the same categories of personal information as ñsensitiveò as those under the EU GDPR and the UK DPA.[522] Sensitive information may be used or disclosed only if the individual has consented to the use and it is directly related to the primary purpose of collection.[523]Australia follows a unique system in that it recognises certain categories of information such as health information as particularly sensitive and contains provisions on how it may be processed within the Privacy Act. For instance, the Privacy Act provides for the creation of certain legally binding guidelines for researchers handling health information for research purposes.[524] This is something that the Indian data protection law could also consider. With respect to the inclusion of financial information in the categorisation of sensitive information (as has been done by the SPDI Rules), the Australian Law Reform Commission (ALRC) has opined that though there are certain aspects of it which can be considered sensitive, it may not be advisable to equate it with other categories of information which form an intrinsic part of the identity of an individual. [525] The Privacy Act does however, recognise that certain aspects of financial information such as credit history could be seen as prejudicial and should only be disclosed in appropriate circumstances.

Canada

---

[520] ICO, ó*Key Definitions of the Data Protection Act*ô, available at: https://ico.org.uk/for-organisations/guide-to-data-protection/key-definitions/, (last accessed 29 October 2017).

[521] Sections 26 and 27, POPI Act.

[522] As per Section 6, Privacy Act, sensitive information means: information or an opinion about an individualôs- (i) racial or ethnic origin; political opinions; membership of a political association; religious beliefs or affiliates; membership of a trade union; sexual orientation or practices; criminal record. Sensitive information also includes: health information about an individual; genetic information about an individual; biometric information that is to be used for the purposes of verification; and biometric templates.

[523] Paragraph 6.2, APP 6, Privacy Act.

[524] Guidelines under Section 95, Privacy Act, which set out procedures that Human Research Ethics Committees (HREC) must follow when personal information is disclosed for research purposes and Guidelines under Section 95A, Privacy Act, which provide a framework for HRECs to assess proposals to handle health information held by organisations for health research.

[525] Australian Law Reform Commission, ó*6. The Privacy Act: Some Important Definitions: Sensitive Information*ô, available at: https://www.alrc.gov.au/publications/6.%20The%20Privacy%20Act%3A%20Some%20Important%20Definitions/sensitive-information#_ftnref107, (last accessed 30 October 2017).

PIPEDA does not specifically deal with sensitive information. It provides that the form of consent sought by organisations may vary depending on the circumstances of use and the type of information. An organisation would have to seek express consent, when the information is likely to be considered sensitive. For instance, medical records and income records are almost always considered to be sensitive. Any information could be considered sensitive based on the context in which it is used.[526] For instance, collecting names of individuals for magazine subscriptions will not be problematic. However, releasing a list of names of individuals who subscribe to a special-interest magazine may be problematic, as it could lead to identification and discrimination against those individuals. This method of handling sensitive information could be problematic as it shifts the burden on the organisation to determine whether a particular use would cause harm, and this analysis would vary on a case-to-case basis.

United States

Although there is no broad definition of what constitutes ñsensitive dataò in the US, several sector-specific laws and guidelines implement safeguards where it may be considered necessary. For instance the FTCôs Behavioural Advertising Principles[527] suggest that website operators should obtain the express affirmative consent of the consumer before using sensitive consumer data, which may include financial data, data relating to children, health information, and precise geographic information.[528] The Fair Credit Reporting Act limits how consumer reports and credit card account numbers can be used and disclosed, although it does not term them as ñsensitiveò.[529] HIPAA regulates medical information and how it may be collected and disclosed. [530] The Security Standards for the Protection of Electronic Health Information (HIPAA Security Rule) provides standards for protecting medical data. For instance, there are specific rules, which regulate the disclosure of psychotherapy notes, even for the purpose of medical treatment.[531]

Therefore, largely the approach of most jurisdictions is to identify and carve out categories and types of information, which are considered sensitive. These categories of information are then protected by certain safeguards, which limit their collection, use and disclosure, in order to mitigate harm to the individual.

6.4 Provisional Views

[526] Schedule 1, Section 4.3.4, Principle 3- Consent, PIPEDA.
[527] FTC , ôFTC Staff Report: Self-Regulatory Principles for Online Behavioural Advertisingô (February 2009), available at: https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf, (last accessed 30 October 2017).
[528] FTC , ôFTC Staff Revises Online Behavioural Advertising Principlesô (12 February 2009), available at: https://www.ftc.gov/news-events/press-releases/2009/02/ftc-staff-revises-online-behavioral-advertising-principles, (last accessed 30 October 2017).
[529] 15 USC Section 1681.
[530] 42 USC Section 1301.
[531] HIPAA Privacy Rule.

1. It is recognised that the processing of certain types of personal data has a greater likelihood of causing harm to the individual, due to the inherent nature of the information.

2. The existing categories of information defined as ñsensitiveò under the SPDI Rules may be re-examined to determine whether those categories are sufficient or need to be modified. These categories need to be examined keeping in mind Indiaôs unique socio-economic context, where individuals have faced discrimination and harm due to various reasons currently not captured in the definition.

3. There may be a need to provide heightened grounds of protection for the processing of such types of data.

6.5 Questions

1. What are your views on how the processing of sensitive personal data should be done?

2. Given that countries within the EU have chosen specific categories of ñsensitive personal dataò, keeping in mind their unique socio-economic requirements, what categories of information should be included in Indiaôs data protection law in this category?

3. What additional safeguards should exist to prevent unlawful processing of sensitive personal data?

   Alternatives:

   a. Processing should be prohibited subject to narrow exceptions.
   b. Processing should be permitted on grounds which are narrower than grounds for processing all personal data.
   c. No general safeguards need to be prescribed. Such safeguards may be incorporated depending on context of collection, use and disclosure and possible harms that might ensue.
   d. No specific safeguards need to be prescribed but more stringent punishments can be provided for in case of harm caused by processing of sensitive personal information.

4. Should there be a provision within the law to have sector specific protections for sensitive data, such as a set of rules for handling health and medical information, another for handling financial information and so on to allow contextual determination of sensitivity?

5. Are there any alternative views on this which have not been discussed above?

CHAPTER 7: STORAGE LIMITATION AND DATA QUALITY

7.1 Introduction

(i) Storage Limitation

As discussed in Part III, Chapter 5 of the White Paper, the principle of purpose specification requires that the purpose for which data is being collected must be specified at the time of collection, and subsequent use of such data must ordinarily be limited to such purpose(s). Adherence to this principle is necessary to ensure that the processing of data is lawful. A closely connected principle is that of storage limitation. This principle requires that data must be retained by an organisation only for the time period that is reasonably necessary to fulfill the purpose for which it was collected. Thus, when data no longer serves a purpose, it may be necessary, if practicable, to have it erased or anonymised.[532]

(ii) Data Quality

The related principle of data quality is an obligation on data controllers to create, maintain, use or disseminate personal data in such a manner as to ensure the reliability of such data for its intended use.[533] The OECD Guidelines stipulates that ñPersonal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.ò[534] Such an obligation exists since processing of incorrect or inaccurate data can have detrimental consequences for the concerned individual, such as denial of services like loans, credit etc. Data quality is also closely linked with individual participation rights (discussed in Part III, Chapters 8, 9 and 10 of the White Paper) since an individual can, by accessing oneôs data, require the organisation to correct it in case it is inaccurate.

7.2 Issues

(i) Implementation

The principle of storage limitation requires an organisation to store personal data only for a time period that is ñreasonably necessaryò for the purpose for which it was collected. The use of a subjective term such as ñreasonably necessaryò may affect implementation since it will be difficult to impose a tangible obligation on the organisation. For instance, an organisation

[532] OECD, óOECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Dataô (2013), available at: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (last accessed 31 October 2017).

[533] CIPP Guide, óThe HEW Report: Defining the Fair Information Practicesô, available at: https://www.cippguide.org/2012/08/23/the-hew-report-defining-the-fair-information-practices/, (last accessed 26 October 2017).

[534] OECD, óOECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Dataô (2013), available at: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (last accessed 31 October 2017).

may continue to retain data for long periods of time on vague grounds such as ñimproving user experienceò etc. On the other hand, an approach like section 67-C of the IT Act may not be feasible either. Section 67-C requires intermediaries to preserve and retain information only for such duration as prescribed by the Central Government. Different categories of personal data may be required to be preserved for different periods of time. For instance, under the IMC Code, medical information can be preserved for three years from the date of commencement of treatment.[535] The Government will be burdened with the task of prescribing different retention guidelines for different categories of data, and may not end up performing this task satisfactorily. Similarly, the principle of data quality requires reasonable steps to be taken to ensure accuracy of data. Here again, imprecision may result in implementation challenges.

Further, for an organisation that holds large volumes of data across different formats, adhering to an obligation to ensure accuracy of data may prove to be challenging. This may have the unintended consequence of shifting the onus on to the individual to ensure her data is accurate, which is not ideal, given the limited awareness and exercise of individual participation rights. This also holds for the storage limitation principle, which will require organisations to regularly review data in their possession and methodically cleanse their databases[536] thus increasing the compliance burden.

(ii) Modern technology and processing

As mentioned earlier, modern technology and big data analytics have revolutionised how data is collected and used. Thus, the potential use of data may not be determinable at the time of collection.[537] In this light, principles such as data retention may not be implementable since one cannot store data for a specific time period since new purposes may be discovered post collection of such data thereby requiring the organisation to hold onto the data indefinitely. In this context the focus may need to shift to data security as well as alternative obligations such as ensuring anonymization of data which in most circumstances should adequately achieve the objectives of big data analytics that do not, by definition, require personal data.

7.3 International Practices

(i) Storage Limitation

European Union

The EU GDPR does not allow personal data to be stored in a form that permits the identification of individuals for a period longer than required unless such data is processed

[535] Regulation 1.3, IMC Code.
[536] Karin Tien *et al.,* ôThe data protection principles under the General Data Protection Regulationõ, Taylor Wessing (November 2016), accessed at: https://united-kingdom.taylorwessing.com/globaldatahub/article-the-data-protection-principles-under-the-gdpr.html, (last accessed 5 November 2017).
[537] Jordi Soria-Comas and Josep Domingo-Ferrer, ôBig Data Privacy: Challenges to Privacy Principles and Modelsõ, 1(1) Data Science and Engineering (March 2016), available at: https://link.springer.com/article/10.1007/s41019-015-0001-x (last accessed 31 October 2017).

solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.[538]

United Kingdom

Under the UK DPA data processed for a purpose should not be kept longer than is required for such purpose.[539]

Canada

Under PIPEDA, personal information that is no longer required to fulfill the identified purpose must be destroyed, erased, or made anonymous.[540] Further, organisations are required to develop guidelines and implement procedures for the destruction of data.[541]

Australia

Under the Privacy Act, an organisation is required to take reasonable steps to destroy or de-identify information that is no longer required for any purpose.[542] There are exceptions to this principle, namely, the information is contained in a Commonwealth record or the entity is required under law or an order of Court/Tribunal to retain the information.[543] This is seen as an application of the security principle.

South Africa

Under the POPI Act, data must not be retained for any longer than necessary for achieving the purpose for which it was collected.[544] However, there are certain exceptions to this, namely, if retention is required by law, or by contract between the parties, etc.[545] Further, retention of personal data is permissible for historical, statistical and research purposes, and the organisation should adopt appropriate safeguards against the data being used for other purposes.[546]

(ii) Data Quality

European Union

[538] Article 5(1)(e), EU GDPR.
[539] Principle 4, Part 1, Schedule 1, UK DPA.
[540] Principle 5, PIPEDA.
[541] Principle 5, PIPEDA.
[542] Principle 11.2, Schedule 1, Privacy Act.
[543] Principle 11.2, Schedule 1, Privacy Act.
[544] Section 14, POPI Act.
[545] Section 14, POPI Act.
[546] Section 14(2), POPI Act.

The EU GDPR prescribes that data must be accurate and where necessary kept up to date. Further, organisations must take every reasonable step to ensure, in light of the purpose for which they are processed, inaccurate data are erased or rectified.[547]

United Kingdom

Under the UK DPA, personal data is required to be accurate and where necessary, kept upto date.[548]

Canada

Under PIPEDA, the principle of accuracy requires that data be accurate, complete and up-to-date as is necessary for the purposes for which it is used.[549] However, the principle specifies that an organisation shall not routinely update personal information, unless it is necessary for the purpose for which it was collected.[550]

Australia

Under the Privacy Act, an organisation is required to take steps which are reasonable in the circumstances to ensure that the personal data it collects is accurate, up-to date and complete. Such as obligation also exists at the stage of use and disclosure.[551]

South Africa

In South Africa an organisation needs to take reasonably practicable steps to ensure personal information is complete, accurate, not misleading and updated where necessary.[552] While ensuring accuracy of data, the organisation must have regard for the purpose for which the data is to be processed.[553]

7.4 Provisional views

1. *Storage Limitation:* The principle of storage limitation is reflected in most data protection laws and may consequently also find place in a data protection law for India. Further, it may not be feasible to prescribe precise time limits for storage of data since the purpose of processing will determine the same. However, the use of terms ñreasonably necessary/necessaryò may be employed and thereafter guidelines issued by the regulator, industry practices, interpretation by courts can bring clarity when it comes to implementation.

[547] Article 5(1)(d), EU GDPR.
[548] Principle 4, Part 1, Schedule 1, UK DPA.
[549] Principle 6, Schedule 1, PIPEDA.
[550] Principle 6, Schedule 1, PIPEDA.
[551] APP 10, Schedule 1, Privacy Act.
[552] Section 16(1), POPI Act.
[553] Section 16(2), POPI Act.

2. *Data Quality:* The principle of data quality is reflected in most data protection laws and consequently may be incorporated in a data protection law. Further, such a provision ought to achieve a balance between the burden imposed on industry and the requirement for accuracy. Again, the employment of terms ñreasonably necessaryò may be employed to achieve this purpose.

7.5 Questions

1. What are your views on the principles of storage limitation and data quality?

2. On whom should the primary onus of ensuring accuracy of data lie especially when consent is the basis of collection?

   Alternatives:

   a. The individual
   b. The entity collecting the data

3. How long should an organisation be permitted to store personal data? What happens upon completion of such time period?

   Alternatives:

   a. Data should be completely erased
   b. Data may be retained in anonymised form

4. If there are alternatives to a one-size-fits-all model of regulation (same rules applying to all types of entities and data being collected by them) what might those alternatives be?

5. Are there any other views relating to the concpets of storage limitation and data quality which have not been considered above?

CHAPTER 8: INDIVIDUAL PARTICIPATION RIGHTS-1

***Rights**: Right to Confirmation, Right to Access, and Right to Rectification*

8.1 Introduction

One of the core principles of data privacy law is the ñindividual participation principleò which stipulates that the ñprocessing of personal data must be transparent to, and capable of being influenced by, the data subjectò.[554] This principle manifests itself in the form of individual participation rights, which lie at the heart of data protection legislation[555] and allow an individual to participate in, and influence the manner in which, their personal data is used by data controllers and other individuals.[556] In addition to consent, they are the most direct means to provide an individual control over her personal data and are regarded as one of the most important privacy protection safeguards.[557]

(i) Origin

Individual participation forms three out of five FIPPS, which is deemed to be the bedrock of data privacy laws.[558] They are:[559]

a. There must be a way for an individual to find out what information about him is in a record and how it is used.
b. There must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent.
c. There must be a way for an individual to correct or amend a record of identifiable information about him.

Subsequently the OECD Guidelines[560] which were significantly influenced by the FIPPS translated the individual participation principle into concrete rights.[561] Further, a perusal of

---

[554] Lee Andrew Bygrave, óData Privacy Law: An International Perspectiveô 2 (Oxford University Press, 2014).
[555] Ministry of Justice, UK, óImpact Assessment of Proposal for an EU Data Protection Regulationô (22 November 2012), available at: https://consult.justice.gov.uk/digital-communications/data-protection-proposals-cfe/results/eu-data-protection-reg-impact-assessment.pdf , (last accessed 21 October 2017).
[556] Ministry of Justice, UK, óImpact Assessment of Proposal for an EU Data Protection Regulationô (22 November 2012), available at: https://consult.justice.gov.uk/digital-communications/data-protection-proposals-cfe/results/eu-data-protection-reg-impact-assessment.pdf , (last accessed 21 October 2017).
[557] OECD, óOECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Dataô (2013), available at: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (last accessed 31 October 2017).
[558] Paul M. Schwartz, óPrivacy and Democracy in the Cyber Spaceô, 52 Vanderbilt Law Review 1609 (1999).
[559] CIPP Guide, óThe HEW Report: Defining the Fair Information Practicesô, available at: https://www.cippguide.org/2012/08/23/the-hew-report-defining-the-fair-information-practices/, (last accessed 26 October 2017).
[560] OECD, óOECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Dataô (2013), available at: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (last accessed 31 October 2017).

data protection laws across jurisdictions also shows that there are three rights which form the core of individual participation.[562] They are as follows:

a. The right to seek confirmation about whether oneôs personal data is being processed.
b. The right to access oneôs personal data, including details such as[563]: The purpose of processing; the categories of data being processed; the period of storage; the rights vis-a-vis the organisation; the right to lodge a complaint; the source from where the data was collected, if it is not the individual; in case of automated decision making, the logic involved behind such decision and its consequences.
c. The right to challenge the accuracy of oneôs personal data, and to have it amended.

Thus, the right of an individual to gain access to their personal data has historically been a core requirement of data protection laws. This right allows an individual to determine if data held about them is correct and is being handled lawfully. It also opens the door to exercise of further rights, such as getting inaccurate data corrected.[564]

8.2 Issues

(i) Costly implementation

The implementation of individual participation rights are costly for data controllers. Some data protection laws[565] permit data controllers to impose a fee for responding to individual requests. However, these fees are negligible. It has been estimated that the cost for responding to individual requests varies anywhere between GBP 50-100 per request (though some stakeholders from the financial sector have estimated the cost to range between GBP 550-650 per request) in the UK.[566] Under the EU GDPR individual participation rights are exercisable free of cost. There is concern that the abolition of fees will lead to an increase in frivolous and

---

[561] OECD, óOECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Dataô (2013), available at: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (last accessed 31 October 2017). The relevant individual participation rights contained herein include:
(a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
(b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him;
(c) to be given reasons if a request made under subparagraphs(a) and (b) is denied, and to be able to challenge such denial; and
(d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

[562] Sally Annereau, óAn Introduction to Subject Access Rightsô, Taylor Wessing (November 2013), available at: https://united-kingdom.taylorwessing.com/globaldatahub/article_intro_sar.html, (last accessed 22 October 2017).

[563] Illustrative list from Section 7, UK DPA.

[564] Sally Annereau, óAn Introduction to Subject Access Rightsô, Taylor Wessing (November 2013), available at: https://united-kingdom.taylorwessing.com/globaldatahub/article_intro_sar.html, (last accessed 22 October 2017).

[565] The UK DPA and The Dutch Personal Data Protection Act.

[566] Ministry of Justice, UK, óImpact Assessment of Proposal for an EU Data Protection Regulationô (22 November 2012), available at: https://consult.justice.gov.uk/digital-communications/data-protection-proposals-cfe/results/eu-data-protection-reg-impact-assessment.pdf , (last accessed 21 October 2017).

vexatious requests thus putting a strain on resources.[567] The increased compliance cost may prove to be particularly difficult for small and medium organisations to bear.

(ii) Technical Challenges

Another challenge facing the implementation of individual participation rights pertains to data controllers holding large volumes of data in unstructured formats such as emails. Data controllers not only hold large volumes of electronic data but they also hold them in a number of different formats and often a mixture of different types of data.[568] For instance, an organisation may have a billion emails which may contain information on a number of different topics and individuals.[569] As a consequence, extracting information about a specific individual from such a large and complex mass of data is challenging. Similarly government bodies may hold vast stores of data that relate to a variety of inter-related functions. The same may be true for some organisations which derive personal information from non personal data trails. In such situations, responding to a broad individual access request for ñallò personal data pertaining to an individual can be extremely difficult.[570]

(iii) Logic behind automated decisions

The right to access in most EU jurisdictions includes the right to access the logic behind automated decisions. Automated decision making has come under tremendous scrutiny since it involves algorithm based decisions without any human intervention. A research paper by Alan Turing Institute and the University of Oxford argues that meaningful implementation of this particular right is not feasible since the information required to be communicated to the individual who exercises this right is likely to be heavily limited by factors such as trade secrets and interests of the processing organisations.[571] As a result, a person turned down for a credit card might only be told that the algorithm took their credit history, age and postcode into account, while not specifying why their application was rejected, i.e. the logic behind automated processing.[572]

---

[567] Kingston Smith Consulting, ôThe Right to be Forgotten and the problems with Unstructured Dataõ (20 May 2014), available at: https://www.kingstonsmith.co.uk/wp-content/uploads/2016/04/SubjectAccessRequests.pdf (last accessed 22 October 2017).

[568] Kingston Smith Consulting, ôThe Right to be Forgotten and the problems with Unstructured Dataõ (20 May 2014), available at: https://www.kingstonsmith.co.uk/wp-content/uploads/2016/04/SubjectAccessRequests.pdf (last accessed 22 October 2017).

[569] Kingston Smith Consulting, ôThe Right to be Forgotten and the problems with Unstructured Dataõ (20 May 2014), available at: https://www.kingstonsmith.co.uk/wp-content/uploads/2016/04/SubjectAccessRequests.pdf (last accessed 22 October 2017).

[570] Kingston Smith Consulting, ôThe Right to be Forgotten and the problems with Unstructured Dataõ (20 May 2014), available at: https://www.kingstonsmith.co.uk/wp-content/uploads/2016/04/SubjectAccessRequests.pdf (last accessed 22 October 2017).

[571] Sandra Wachter *et al.*, ôWhy a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulationõ, 7(2) International Data Privacy Law 76 (1 May 2017), available at: https://academic.oup.com/idpl/article/7/2/76/3860948 (last accessed 18 November 2017).

[572] Ian Sample, ôAI watchdog needed to regulate automated decision-making say expertsõ, The Guardian, (27 January 2017) available at: https://www.theguardian.com/technology/2017/jan/27/ai-artificial-intelligence-watchdog-needed-to-prevent-discriminatory-automated-decisions, (last accessed 22 October 2017).

The requirement to be provided the logic behind an automated decision derives from the early days of automation when such logic was easily available. Today, black box algorithms are designed so that they are completely inscrutable to humans. It is not possible, as a matter of design, for the logic behind these algorithms to be exposed. Under these circumstances simply requiring the logic for the decision may not be a suitable response to the challenge of automated decision making. Accordingly individuals need different forms of protection against the harms that could arise out of automated decision making. India needs to ensure that a legally tenable and feasible right find place in its data protection law.

(iv) Limited exercise of rights

Individuals are often unable to gauge the impact of the collection and use of their personal data on their privacy and autonomy, thus leading to ignorance on their part of their rights under data protection laws.[573] Further, it has been observed that relevant case-laws in European member countries on individual participation rights are hard to find thus furthering the belief that these rights are possibly not commonly exercised by individuals in some countries.[574] The low level of engagement with courts could point to the lack of awareness of informational rights amongst data subjects, ñparticularly regarding potential redress mechanisms such as courts, coupled with low levels of expertise regarding data protection matters on behalf of criminal justice professionals extending as far as judgesò.[575] Others also argue that meaningful exercise of these rights require an individual to know where to look, know that such a right exists in the first place, ascertain whom to ask for, etc. and also for an organisation to seriously consider these requests and respond.[576] This is a challenge India is very likely to face given the low exposure of its citizens to issues of data protection.

8.3 International Practices

European Union

Under the EU GDPR an individual has the right to receive information concerning the identity and contact of the data controller, the purpose of processing as well as the legal basis of such processing, and information concerning the existence of the other rights of the data

[573] Lee A. Bygrave and Dag Wiese Schartum, ó Consent, Proportionality and Collective Power, Reinventing Data Protection?ô, 4, (Springer Link, 2009).
[574] Antonella Galetta *et al.*, ôMapping the Legal and Administrative Frameworks of Access Rights in Europe ï A Cross-European Comparative Analysisô 34 Law Governance and Technology (2017), available at: http://irissproject.eu/wp-content/uploads/2014/06/IRISS-WP5-Summary-Meta-Analyses-for-Press-Release.pdf, (last accessed 22 October 2017).
[575] Antonella Galetta *et al.*, ôMapping the Legal and Administrative Frameworks of Access Rights in Europe ï A Cross-European Comparative Analysisô 34 Law Governance and Technology (2017), available at: http://irissproject.eu/wp-content/uploads/2014/06/IRISS-WP5-Summary-Meta-Analyses-for-Press-Release.pdf ,(last accessed 22 October 2017).
[576] B.J. Koops, ôThe Trouble with European Data Protection Lawô, 4(4) International Data Privacy Law, (1 November 2014), available at: http://www.isaca.org/Groups/Professional-English/privacy-data-protection/GroupDocuments/2014-08-24%20%20The%20Trouble%20with%20European%20Data%20Protection%20Law.pdf ,(last accessed 22 October 2017).

subject in relation to the data controller.[577] Further, an individual has the right to access her personal data which includes the right to confirm whether her personal data is being processed or not, and in the event that it is, information concerning the purpose of processing, the categories of personal data being processed, the recipients of such personal data, the period of storage of personal data, meaningful information about the logic behind automated decisions amongst others.[578] Additionally, an individual has the right to seek rectification of her data, subject to certain grounds and exceptions.[579]

United Kingdom

Under the UK DPA an individual has the right to access personal data which includes the right to be informed about whether oneôs personal data is being processed, and in the event it is, the description of such personal data, the purpose of processing and the recipients to whom such data may be disclosed.[580] Also, where processing was based on automatic means for the purpose of taking evaluative decisions about the individual which may significantly affect her, then the logic behind such decision must be made available.[581] Further, in the event that her personal data is inaccurate, an individual has the right to approach the appropriate court for an order which directs the data controller to rectify, block, erase or destroy those data.[582] However, these rights are subject to exceptions.

Canada

The principle of individual access is contained in Schedule 1[583] of PIPEDA. The principle of individual access allows an individual, upon request, to be informed of the existence, use and disclosure of her personal information.[584] Further, an individual can challenge the accuracy and completeness of her information and have it amended.[585] However, there can be exceptions to individual access. These exceptions have to be limited and specific and can include situations such as the disclosure of such information is prohibitively costly, amongst others.[586]

Australia

Under the Privacy Act, an individual has the right to access personal information held by an organisation. However, such right is not absolute and is subject to exceptions. If the organisation is a government body then disclosure can be refused under the Freedom of

[577] Article 13, EU GDPR.
[578] Article 15, EU GDPR.
[579] Article 16, EU GDPR.
[580] Section 7, UK DPA.
[581] Section 7(1)(d), UK DPA.
[582] Section 14, UK DPA.
[583] Schedule 1 of the PIPEDA houses the ñNational Standard of Canada Entitled Model Code for Protection of Personal Informationô.
[584] 4.9, Principle 9, Schedule 1, PIPEDA.
[585] 4.9, Principle 9, Schedule 1, PIPEDA.
[586] 4.9, Principle 9, Schedule 1, PIPEDA.

Information Act, 1982 or other appropriate laws/enactments.[587] If the organisation is a private body then access can be refused on certain grounds, such as: belief that access would pose a serious threat to the life, health or safety of any individual, or to public health or public safety or that such access would have an unreasonable impact on the privacy of other, amongst others.[588] Further in the event that the personal information held by the organisation is inaccurate, not up-to-date, incomplete, irrelevant or misleading, then the individual has the right to make a request to such entity to correct her personal data.[589]

South Africa

Under the POPI Act an individual has the right to confirm if information about her is being held by an organisation, and obtain a record of the information as well as identities of third parties who have access to such information.[590] Access to information can be refused on multiple grounds which are housed in another Act namely the Promotion of Access to Information Act, 2000. Further the grounds for refusal of access are different for private and public bodies.[591] Further, an individual can get an organisation to correct or delete data that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or is obtained unlawfully corrected/deleted.[592] This also includes the right to get data which the organisation is no longer authorised to retain destroyed/deleted.[593]

8.4 Provisional Views

1. The right to seek confirmation, access and rectify personal data allow an individual control over data once such data has been collected by another entity. These rights may be suitably incorporated. However these rights are harder to enforce in the context of personal information that has been derived from the habits and observed behaviour of the individual and other such inferred insights. This information is nevertheless personal and an individual should be made aware of the fact that the data controller has this sort of information.

2. Given that responding to individual participation rights can be costly for organisations, and comes with its set of technical challenges, a reasonable fee may be imposed on individuals when exercising these rights. This will also discourage frivolous and vexatious requests. The fees may be determined via sector specific subsidiary legislation or regulations. An illustration of this is the CIC Act under which the charge for accessing a copy of a personôs credit information report by a specified user is laid down by the RBI via regulations.

[587] Principle 12.2, Part 5 of Schedule 1, Privacy Act.
[588] Principle 12.3, Part 5 of Schedule 1, Privacy Act.
[589] Principle 13.1, Part 5 of Schedule 1, Privacy Act.
[590] Section 23, POPI Act.
[591] Section 23(4)(a), POPI Act.
[592] Section 24(1)(a), POPI Act.
[593] Section 24(1)(b), POPI Act.

3. Reasonable exceptions to the right to access and rectification exist in all jurisdictions. Such exceptions must also be carved out to ensure that organisations are not overburdened by requests which are not feasible to respond to.

8.5 Questions

1. What are your views in relation to the above?

2. Should there be a restriction on the categories of information that an individual should be entitled to when exercising their right to access?

3. What should be the scope of the right to rectification? Should it only extend to having inaccurate date rectified or should it include the right to move court to get an order to rectify, block, erase or destroy inaccurate data as is the case with the UK?

4. Should there be a fee imposed on exercising the right to access and rectify oneôs personal data?

   Alternatives:

   a. There should be no fee imposed.
   b. The data controller should be allowed to impose a reasonable fee.
   c. The data protection authority/sectoral regulators may prescribe a reasonable fee.

5. Should there be a fixed time period within which organisations must respond to such requests? If so, what should these be?

6. Is guaranteeing a right to access the logic behind automated decisions technically feasible? How should India approach this issue given the challenges associated with it?

7. What should be the exceptions to individual participation rights?

   [For instance, in the UK, a right to access can be refused if compliance with such a request will be impossible or involve a disproportionate effort. In case of South Africa and Australia, the exceptions vary depending on whether the organisation is a private body or a public body.]

8. Are there any other views on this, which have not been considered above?

CHAPTER 9: INDIVIDUAL PARTICIPATION RIGHTS-2

Rights: *Right to Object to Processing, Right to Object to processing for purpose of Direct Marketing, Right to not be subject to a decision based solely on automated processing, Right to Data Portability, and, Right to restrict processing.*

9.1 Introduction

In addition to confirmation, access and rectification, certain other individual participation rights have been recognised.[594] While their recognition is primarily in the EU and countries which follow a similar model for regulation, the rationale for their inclusion in this paper is to demonstrate current thinking around the remit of participation rights and assess their justification and suitability for India. These rights are:

(i) The right to object to processing

The essence of the right to object to processing is that even when personal data is being processed on lawful grounds, the competing rights and interests of the individual may trump those of the data controller. An individual has the right to object to processing, on grounds relating to her particular circumstance[595], when such processing is carried out either in exercise of official authority or in public interest, or on the ground of legitimate interest.[596] Further, the data controller must stop processing of such data unless it is able to demonstrate that it has a compelling legitimate interest which overrides the interests, rights and freedoms of the individual, or processing serves the establishment, the exercise or defence of its legal rights.

(ii) The right to object to processing for the purpose of direct marketing

Direct marketing is any advertising or marketing communication that is directed to particular individuals.[597] Direct marketers generally compile personal data about individuals such as contact details from multiple sources, including publicly available sources.[598] Thus an individual may not, in all circumstances, have consented to the processing of their personal data for direct marketing.

Processing of personal data for the purpose of direct marketing has garnered significant attention across jurisdictions thus warranting a specific provision for its regulation in data

[594] These are the right to object to processing generally and for direct marketing, to not be subject to a decision based solely on automated processing,

[595] Illustrations of particular circumstances include an individualôs family circumstances or professional interests in confidentiality. *See* Paul Voight and Axel Von Dem Bussche, ôThe EU General Data Protection Regulation (GDPR): A Practical Guideô (Springer, 2017).

[596] These grounds of processing have been explained in Part III, Chapter 4 of this White Paper.

[597] Thomas Reuters Practical Law, ôDirect marketing: a quick guideô available at: https://goo.gl/nZz15o , (last accessed 24 October 2017).

[598] Australian Law Reform Commission, ôDirect Marketing: Introductionô, available at: https://www.alrc.gov.au/publications/26.%20Direct%20Marketing/introduction, (last accessed 24 October 2017).

protection laws. This is because there has been a strong push from consumers and consumer advocates to regulate direct marketing strictly, particularly unsolicited direct marketing.[599] This takes from the conceptualisation of privacy as ñthe right to be let aloneò.[600] Under EU law, an individual has the right to object to the processing of her data for direct marketing, and upon such objection, the processing must be stopped.

(iii) Right to not to be subject to a decision based solely on automated processing

A report by the Alan Turing Institute in London and the University of Oxford indicates that outcomes based on algorithmic automated decisions without any human intervention may be flawed or discriminatory because the data samples are too small or based upon incorrect or incomplete assumptions or statistics.[601] For instance, a veteran American Airline pilot had been detained on 80 occasions after an algorithm confused him for an IRA leader.[602] Further, as a consequence of erroneous automated processing, individuals have lost their jobs, had their car licenses revoked, and have been removed from electoral registers.[603]

Recognising the potential harms associated with automated decision making, the EU grants an individual the right to not be subject to a decision based solely on automated processing.[604] However, this right is qualified since one has a right to object to only those automated decisions which produce legal effects or significantly affect the individual.[605]

(iv) Right to Restrict Processing

The right to restrict processing serves as a temporary relief available to an individual when the data is inaccurate or when the legitimate basis for processing cannot be immediately proven.[606] It is exercisable when[607]:

a. the accuracy of the data is contested - for the period the organisation can verify the accuracy of the data,

---

[599] Australian Law Reform Commission, ódirect Marketing: Current Coverage by IPPs and NPPsô available at: https://www.alrc.gov.au/publications/26.%20Direct%20Marketing/current-coverage-ipps-and-npps, (last accessed 24 October 2017).
[600] Australian Law Reform Commission, ódirect Marketing: Current Coverage by IPPs and NPPsô available at: https://www.alrc.gov.au/publications/26.%20Direct%20Marketing/current-coverage-ipps-and-npps, (last accessed 24 October 2017).
[601] Lexis Nexis, óShould we rely on automated decision making technologies?ô (15 February 2017), available at: https://www.bristows.com/assets/pdf/Should%20we%20rely%20on%20automated%20decision%20making%20technologies.pdf, (last accessed 24 October 2017).
[602] Ian Sample, óAI watchdog needed to regulate automated decision-making say expertsô, The Guardian, (27 January 2017) available at: https://www.theguardian.com/technology/2017/jan/27/ai-artificial-intelligence-watchdog-needed-to-prevent-discriminatory-automated-decisions, (last accessed 22 October 2017).
[603] Ian Sample, óAI watchdog needed to regulate automated decision-making say expertsô, The Guardian, (27 January 2017) available at: https://www.theguardian.com/technology/2017/jan/27/ai-artificial-intelligence-watchdog-needed-to-prevent-discriminatory-automated-decisions, (last accessed 22 October 2017).
[604] Article 22, EU GDPR.
[605] Article 22(1), EU GDPR.
[606] Laura Vegh, óErasure, Restriction and Objection ï Rights - Part 3ô, EU GDPR Compliant (5 July 2017), available at: https://eugdprcompliant.com/erasure-restriction-objection/, (last accessed 24 October 2017).
[607] Article 18, EU GDPR.

b. the processing is unlawful and the individual opposes the erasure of such data,
c. the organisation no longer needs the personal data for the purposes of the processing, but they are required by the individual for the establishment, exercise or defence of legal claims,
d. the individual has exercised her right to object to processing - for the time period the organisation determines whether its legitimate interests trumps those of the individual.

(v) Right to Data Portability

The right to data portability empowers individuals regarding their personal data as it facilitates their ability to move, copy or transmit personal data easily from one IT environment to another.[608] For example, by exercising this right an individual should be able to transfer her playlist from one music streaming service to another. In the context of medical data and financial information, this would empower the individual by serving as a protection against that individual being locked into a service. Limited data portability has already been allowed in the context of the telecom industry where individuals are allowed to port their number from one service provider to another. This concept could be more broadly applied across all sectors in which personal data of the individual is stored with data controllers to ensure that the individual is given control over her own data.

There are two rights guaranteed by the right to data portability: the right to receive the personal data provided by the individual to the organisation in a commonly used machine-readable format, and the right to transmit personal data from one organisation to another, where technically feasible. Further this right is only exercisable when the ground for processing the data is either consent or the performance of a contract, and when processing is carried out via automated means.[609]

9.2 Issues

(i) Costly implementation

The newly introduced rights such as those of data portability and the right to erasure are expected to be particularly expensive for organisations to implement.[610] For instance, after the Google Spain ruling on the right to be forgotten, Google received thousands of removal requests (91,000 in three months) and had to set up a team of people to review each application individually.[611] Similarly, data portability requires an organisation to modify

[608] Article 29 Data Protection Working Party, ‘Guidelines on the Right to Data Portability’, European Commission (13 December 2016), available at: http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_en_40852.pdf, (last accessed 24 October 2017).
[609] Article 20(1)(a), EU GDPR.
[610] Ministry of Justice, UK, ‘Impact Assessment of Proposal for an EU Data Protection Regulation’ (22 November 2012), available at: https://consult.justice.gov.uk/digital-communications/data-protection-proposals-cfe/results/eu-data-protection-reg-impact-assessment.pdf , (last accessed 21 October 2017).
[611] Samuel Gibbs, ‘Google to extend ‘Right to be Forgotten’ to all its domains accessed in EU, The Guardian (11 February 2016), available at: https://www.theguardian.com/technology/2016/feb/11/google-extend-right-to-be-forgotten-googlecom, (last accessed 21 November 2017); David Drummond, ‘We need to talk about the right to

existing technology in order to be able to provide data subjects with their personal data in a machine readable format.[612] The feasibility of these rights will have to be carefully measured in light of the above concerns.

(ii) Inchoate nature of rights

A lack of understanding about the provisions of the EU GDPR continues to persist across business. For instance, the contours of the right to data portability continues to remain vague. Under the right to data portability, the data must be provided by an individual to the organisation. The scope of the term ñprovided byò is still unsettled. The Article 29 Working Party Opinion accords a broad interpretation to ñprovided byò as including[613]:

a. Data provided actively and knowingly by the individual; and
b. Observed data which is provided by the individual by the virtue of the use of service or device.

However, the European Commission has expressed concerns over this broad interpretation since it goes beyond intended legislative scope,[614] thus heightening the confusion around this right. The same concern is present in relation to the right to not to be subject solely to automated decision-taking, its contours and exceptions.

Finally, since the new individual participation rights introduced by the EU GDPR have not been implemented in any jurisdiction, there is no precedent available for India when it comes to translating these principles into concrete statutory provisions. That said, the principle of placing the individual in control of her data is at the core of Indiaôs digital philosophy and the fact that there is no prior experience elsewhere in the world should not come in the way of preparing a *sui generis* legislative framework to reflect this principle.

(iii) Unsuitability for India

Rights such as the right to object to processing can only be exercised when the ground for processing is in exercise of official authority or in public interest, or legitimate interest of the organisation. These two grounds of processing are particularly unique to the EU, and thus

---

be forgottenô, The Guardian (10 July 2014), available at: https://www.theguardian.com/commentisfree/2014/jul/10/right-to-be-forgotten-european-ruling-google-debate, (last accessed 24 October 2017).

[612] Ministry of Justice, UK, óImpact Assessment of Proposal for an EU Data Protection Regulationô (22 November 2012), available at: https://consult.justice.gov.uk/digital-communications/data-protection-proposals-cfe/results/eu-data-protection-reg-impact-assessment.pdf , (last accessed 21 October 2017).

[613] Article 29 Data Protection Working Party, óGuidelines on the Right to Data Portabilityô, European Commission (13 December 2016), available at: http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_en_40852.pdf, (last accessed 24 October 2017).

[614] William RM Long and Thomas Fearon, óWP29 Adopts Final GDPR Guidelines on Data Portabilityô, Sidley Austin LLP (12 May 2017), available at: https://www.lexology.com/library/detail.aspx?g=0c8b6a0a-97eb-42ae-b69c-17e971182f36, (last accessed 21 November 2017).

such a right may be unsuitable in the Indian context unless similar grounds for processing are deemed suitable for India (see Part III, Chapter 4 of this White Paper).

(iv) Overlap with sector-specific regulations

Data protection laws of several jurisdictions have special provisions for ódirect marketingô which at times, supplement special laws for dealing with spam or telemarketers. For instance, in the EU, the Privacy and Electronic Communication Directive 2002 deals with questions of unsolicited communication. Similarly, in Australia in addition to provisions on direct marketing in the Privacy Act, [615] there exists sector specific laws such as the Spam Act, 2003 and the Do Not Call Register Act, 2006. In Canada on the other hand, there is no specific provision on direct marketing in the PIPEDA and it can be presumed that direct marketing takes place on the ground of consent and consequently an individual can withdraw consent. Canada however has an Anti-Spam Legislation 2014 that prohibits businesses from sending ñcommercial electronic messagesò to an individual without her consent.[616] In India, the TRAI Regulations deals with unsolicited commercial communications. However, it is limited to messages and other communication through phones, and would not cover an email application or advertisements appearing on browsers. In light of this, a call needs to be taken about whether direct marketing should be treated as a discrete privacy principle in India or addressed via sector specific regulations.

(v) Automated Decision Making

Provisions regarding automated decision making are missing vital safeguards. For instance, an individual can only object to automated decisions which are processed solely by automated means and which have ñlegal or other significant effectsò. Such requirements significantly limit the scope of the right since any human involvement in a decision-making process could mean it is not óautomated decision-makingô.[617] Similarly, issues could arise *vis-a-vis* the terms like ñlegal or significant effectsò since their scope continues to be unsettled.[618] That said, it should be kept in mind that such provisions must keep pace with technological developments.

9.3 International Practices

The above discussed rights are particularly unique to the EU. Thus, they are reflected only in EU jurisdictions or jurisdictions broadly following the EU model such as South Africa. Further, the right to restrict processing, the right to data portability and the right to be

[615] Principle 7, Schedule 1, Privacy Act.
[616] Section 6, The Electronic Commerce Protection Act.
[617] Sandra Wachter *et al.*, ôWhy a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulationô, 7(2) International Data Privacy Law 76 (1 May 2017), available at: https://academic.oup.com/idpl/article/7/2/76/3860948 (last accessed 18 November 2017).
[618] Sandra Wachter *et al.*, ôWhy a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulationô, 7(2) International Data Privacy Law 76 (1 May 2017), available at: https://academic.oup.com/idpl/article/7/2/76/3860948 (last accessed 18 November 2017).

forgotten have not translated into law. Only specific examples of best practices that require particular consideration in addition to the EU GDPR are dealt with below.

United Kingdom

Under the UK DPA the right to object to processing exists where such processing was in pursuance of public interest or legitimate interest (distilled to suit the UK context) and in cases where such processing has caused or is likely to cause substantial damage or substantial distress to individuals, which is not warranted.[619] The Information Commissioner has set out in guidance, notes on what damage or distress could mean: substantial damage would be financial loss or physical harm; and substantial distress would be a level of upset, or emotional or mental pain, that goes beyond annoyance or irritation, strong dislike, or a feeling that the processing is morally abhorrent.[620] The UK DPA also incorporates the right to object to processing for direct marketing similar to as already described.[621]

The right in relation to automated decision making arises if two conditions are satisfied: first, the personal data must be processed using solely automated means, and second, such processing must significantly affect the concerned individual. Further, there are three rights guaranteed to an individual: first, the right to prevent automated decisions from taking place, second, the right to be informed when automated decisions are taken about the individual, and third, the right to object to an automated decision and ask for such decision to be reconsidered or taken on a different basis. Finally, certain decisions are exempt from the exercise of such right. If a decision is authorised or required by legislation, or is taken in preparation for, or in relation to, a contract with the individual concerned, and is to grant a request to the individual, or steps have been taken to safeguard the legitimate interests of the individual, it is exempted.[622]

Netherlands

The Dutch Personal Data Protection Act guarantees an absolute right to object to processing, if the ground for such processing is public interest or legitimate interest.[623] Further unlike the UK, the individual does not have to demonstrate that such processing has resulted in or is likely to result in substantial damage or distress. The right to object to processing for direct marketing in the Netherlands not only extends to commercial information but also to canvassing for charitable purposes.[624]

Finally, the Dutch Personal Data Protection Act goes one step ahead of the UK and prohibits any evaluative decision which produces legal effects or significantly affects an individual,

[619] Section 10, UK DPA.
[620] ICO, ôPreventing processing likely to cause damage or distressô available at: https://ico.org.uk/for-organisations/guide-to-data-protection/principle-6-rights/damage-or-distress, (last accessed 5 November 2017).
[621] Section 11, UK DPA.
[622] Section 12, UK DPA.
[623] Article 40, The Dutch Personal Data Protection Act.
[624] Article 41, The Dutch Personal Data Protection Act.

from being taken solely on the basis of automated processing of data.[625] The exemptions are similar to those under the UK DPA.

South Africa

The POPI Act guarantees the right to object to processing, on reasonable grounds, if the basis of processing was: protection of legitimate interest of the individual, proper performance of public law duty by a public body, or, pursuit of legitimate interest of the organisation.[626] The exception to the right is that such processing was permitted by legislation. [627]

Under the POPI Act processing for direct marketing is permissible only if the individual has consented to the same. Further, the individual has a right to opt-out of such processing.[628] Finally, the right in relation to automated processing is similar to that guaranteed under the Dutch Personal Data Protection Act.[629]

9.4 Provisional Views

1. It is important to include concepts of data portability into Indian privacy jurisprudence in order to ensure that the data subject is placed in a central position and has full power over her own personal data.Accordingly, every individual should have the right to demand that all personal data about that individual that is in the control of the data controller be made available to her in a universally machine readable format or ported to another service provide with the specific consent of that individual. All data must therefore be held in an interoperable format.

2. A general right to object to processing may not prove to be suitable for India. This is because, as explained in the section on other grounds of processing in this note, public interest and legitimate interest may not be imported as grounds for processing in a data protection law for India.

3. Automated decisions have proven to have detrimental consequences in many cases. This right is also found across most EU data protection regimes. However, given the concerns raised about automated decisions and their pervasiveness in the digital economy, a practically enforceable and effective right may be carved out.

4. Processing of personal data for direct marketing purposes may be recognised as a discrete privacy principle in a data protection law for India. This is because despite there being independent legislations regulating direct marketing, direct marketing is medium and technology-agnostic and consequently needs to be governed by general rules.

[625] Article 42, The Dutch Personal Data Protection Act.
[626] Section 11(3)(a), POPI Act.
[627] Section 11(3)(a), POPI Act.
[628] Section 69, POPI Act
[629] Section 71, POPI Act.

9.5 Questions

1. What are your views on the above individual participation rights?

2. The EU GDPR introduces the right to restrict processing and the right to data portability. If India were to adopt these rights, what should be their scope?

3. Should there be a prohibition on evaluative decisions taken on the basis of automated decisions ?

   Alternatives:
   a. There should be a right to object to automated decisions as is the case with the UK.
   b. There should a prohibition on evaluative decisions based on automated decision making.

4. Given the concerns related to automated decision making, including the feasibility of the right envisioned under the EU GDPR, how should India approach this issue in the law?

5. Should direct marketing be a discrete privacy principle, or should it be addressed via sector specific regulations?

6. Are there any alternative views which have not been considered?

CHAPTER 10: INDIVIDUAL PARTICIPATION RIGHTS 3- RIGHT TO BE FORGOTTEN

10.1 Introduction

The right to be forgotten in the digital sphere refers to the right of individuals to request data controllers to erase any data about them from their systems.[630] The principal driver behind the idea of the right to be forgotten is the massive expansion in the availability and accessibility of information associated with the digital world of the Internet.[631]

It is quite common for Internet users to reveal personal information they later regret,[632] or to have information posted about them that they wished had remained secret.[633] Information posted on the Internet is never truly forgotten. Once personal data enters the online ecosystem, the original purpose behind disclosure becomes irrelevant.[634] When allowed to flow freely, data is open to interpretation and use (or misuse) completely divorced from their original context.[635] Often, the very fact of certain information being online may itself cause considerable embarrassment and loss of reputation for an individual. For example, in *the Google Spain Case,*[636] an old article concerning an attachment and garnishment action against a Spanish individual (that was later resolved) was the first link when anyone ran an online search of this individualôs name which allegedly resulted in his loss of reputation.

The Indian judiciary through the Karnataka High Court in *Sri Vasunathan v. The Registrar General*[637] has recognised the right to be forgotten and safeguarded the same in sensitive cases involving women in general and highly sensitive cases involving rape or affecting the modesty and reputation of the person concerned, in particular. Further, the importance of a right to be forgotten was further emphasised by the Supreme Court in *Puttaswamy*.[638] The

---

[630] Viktor Mayer-Schonberger, ôDelete: The virtue of forgetting in the digital ageô (Princeton University Press, 2011).

[631] Frank La Rue, ôReport of the Human Rights Councilôs Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expressionô, 19, (A/HRC/17/27) (16 May 2011), available at: http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf, (last accessed 28 October 2017).

[632] *Snyder v. Millersville University* No. 07-1660, (2008) WL 5093140; *See* Yang Wang *et al*., ôI regretted the minute I pressed share: A Qualitative Study of Regrets on Facebookô, Symposium on Usable Privacy and Security, Pittsburgh, (July 20ï22, 2011), available at: http://citeseerx.ist.psu.edu/viewdoc/download?rep=rep1&type=pdf&doi=10.1.1.207.8881, (last accessed 28 October 2017).

[633] *Balsley v. LFP, Inc* No. 1:08 CV 491, (2011) WL 1298i80.

[634] *See* Charles J. Sykes, ôThe End of Privacyô 221 (1999, Macmillan); Jonathan Zittrain, ôThe Future of the Internet-and How to Stop Itô (Yale University Press, 2008); Jeffrey Rosen, ôThe Web Means the End of Forgettingô, New York Times Magazine (21 July 2010), available at: http://www.nytimes.com/2010/07/25/magazine/25privacy-t2.html?pagewanted=all, (last accessed 25 October 2017).

[635] James Boyle, ôShamans, Software, and Spleens: Law and the Construction of the Information Societyô (Harvard University Press, 1996); Helen Nissenbaum, ôPrivacy in Context-Technology, Policy, and the Integrity of Social Lifeô, 36, (Stanford University Press, 2010).

[636] *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.

[637] *Sri Vasunathan v. The Registrar General*, 2017 SCC OnLine Kar 424.

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

Supreme Court opined that, ñ*the impact of the digital age results in information on the Internet being permanent. Moreover, any endeavour to remove information from the Internet may not result in its absolute obliteration. It is thus, said that in the digital world preservation is the norm and forgetting a struggle.*[639] *People are not static; they are entitled to re-invent themselves and correct their past actions. It is privacy which nurtures this ability and removes the shackles of unadvisable things which may have been done in the past.*ò[640]

Therefore, the recognition of the right to privacy envisages within its contours the right to protect personal information on the Internet. Consequently, from this right, it follows, that any individual may have the derivative right to remove the óshackles of unadvisable past thingsôon the Internet and correct past actions.

10.2 Issues

While there is an obvious need for the possibility to erase damaging data, this right should not amount to rewriting history. It is essential that this right is balanced against other fundamental rights like the freedom of expression or freedom of the press. Additionally, it is necessary to clarify which parties are required to act when the erasure of data is being requested.

(i) Conflict with freedom of speech

In a widely cited blog post, Peter Fleischer, chief privacy counsel of Google, noted that the right to be forgotten, as discussed in Europe, often covers three separate categories, each of which proposes progressively greater threats to free speech.[641]

a. ñIf I post something online, do I have the right to delete it?ò
b. ñIf I post something, and someone else copies it and re-posts it on their own site, do I have the right to delete it?ò
c. ñIf someone else posts something about me, do I have a right to delete it?ò

Therefore, the issue at hand is to what extent can the right to be forgotten be compatible with the right to freedom of speech and expression ï whether it will cover only category one, or will it cover both category one and two, or will it cover all three categories.

According to the EU GDPR, when someone demands the erasure of personal data, an Internet Service Provider ñshall have the obligation to erase personal data without undue delayò, unless the retention of the data is necessary for exercising ñthe right of freedom of expression.ò[642] In another section, the regulation creates an exemption from the duty to

[639] *Justice K.S. Puttaswamy (Retd.)& Anr. v. Union of India & Ors.,* (2017) 10 SCALE 1 at Paragraph 65; *See,* Ravi Antani, óThe Resistance of memory: Could the European Unionôs Right to be Forgotten exist in the United States?ô 30 Berkeley Tech Law Journal 1173 (2015), available at: http://scholarship.law.berkeley.edu/btlj/vol30/iss4/20/, (last accessed 21 October 2017).
[640] *Justice K.S. Puttaswamy (Retd.)& Anr. v. Union of India & Ors.,* (2017) 10 SCALE 1.
[641] Jeffrey Rosen, óThe Right to be Forgottenô64 Stanford Law Review 90 (February 2012).
[642] Article 17, EU GDPR.

remove data for ñthe processing of personal data for journalistic purposes, or for the purposes of academic, artistic or literary expression.ò[643]

However, the exact scope and contours of such a right to be forgotten will only be clearly visible after the EU GDPR comes into force in 2018.

(ii) Compliance of Third Parties

While formulating a right to be forgotten, it is essential to outline whether third party providers of informationð eg: search enginesð can be held accountable for failing to comply with erasure requests.

This issue was addressed in the *Google Spain Case.*[644]In this case, the issue before the Court of Justice of the EU (CJEU) concerned an order from Spainôs highest court, AudienciaNacional, to Google requiring it to delete information concerning a Spanish citizenôs financial problems from its search engine results. In this case, 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 CJEU. The Court held that this processing was in the context of the activities of Google Spain, an establishment in the Union, despite the fact that it was only operating in the area of advertising. On this basis, the CJEU found that the Data Protection Directive was applicable to that particular case and held that search engines were indeed data controllers that needed to remove personal data that met the criteria for a óright to be forgottenô.

This judgment essentially invokes long arm jurisdiction to hold the parent entity of a subsidiary company liable for processing of data related to an EU entity and subject. However, practical issues of compliance remains as the links to the Spanish article will be removed from Google Spain (and maybe, all Google subsidiaries in the EU) but it will be available on other jurisdictions which do not recognise the right to be forgotten such as the US (in Google US) to people disguising their location using a Virtual Private Network (popularly known as a VPN).[645]

However, this judgment comes with its own repercussions. The decision potentially allowed individuals to seek erasure of information made available by a number of other providers of social networking and information services.

10.3 International Practices

European Union

[643] Article 85, EU GDPR.
[644] *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.
[645] Klint Finley, ôIn Europe you will need a VPN to see real search resultsô, Wired (8 March 2016), available at: https://www.wired.com/2016/03/europe-youll-need-vpn-see-real-google-search-results/, (last accessed 28 October 2017).

The EU GDPR has chosen to recognise the right to be forgotten;[646] however, it has done so while acknowledging the social ramifications of obliterating all aspects of the past existence of certain data. According to the regulation, an individual who is no longer desirous of his personal data to be processed or stored would be able to erase it so long as the personal data is no longer necessary, relevant, or is incorrect and serves no legitimate interest.[647] Thus, it would follow that the right cannot be exercised where the information/data is necessary; for exercising the right of freedom of expression and information, for compliance with legal obligations, for the performance of a task carried out in public interest, on the grounds of public interest in the area of public health, for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, or for the exercise or defence of legal claims.[648] Under the EU GDPR, the decision on whether the right to erasure can be exercised, is to be taken by the data controller.[649]

The quantum of fine that is applicable to the data controller if such an entity takes an incorrect view or otherwise infringes Article 17 of the EU GDPR (right to erasure) may amount to 20 million euros or up to four percent of the total worldwide annual turnover of the preceding financial year, whichever is higher.[650]

Canada

Schedule 1, Principle 5 of PIPEDA provides the deletion of personal information that is no longer required.[651] Further, organisations are mandated to develop guidelines and implement procedures. Though PIPEDA allows the erasure of personal information to a certain extent, it is often criticised for including loopholes that allow freedom of speech to outweigh the right to be forgotten. It is thought that the right to be forgotten cannot be shoehorned into existing privacy law because search engines do not come within the scope of PIPEDA and the activity of indexing newsworthy content online is subject to the journalism exception in PIPEDA. Furthermore, any attempt to compel a search engine to not include particular results- particularly pointing to lawful content- falls foul of the freedom of expression right under the Canadian Charter of Rights and Freedoms.[652]

---

[646] Michael L. Rustad, Sanna Kulevska, ôReconceptualising the right to be forgotten to enable transatlantic data flowô, 28(2) Harvard Journal of Law & Technology 349 (2015).
[647] Article 17, EU GDPR.
[648] Article 17, EU GDPR.
[649] Article 17, EU GDPR.
[650] Article 83, EU GDPR.
[651] Schedule 1, Principle 5 of PIPEDA; Office of the Privacy Commissioner of Canada, ôSchedule 1, Principle 5 of PIPEDA; Personal Information Retention and Disposal: Principles and Best Practicesô (June 2014), available at: https://www.priv.gc.ca/en/privacy-topics/safeguarding-personal-information/gd_rd_201406/ ,(last accessed 28 October 2017).
[652] David T.S. Fraser, ôYouôd better forget the right to be forgotten in Canadaô (April 2016), available at: http://blog.privacylawyer.ca/2016/04/youd-better-forget-right-to-be.html, (last accessed 28 October 2017) cited in Office of the Privacy Commissioner of Canada, ôSubmissions received for the consultation on Online Reputationô, available at: https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-on-online-reputation/submissions-received-for-the-consultation-on-online-reputation/or/sub_or_07/ (last accessed 21 November 2017).

South Africa

Section 24 of the POPI Act states that personal information may only be stored or used to the extent it is adequate, relevant and not excessive in relation to its purpose.[653] Although POPI Act does not explicitly grant a right to be forgotten, Section 24 allows data subjects to request responsible parties to correct or delete personal information or records.[654]

The right to be forgotten in POPI Act only allows for deletion of personal information that is ñinaccurate, irrelevant, excessive, out-of-date, incomplete, misleading or obtained unlawfully.ò In addition, the act also requires responsible parties to delete or destroy records that should no longer be retained.[655]

10.4 Provisional Views

1. The right to be forgotten may be incorporated within the data protection framework for India as has been adverted to by the Supreme Court in *Puttaswamy.* Further, international practices in the EU GDPR and Canada also envisage a right to be forgotten in some form or manner thus strengthening the case for its incorporation.

2. The right to be forgotten should be designed in such a manner that it adequately balances the right to freedom of speech and expression with the right to privacy. The scope and contours of such a right may be determined in accordance with the capabilities of the data controllers to undertake the balancing exercise and determine the legitimacy of the request. Further, clear parameters on the basis of which a controller will carry out the balancing exercise may be incorporated in the law to enable them to effectively carry out this exercise. A residuary role for a sector regulator to develop particular guidelines for each sector may become necessary.

10.5 Questions

1. What are your views on the right to be forgotten having a place in Indiaôs data protection law?

2. Should the right to be forgotten be restricted to personal data that individuals have given out themselves?

3. Does a right to be forgotten add any additional protection to data subjects not already available in other individual participation rights?

4. Does a right to be forgotten entail prohibition on display/dissemination or the erasure of the information from the controllerôs possession?

---

[653] Section 24, POPI Act.
[654] Section 24, POPI Act.
[655] Andrew Weeks, ôThe Right to Be Forgotten in South Africaõ, Michalsons (26 March 2013), available at: https://www.michalsons.com/blog/the-right-to-be-forgotten/11868, (last accessed 28 October 2017).

5. Whether a case-to-case balancing of the data subjectôs rights with controller and public interests is a necessary approach for this right? Who should perform this balancing exercise? If the burden of balancing rests on the data controller as it does in the EU, is it fair to also impose large penalties if the said decision is deemed incorrect by a data protection authority or courts?

6. Whether special exemptions (such as the right to freedom of expression and information) are needed for this right? (over and above possible general exemptions such as national security, research purposes and journalistic or artistic expression)?

7. Are there any alternative views on this?

PART IV
REGULATION AND ENFORCEMENT

CHAPTER 1: ENFORCEMENT MODELS

1.1 Introduction

As a result of the nature and complexity of the legal provisions commonly constituting a data protection law, a broad range of questions arise regarding how these provisions can best be enforced. So as to develop a sound legal and regulatory framework, we must consider certain aspects of institutional design and overall approach before we can develop and align individual elements of the framework. This may be in terms of the extent of burden placed on entities covered under such framework, the structure and functions of any enforcement agency, or the tools at its disposal.

The enforcement of data protection norms is complicated by two factors primarily: first, the application of the norms across different fields, sectors, industries and contexts and, second, the rapid pace of development and change in data processing technologies.[656] These factors produce unique enforcement problems not found in other regulatory fields.

For instance, while many laws apply across different sectors, it has been observed that norms regarding information can be very contextual.[657] It could be quite problematic for a data protection law to run slip-shod over requirements in distinct walks of life that individuals desire to differentiate. Similarly, privacy norms have always been catching up to changes in technology that modify the playing field on which information is shared. The original conception of the right to privacy by Warren & Brandeis was driven by technological changes that permitted easier dissemination of information.[658] Similarly, the rise of computers and the internet have posed profound challenges for informational privacy.[659]

If anything, the rate of change of technology has only increased with time and appropriate legal responses are called for with greater rapidity. To add to this, different technologies with similar effects often come to be assessed according to various criteria including their prevalence and acceptability in society.[660] These concerns may not be capable of being addressed even where the substantive provisions of the law are technology-neutral. Instead, they additionally raise issues regarding the capacity of a data protection authority, if such an authority has been envisaged.

---

[656] Report of the Justice AP Shah Committee, 75 (October 16, 2012).
[657] Helen Nissenbaum, ôPrivacy as Contextual Integrity,ô 79 Washington Law Review 119, 137-41 (2004).
[658] Samuel Warren and Louis Brandeis, ôThe Right to Privacy,ô 4(5) Harvard Law Review 193 (15 December 1890).
[659] Jerry Kang, ôInformation Privacy in Cyberspace Transactionsô, 50 Stanford Law Review 1193, 1202-03 (April 1998).
[660] For example, in determining whether there had been a ôsearchô under the Fourth Amendment, the US Supreme Court has differentiated aerial surveillance from thermal imaging of homes on the basis of how common each practice was. See, *Florida v. Riley*, 488 U.S. 445, 447, 452 (1989) and *Kyllo v. United States*, 533 U.S. 27, 34, 40 (2001).

1.2 Types of Enforcement Models

There have been concerns in the past regarding the strength and effectiveness of enforcement mechanisms in the Indian context, especially when it comes to technology-related laws.[661] Appropriate consideration must thus be given to the enforcement model that is to be employed. Generally, one may consider three different variations:[662]

(i) ócommand and controlô regulation

This approach requires the State to provide legal rules or clear prescriptions for regulated entities, with no room for discretion. If these prescriptions are not followed, the State exercises its power to sanction. Where elements of a ócommand and controlô system are adopted, necessary features include the involvement of some governmental authority or the other, whether this involvement is through the establishment of a single, specialized agency or the creation of a federated, sectoral framework.

A number of issues are raised on this point, including whether the state machinery involved should be unified, how independent it should be from governmental control and industry influence, whether it should have regional spread, what regulatory tools and forms of sanction it should have at its disposal etc. Most jurisdictions do not have data protection frameworks that are purely ócommand and controlô in nature and create some room for industry involvement.

(ii) Self-regulation

This approach involves private organisations complying with standards they set for themselves without any enforcement by the State.[663] In a self-regulatory framework, norms become established either through market forces (such as demand for privacy from consumers), through industry standard-setting or through some limited facilitation of market transactions in the form of choice-enhancing legal rules such as information disclosure norms.

Legal obligations that enhance the fairness of transactions such as notice and privacy policy requirements may require governmental enforcement machinery and do not always fit comfortably in the self-regulation rubric. The US is a good example of a jurisdiction with largely self-regulatory elements, though a few sector-specific and state-specific laws are also in place. As these rules are a threshold requirement for achieving regulatory effectiveness,

---

[661] Deborah Roach Gaut and Barbara Crutchfield George, óOffshore Outsourcing to India by U.S. and E.U. Companies Legal and Cross-Cultural Issues that Affect Data Privacy Regulation in Business Process Outsourcingô, 6 UC Davis Business Law Journal 13 (2006).

[662] Dennis D. Hirsch, óThe Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation?ô 34 Seattle University Law Review 439, 440-41 (2011).

[663] Reuben Binns, óData Protection Impact Assessments: A meta-regulatory approach,ô 7(1) International Data Privacy Law 22, 25-29 (2017); Cary Coglienese and Evan Mendelson, óMeta-regulation and Self-Regulationô in Oxford Handbook of Regulation, 146, 147-148 (Robert Baldwin *et al eds.*, 2010).

they form core, substantive elements of a data protection framework and are not, appropriately, to be considered as part of the enforcement mechanism.

(iii) Co-regulation

This typically involves elements of both ócommand and controlô regulation and self-regulation. Co-regulation may be described as ñinitiatives in which government and industry share responsibility for drafting and enforcing regulatory standards.ò[664] This model advocates the formulation of a general data protection statute with broad provisions complemented by ñcodes of practices or conductò formulated by the industry and approved by the government or the relevant data protection authority.

Once these codes are approved, compliance with the detailed requirements of the code is treated as compliance with or evidence of compliance with the general provisions of the statute, thus promoting legal certainty within an otherwise uncertain regulatory scheme through the creation of ósafe harboursô.[665] The reason for the uncertainty that would otherwise prevail is the inherent generality of a broad statute that is unable to capture the multitude of situations that can arise in data processing. Such a co-regulatory approach would therefore appear useful in promoting compliance while also making room for innovation within the digital economy which may otherwise come to be severely restricted, especially for small businesses and start-ups.

In the context of privacy law in India, it may be noted that a co-regulatory model was suggested by the Justice AP Shah Committee.[666] A ócommand and controlô regulatory mechanism may be too rigid and may lag behind rapid technological changes which are prevalent in todayôs day and age. On the other hand, a pure self-regulation approach may lack enforcement and may lead to a situation where the objectives sought to be achieved by a data protection law are, effectively, not met.[667] Co-regulation may seem like an appropriate middle path that combines the flexibility of self-regulation with the rigour of government rule-making.[668]

---

[664] Dennis D. Hirsch, óThe Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation?ô 34 Seattle University Law Review 439, 441 (2011) (describing co-regulation as ñinitiatives in which government and industry share responsibility for drafting and enforcing regulatory standardsò); Hans-Bredow-Institut and Institute of European Media Law, óFinal Report: Study on Co-Regulation Measures in the Media Sectorô, 17 (June 2006).

[665] Dennis D. Hirsch, óGoing Dutch? Collaborative Dutch Privacy Regulation and the Lessons it Holds for U.S. Privacy Law,ô 2013 Michigan State Law Review 83, 86-87, 96 (2013); Ira S. Rubinstein, óRegulating Privacy by Design,ô 26 (3) Berkeley Technology Law Journal 1410, 1451-53 (2011).

[666] Report of the Justice AP Shah Committee, 75 (October 16, 2012).

[667] S. Pearson and A. Charlesworth, óAccountability as a Way Forward for Privacy Protection in the Cloudô, in 5931 Cloud Computing, Lecture Notes in Computer Science 131, 133 (M.G. Jaatun *et al eds*., 2009).

[668] However, the processes by which rule-making and enforcing powers are shared can raise concerns regarding undue benefits to industry with public interest being sidelined; Neil Gunningham and Darren Sinclair, óLeaders & Laggards: Next Generation Environmental Regulationô, 105-06 (Greenleaf, 2002); regarding the scope for abuse, *see* Bradyn Fairclough, óPrivacy Piracy: The Shortcomings of the United States Data Privacy Regime and How to Fix It,ô 42 (2) The Journal of Corporation Law 461, 476-77 (2016).

1.3 Provisional Views

Given that a co-regulation model envisages a spectrum of frameworks involving varying levels of government involvement and industry participation, it may be appropriate to pursue such a model that may be moulded to meet the circumstances as they emerge in the Indian context. It is also relevant to note that the co-regulation model is being adopted in most modern data protection systems to respond to the peculiar characteristics of this field of law.

1.4 Questions

1. What are your views on the above described models of enforcement?

2. Does co-regulation seem an appropriate approach for a data protection enforcement mechanism in India?

3. What are the specific obligations/areas which may be envisaged under a data protection law in India for a (i) ócommand and controlô approach; (ii) self-regulation approach (if any); and (iii) co-regulation approach?

4. Are there any alternative views to this?

CHAPTER 2: ACCOUNTABILITY AND ENFORCEMENT TOOLS

ACCOUNTABILITY

2.1 Introduction

The processing of personal data entails an increase of power (in terms of knowledge and its consequent insights) of the data controller vis-à-vis the individual. Data protection regulations are a means to help protect individuals from abuses of power resulting from the processing of their personal data. The method by which this protection was traditionally sought to be achieved was using notice and consent, offering the individual the autonomy to decide whether or not to allow her data to be processed after providing her full knowledge of what was going to be done with that data. As we have seen, that model has begun to come under pressure. Owing to the abundance of services, the complexity of data processing requirements and the multiplicity of purposes to which data can be put, notices have become too complex to understand. As a result, the concept of privacy self-management is coming under pressure given the complexity of the trade-offs between the benefits and the harms of modern technology.

To offset the flaws of the notice and choice model, a key principle that has emerged is of accountability as articulated in the EU GDPR. Central to accountability are the concepts of ôprivacy by designô and ôprivacy by defaultô which oblige businesses to consider data privacy at the initial design stages of a project as well as throughout the life cycle of the relevant data processing.[669] In this sense, accountability does not redefine data protection, nor does it replace existing law or regulation, since accountable organisations must comply with existing applicable law. Instead, accountability shifts the focus of privacy governance to an organisationôs ability to demonstrate its capacity to achieve specified privacy objectives.[670] A recent paper has suggested a much more aggressive use of accountability by holding data controllers responsible for all data under its control so much so that if a data subject suffers any harm as a result of a security breach or from the manner in which the data is processed, the data controller will be held liable for these harms.[671]

The essential elements of the principle of accountability in the EU are two-fold. First, a data controller should take appropriate measures to implement data protection principles. Second,

---

[669] Andrew Dunlop, Burges Salmon LLP, ôGDPR: The Accountability Principleô, Lexology (10 November 2016), available at: https://www.lexology.com/library/detail.aspx?g=5454293d-7fea-4963-afc4-7e4310ed0a1e, (last accessed 23 November 2017).

[670] Centre for Information Policy Leadership, ôData Protection Accountability: The Essential Elements A Document for Discussionô, Hunton & Williams LLP (October 2009), available at: https://www.hunton.com/files/webupload/CIPL_Galway_Accountability_Paper.pdf, (last accessed 21 November 2017).

[671] Rahul Matthan, ôBeyond Consent: A New Paradigm for Data Protection- Discussion Document 2017-03ô, Takshashila Institution (19 July 2017), available at: http://takshashila.org.in/wp-content/uploads/2017/07/TDD-Beyond-Consent-Data-Protection-RM-2017-03.pdf, (last accessed 24 October 2017).

a data controller must be in a position to demonstrate, when asked by a supervisory authority, that such measures have been adopted.[672]

The principle of accountability emphasises that standards prescribed externally either by the law or by the industry must be implemented internally by organisations.[673] The onus of proving that such measures have been complied with is placed on the organisation. This in many ways paves the way for effective implementation of data protection principles.

A more expansive use of accountability may hold the data controller strictly liable for any harm caused as a consequence of processing by it, irrespective of whether appropriate measures to implement data protection principles are put in place and implemented. This principle may be considered for processing that is inherently risky, in consonance with the strict liability principle as developed in traditional tort law.[674]

To illustrate the working of the general principle of accountability, consider a data controller embarking on a new process that involves personal data processing. The data controller, before commencing such processing, must consider the relevant standards in the law which apply to the processing. The standards may include requirements relating to grounds of processing, notice, consent, data quality, security of collected data, questions of access to data when data is to be handled by a data processor, etc. The data controller must draw up a procedure or policy as to how it intends to meet these standards. In drawing up this policy or procedure, it must have regard to any binding code of practice, industry practices and any other external binding standard. The data controller may also take into account any voluntary standard beyond the baseline norm which it abides by. If harm is caused to an individual owing to such processing, the data controller will bear the burden of proof to demonstrate that it had a policy to prevent such harm and implemented such policy. If such a policy does not exist, or was not implemented strictly, the data controller would be liable for damages. If however it does exist and it has been implemented, there is still a strong case that the data subject should not be left without recourse. One way in which a situation like this can be met is for data controllers to insure against such contingency to adequately compensate the data subject.

In addition, or as an alternative, if the nature of data processing is inherently risky, then any harm caused to an individual that can be traced back to the processing, would result in liability of the data controller.[675] Simply demonstrating that certain organisational measures

---

[672] Article 29 Working Party, ‘Opinion 3/2010 on the principle of accountability’, European Commission (13 July 2010), 9, available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp173_en.pdf, (last accessed 2 November 2017).

[673] Centre for Information Policy Leadership, ‘Data Protection Accountability: The Essential Elements A Document for Discussion’, Hunton & Williams LLP (October 2009), available at: https://www.hunton.com/files/webupload/CIPL_Galway_Accountability_Paper.pdf, (last accessed 21 November 2017).

[674] *Rylands v. Fletcher*, 1868 UKHL 1.

[675] *See* Baker Mckenzie, ‘Accountability Obligations under the GDPR’, available at: http://globalitc.bakermckenzie.com/files/Uploads/Documents/Global%20ITC/13%20Game%20Changers/BM-Accountability%20Obligations%20under%20the%20GDPR.pdf, (last accessed 23 November 2017).

have been taken or that the data subject consented to such use may not, by itself, be sufficient to disclaim liability.

The operation of this principle would mean that the processing of personal data by a data controller for its business needs commences and continues only in a manner which is in accord with the data protection principles. This approach, to some extent, shifts the burden away from the individual from having to constantly monitor whether his or her data is being processed as per law and ensures greater accountability for data controllers.

2.2 Issues

(i) Harm and Liability

The principle of accountability bears a close link to the liability to be cast on the data controller. In order to determine the contours of such liability, it may be important to establish what constitutes harm. For instance, if as a result of the manner in which the data is processed, the reputation of the individual is impaired so as to result in a loss in reputation or social standing of the individual, this could could have serious repercussions for the individual. Similarly, as a consequence of processing the data, the individual suffers any direct or indirect financial loss this could be easily identified as a harm that the data controller should be held accountable for. If the data controller uses the personal data about the individual in order to limit the choice available to the individual whether in terms of the information that she can access or any products or services that she is allowed to avail of, this too could be a harmful restriction of the options available to the individual. However, this kind of harm is of a qualitatively different nature as compared to the first two examples, constituting a denial of access or fair treatment, rather than material loss.

From amongst these, the data protection law could identify categories of material and non-material harm. If such harm is occasioned, it could trigger liability only on proof of failure to to take appropriate measures. Alternatively, if the nature of processing is inherently risky, the data controllers could become strictly liable, subject to the exceptions that the harm was caused by an act of God or the data subject herself contributed to the harm. A third alternative is for data controllers, or a certain class of data controllers to compulsorily take out insurance to cover certain types of harms caused to data subjects due to processing activities, even in a situation where the data controller has taken all reasonable measures according to law and established practices and standards.

(ii) Joint Controllers and Remoteness of Liability

Modern data processing is complex and often involves multiple service providers who process the individualôs data simultaneously or sequentially. Primary data collected directly from the individual is often made available through application programming interfaces (APIs) that can be accessed by various secondary data controllers who either process this data themselves or make the data available for further processing down the line. If any harm

results from this chain of processing it will be difficult to adequately allocate responsibility. While the principle of joint and several liability may be applied, it could be unfair to data controllers who have genuinely taken all care and diligence to safeguard the individual from harm. On the other hand, having such a stringent norm could be what is required to ensure that the data controllers take adequate efforts to ensure that anyone down the chain who is given access to the data takes care to ensure that it does not result in any harm. This may be effectuated by data controllers taking indemnities against harm being caused to the data subject owing to any processing in this chain. This is consonant with the baseline principle that harm suffered by an individual should not remain unredressed.

(iii) Audit

Harms that result from improper processing of data are not always immediately evident. For instance, in many cases, the bias inherent in the decision making algorithms is not immediately discernible. It is only after a large number of people suffer from improper processing that we come to realise the harm that is being caused. This could well be too late and in order to appropriately protect the individual the law must suggest proactive measures that detect these harms early enough. Thus, in addition to requiring that personal data processing beyond certain scales must be commenced only after having in place a policy or prescribed organisational procedure, there could be provisions for audits (both internal and external). This would be critical in implementing the second limb of accountability, i.e. maintaining the burden of proof of compliance on the data controller. A requirement of audit would mean that the data controller must maintain records of measures and processes which could provide proof of compliance of data protection principles.

(iv) Security Safeguard Obligations

Appropriate technical and organisational measures to ensure security of personal data are central to the principle of accountability. These measures should be in-tune with the cyber threats of today. At the same time, these security obligations should keep in mind the costs of implementation of such measures which have to be kept operational constantly as security and privacy breach protection require constant assessment and reporting.

The EU GDPR provides general security obligations that the data controller and the processer must follow. These are summarised below:

a. Obligation to assess the risks and implement security measures to mitigate those risks.
b. These risks are of varying likelihood and severity for the rights of individuals, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed.
c. Obligation to train staff having access to personal data on the steps to follow in case of a data breach (adopt an incident response plan).

The EU GDPR focuses on a ñrisk based approachò for continual assessment and adoption of mitigation measures. It does not mention whether the organisation should adopt a specific risk assessment industry standard (eg. ISO 27001, ISO 31000 etc). The only security practice it recommends is the use of pseudonymisation of personal data.

Accountability demands proactive actions from organisations including continuing investments to ensure that security safeguards are up to date. Organisations are expected to empower customers with tools and technologies to protect their data.

Under the existing privacy framework in India, Rule 8 of the SPDI Rules, mentions security practices that a body corporate should have in place for the purpose of protecting sensitive personal data. These security practices and standards should be supplemented by a comprehensive documented information security programme and information security policies that contain managerial, technical, operational and physical security control measures that are commensurate with the information assets being protected with the nature of business.[676] It also mentions making use of international Information Technology Security Standards such as ISO 27001 and the use of code of best practices created by self-regulatory bodies, once approved and duly notified by the government.[677] The use of empanelled auditors to ensure compliance was these practices was also mandated.

Security safeguards obligations should provide adequate protection to the personal data of the individuals while taking into account the financial and organisational capabilities of data controller. A risk-based approach of dealing with potential security and associated privacy incidents could be the general norm. The approach should define the risk criteria, the mitigation measures and mechanisms to ensure reporting and continual improvement.

2.3 International Practices

European Union

The EU GDPR provides that a data controller would be responsible for, and must be able to demonstrate compliance with principles relating to the processing of personal data (these include the purpose limitation principle, data accuracy principle, storage limitation principle etc.).[678] The obligation requires data controllers to implement appropriate technical and organisational measures to ensure and be able to demonstrate that data processing activities are performed in accordance with the data protection obligations set out under the EU GDPR.[679]

Data controllers must also review and update such technical and organisational measures whenever necessary.[680] The measures incorporated would take into account the nature and

[676] Rule 8(1), SPDI Rules.
[677] Rule 8(3), SPDI Rules.
[678] Article 5(2), EU GDPR.
[679] Article 24, EU GDPR.
[680] Article 24(2), EU GDPR.

scope of the processing activity, as well as the risks posed to the individual by processing her personal information.[681] Risks could include physical, material, or non-material damage. Non-material damage could include: discrimination, fraud, and reputational damage.

In order to demonstrate that a data controller has complied with its obligations under the EU GDPR, it could implement internal data protection policies; maintain relevant documentation of processing activities; and use data protection impact assessments where appropriate.[682]

South Africa

The POPI Act sets out that a ñresponsible partyò must ensure that certain conditions for lawful processing of personal data are satisfied at the time of processing.[683] The conditions for lawful processing of personal data are: accountability[684], processing limitation[685], purpose specification[686], further processing limitation,[687] information quality,[688] openness,[689] security safeguards,[690] and data subject participation.[691]

As part of the accountability principle, a responsible party must ensure that it secures the integrity and confidentiality of personal information in its possession by taking appropriate and reasonable technical and organisational measures in order to prevent loss, damage, or unauthorised destruction of personal information. The responsible party must also prevent unlawful access to, and unlawful processing of personal information. [692]

In order to ensure this, the POPI Act provides that a responsible party must take reasonable measures to identify all reasonably foreseeable internal and external risks to the personal information in its control, establish and maintain appropriate safeguards against these identified risks, verify that these safeguards are implemented and also to ensure that the safeguards are updated in order to respond to any new risks or to plug-in deficiencies found in the previous safeguard measures.[693]

The POPI Act has an additional obligation on third parties that process personal data on behalf of a responsible party. It provides that such third parties may process personal data only with the knowledge or authorisation of the responsible party and must treat personal information as confidential.[694] Additionally, the POPI Act provides that where an operator (a

[681] Article 25, EU GDPR, read with Recitals 74 and 75 of the EU GDPR.
[682] ICO, óAccountability and Governanceô, available at: https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/accountability-and-governance/, (last accessed 20 November 2017).
[683] Section 8, POPI Act.
[684] Section 8, POPI Act.
[685] Sections 9, 10, 11 and 12, POPI Act.
[686] Sections 13 and 14, POPI Act.
[687] Section 15, POPI Act.
[688] Section 16, POPI Act.
[689] Sections 17 and 18, POPI Act.
[690] Sections 19, 20, 21 and 22, POPI Act.
[691] Sections 23, 24 and 25, POPI Act.
[692] Sections 19(1)(a) and (b), POPI Act.
[693] Section 19(2), POPI Act.
[694] Section 20, POPI Act.

person who processes personal information for a responsible party on the basis of a contract) processes personal data, such operator is also bound to establish and maintain adequate security measures.[695]

Finally, in the event that the responsible party believes that the personal data of an individual has been accessed or acquired by an unauthorised party, then the responsible party must inform the Information Regulator. The responsible party must also notify the individual as soon as reasonably possible after the discovery of the data breach, and also take steps to restore the integrity of the responsible partyôs information system.[696]

Australia

Although the Privacy Act does not have a specific provision relating to accountability principle, the Privacy Act addresses this topic by way of the APPs under the said Act. For instance, APP 1 mandates open and transparent management of personal information. As per this principle, an APP entity must take reasonable steps to ensure the implementation of privacy practices and systems within the entity, which would ensure compliance with other data protection obligations under the Privacy Act.[697] Additionally, the said principles also provide that any entity holding personal information relating to an individual, must also take reasonable steps to protect this information from misuse, interference, loss, unauthorised access, modification or disclosure.[698]

Entities which come under the scope of the Privacy Act also have an additional obligation to destroy or de-identify personal information which is no longer required by an entity for any purpose.[699] The Privacy Act additionally mandates certain obligations on entities transferring personal information to overseas recipients. APP 8 provides that these entities must take reasonable steps to ensure that cross-border transfers do not breach any of the obligations set out under the Privacy Act and the APPs.[700] A breach of a privacy principle is said to occur when any activity of an entity is contrary to or inconsistent with the provisions set out under any of the APPs.[701]

Further, the OAIC has issued a ñGuide to securing personal informationò, which provides some guidance as to the reasonable steps which entities are required to take in order to protect personal information in their control from misuse, interference, loss, unauthorised access, modification or disclosure. It also provides guidance on the reasonable steps which entities

[695] Section 21(1), POPI Act.
[696] Section 22, POPI Act.
[697] APP 1, Privacy Act.
[698] APP 11, Privacy Act.
[699] APP 11, Privacy Act.
[700] APP 8, Privacy Act.
[701] Section 6A, Privacy Act.

may take once personal information in their possession is no longer required.[702] However, this guide is not legally binding in nature.

Canada

Accountability in relation to privacy is the acceptance of responsibility for personal information protection. An organisation which is accountable to individuals must have in place appropriate policies and procedures that promote good privacy practices.[703] The model code for protection of personal information contained in Schedule 1 of PIPEDA sets out that an organisation is responsible for any personal information that is under its control. The organisation must also designate certain individuals who must be accountable for the organisationôs compliance with the data protection obligations as set out under PIPEDA.[704]

PIPEDA also provides that an organisation is not only responsible for any personal information that is under its control, but is also responsible for any information transferred to a third party for processing. In such situations, an organisation must ensure that the third party also provides a comparable level of protection while processing personal information. This is usually ensured by contractual means.[705]

Additionally, organisations must implement policies and practices to protect personal information; establish procedures to receive and respond to complaints; train its staff about its data protection policies and practices.[706] PIPEDA provides that personal information must be protected by security safeguards appropriate to the sensitivity of the information. Security safeguards are intended to protect personal information against loss, theft, unauthorised access, disclosure, copying, use or modification.[707] The nature of safeguards, which an organisation is expected to implement, will be in accordance with the nature and sensitivity of the personal information in its possession.[708] Therefore, it follows that information of a more sensitive nature will be safeguarded by a higher level of protection. PIPEDA also prescriptively suggests some methods of protection that may be incorporated by an organisation. For instance, an organisation could utilise physical, organisational and technological measures to protect information in its possession.[709] Organisations must ensure that adequate care must be taken while disposing or destroying personal information, in order to prevent unauthorised parties from gaining access to the information.[710] The Office of the Privacy Commissioner has issued a guidance document to provide organisations assistance

[702] OAIC, ôGuide to Securing Personal Information: ôReasonable stepsô to protect personal informationô (January 2015), available at: https://www.oaic.gov.au/resources/agencies-and-organisations/guides/guide-to-securing-personal-information.pdf, (last accessed 20 November 2017).
[703] Office of the Privacy Commissioner of Canada, ôGetting Accountability Right with a Privacy Management Programô, available at: https://www.priv.gc.ca/media/2102/gl_acc_201204_e.pdf, (last accessed 20 November 2017).
[704] Principle 1 of Schedule 1, PIPEDA.
[705] Clause 4.1.3, Principle 1 of Schedule 1, PIPEDA.
[706] Clause 4.1.4, Principle 1 of Schedule 1, PIPEDA.
[707] Clause 4.7.1, Principle 1 of Schedule 1, PIPEDA.
[708] Clause 4.7.2, Principle 1 of Schedule 1, PIPEDA.
[709] Clause 4.7.3, Principle 1 of Schedule 1, PIPEDA.
[710] Clause 4.7.5, Principle 1 of Schedule 1, PIPEDA.

with developing certain baseline accountability principles which would help develop a comprehensive privacy management program.[711]

As is clear from the above, jurisdictions across the world have implemented the principle of accountability in varied forms. At their core, however, these practices require data controllers to adopt processes and procedures which are consistent with data protection principles. In the Indian context, as mentioned above, it may be worth exploring whether a statutory requirement to adopt such measures can be linked to liability in cases of clearly defined harms.

2.4 Provisional Views

Accountability, as a principle of data protection, has existed for some time and has found mention in various privacy laws around the world. It is imperative that the data protection law reflects the principle of accountability. Accountability should not only be enforced for breach of data protection obligations through the adoption and implementation of standards by data controllers, but also in certain well defined circumstances, it could be extended to hold data controllers liable for the harms that they cause to individuals without further proof of violation of any other obligation. The data protection law should appropriately identify such harms for which the data controller should be held liable in this manner.

2.5 Questions

1. What are your views on the use of the principle of accountability as stated above for data protection?

2. What are the organisational measures that should be adopted and implemented in order to demonstrate accountability? Who will determine the standards which such measures have to meet?

3. Should the lack of organisational measures be linked to liability for harm resulting from processing of personal data?

4. Should all data controllers who were involved in the processing that ultimately caused harm to the individual be accountable jointly and severally or should they be allowed mechanisms of indemnity and contractual affixation of liability inter se?

5. Should there be strict liability on the data controller, either generally, or in any specific categories of processing, when well-defined harms are caused as a result of data processing?

[711] Office of the Privacy Commissioner of Canada, ôGetting Accountability Right with a Privacy Management Programõ, available at: https://www.priv.gc.ca/media/2102/gl_acc_201204_e.pdf, (last accessed 20 November 2017).

6. Should the data controllers be required by law to take out insurance policies to meet their liability on account of any processing which results in harm to data subjects? Should this be limited to certain data controllers or certain kinds of processing?

7. If the data protection law calls for accountability as a mechanism for protection of privacy, what would be impact on industry and other sectors?

8. Are there any other issues or concerns regarding accountability which have not been considered above?

ENFORCEMENT TOOLS

2.6 Introduction

A number of regulatory tools and mechanisms may be simultaneously utilized to achieve different enforcement objectives. Some of these may be based on a co-regulatory model whereas others may be based on a ócommand and controlô approach. These are discussed below.

A. CODES OF PRACTICE

2.7 Issues

A code of practice or conduct is considered an important element in establishing a workable co-regulatory data protection scheme. As has been discussed in Part IV, Chapter 1 of the White Paper, a co-regulatory framework is one that integrates elements of self-regulation with elements of governmental regulation. Codes of conduct originate in ordinary industry practices where associations engage in standard-setting for better service provision or manufacturing. They thus naturally form part of some self-regulatory systems in the form of voluntary codes with no force of law.

However, in a co-regulatory system, a code of conduct or practice is integrated into the broader regulatory scheme through recognition of different types in the general statute. While adoption of a code remains voluntary and its formulation still involves industry participation, co-regulation may involve encouraging their creation or allowing compliance with them to serve as evidence of compliance with the data protection statute. Issuance of such codes by a regulator or other forms of legal recognition allows for such standard-setting practices to be formalised and anchored to statutory processes. This would also improve the transparency of the processes by which such codes are formulated while codes themselves create transparency regarding how information is being processed in practice.[712]

Codes of conduct suffer from some issues when conceived of as purely self-regulatory.[713] However, when such codes are viewed as part of a co-regulatory framework, their true potential can be exploited. The manner in which co-regulation can introduce government oversight and other elements of accountability is illustrated in international practices below.

---

[712] OAIC, óGuidelines for developing codes ï issued under Part IIIB of the Privacy Act 1988ô (September 2013), 2, available at: https://www.oaic.gov.au/resources/agencies-and-organisations/advisory-guidelines/guidelines-for-developing-codes.pdf, (last accessed 28 October 2017).

[713] Margot Priest, óThe Privatization of Regulation: Five Models of Self-Regulationô, 29(2) Ottawa Law Review 233, 242 (1998) (Codes of conduct only create accountability towards each other and not to the government; they engage in purely consensual rule-making; there is no real adjudication of violations or dispute resolution; there are very limited sanctions for violation apart from trade association dismissal; there is only limited coverage of the code across the industry due to its voluntary nature; and there is only rarely any involvement of the public or stakeholders external to the industry, no matter how large their stake).

2.8 International Practices

European Union

Under the EU GDPR, codes of conduct are recognised as compliance-signalling or demonstrating tools in a number of provisions.[714] Further provisions deal with the codes themselves stipulating that they can be formulated for subject matters like:[715]

a. fair and transparent processing;
b. the legitimate interests pursued by controllers in specific contexts;
c. the collection of personal data;
d. the exercise of the rights of data subjects;
e. technical and organizational measures, measures introducing data protection by design and by default, and safeguards for the security of processing;
f. the notification of personal data breaches to supervisory authorities and the communication of such personal data breaches to data subjects; or
g. the transfer of personal data to third countries or international organisations.

After drafts of these codes of conduct are prepared by representative bodies and submitted to it, the supervisory authority must provide an opinion on the same and where it finds the code in compliance with the EU GDPR, it must approve, register and publish the same.[716]

United Kingdom

Section 51(3) of UK DPA states that at the direction of the Secretary of State or the discretion of the Information Commissioner, the Information Commissioner may himself prepare and disseminate codes of practice ñfor guidance as to good practiceò after carrying out consultations. As per Section 51(4) of the UK DPA, the Information Commissioner is also required to encourage the preparation of such codes by trade associations. When such a draft code is submitted, the Information Commissioner must consider the draft and carry out consultations after which he may ñnotify the trade association whether in his opinion the code promotes the following of good practice.ò[717]

Canada

Section 24(c) of PIPEDA requires the Privacy Commissioner to encourage organizations to develop detailed policies and practices, including organizational codes of practice, towards compliance with processing obligations.[718]

---

[714] Articles 24(3), 28(5), 32(3), and 35(8), EU GDPR.
[715] Article 40, EU GDPR.
[716] Article 40, GDPR.
[717] Section 52(3), UK DPA further requires the Information Commissioner to lay before each House of Parliament any code of practice prepared on the direction of the Secretary of State but does not place this requirement for codes prepared by trade associations under Section 51(4).
[718] Codes may be developed for compliance with Sections 5 to 10, PIPEDA which deal with general obligations on the protection of personal information.

Australia

The Privacy Act makes extensive use of privacy codes as part of its overall framework through what are called APPs codes and Credit Reporting codes. These are envisaged to be developed by an entity, a group of entities, or a representative body or association of such entities. Under Part III B of the Privacy Act, the OAIC can approve and register enforceable codes developed by entities on their own initiative or on the request of the OAIC. These can be developed by the OAIC directly as well. These codes are envisaged to apply over and above the Privacy Actôs provisions and detail how the Privacy Actôs relevant provisions are to be complied with as well as who is bound by the code.[719] Entities bound by codes are required by law not to breach them[720] and such breach is deemed ñan interference with the privacy of an individualò.[721]

South Africa

Chapter 7 of the POPI Act lays down detailed provisions for codes of conduct, including for their issuance, notification, commencement, complaint mechanism, amendment, revocation, registration, review and compliance. A failure in compliance with an applicable code is deemed to be a breach of lawful processing conditions.[722] The Information Regulator issues such codes on its own initiative or on application by a representative body.[723]

2.9 Provisional Views

1. It may be important to incorporate and make provision for codes of practice within a data protection framework.

2. Such codes of conduct or practices may be issued by a data protection authority after appropriate consultations with the industry and individuals.

3. A data protection law may set out the various matters on which codes may be issued, which may include matters such as the best practices for privacy policies, data quality obligations or more core obligations on processing.

2.10 Questions

1. What are your views on this?

---

[719] OAIC, ógGuidelines for developing codes ï issued under Part IIIB of the Privacy Act 1988ô (September 2013), 2, available at: https://www.oaic.gov.au/resources/agencies-and-organisations/advisory-guidelines/guidelines-for-developing-codes.pdf, (last accessed 28 October 2017).
[720] Sections 26A and 26L, Privacy Act.
[721] Section 13, Privacy Act; the Privacy Act further includes a number of detailed provisions regarding the form of any such code, how it is to be prepared and registered, and how it is to be monitored and governed. These include complaint and investigation provisions as well as provisions for reviewing, varying and removing codes.
[722] Section 68, POPI Act.
[723] Sections 60 and 61, POPI Act.

2. What are the subject matters for which codes of practice or conduct may be prepared?

3. What is the process by which such codes of conduct or practice may be prepared? Specifically, which stakeholders should be mandatorily consulted for issuing such a code of practice?

4. Who should issue such codes of conduct or practice?

5. How should such codes of conduct or practice be enforced?

6. What should be the consequences for violation of a code of conduct or practice?

7. Are there any alternative views?

B. PERSONAL DATA BREACH NOTIFICATION

The aggregation of data in the hands of public and private entities leaves them vulnerable to data breaches. Data breaches can take many forms including; hackers gaining access to data through a malicious attack; lost, stolen, or temporary misplaced equipment; employee negligence; and policy and/or system failure. It is important to identify these threats and establish processes to deal with these breaches.

2.11 Issues and International Practices

(i) Defining Data Breaches

While data breaches may occur in various forms, these breaches can be classified using the fundamental principles of information security, i.e. confidentially, integrity and availability. So, a personal data breach may be categorised as the following:

a. Confidentiality breach: Where there is an unauthorised or accidental disclosure of, or access to, personal data.

b. Integrity breach: Where there is an unauthorised or accidental alteration of personal data.

c. Availability breach: Where there is an accidental or unauthorised loss of access to, or destruction of, personal data.

Based on the circumstances, a breach can concern confidentiality, availability and integrity of personal data at the same time, as well as any combination of these. Whereas determining if there has been a breach of confidentiality or integrity is relatively clear, whether there has been an availability breach may be less obvious. Carefully defining personal data breach is thus imperative.

The EU GDPR defines a ñpersonal data breachò as *"a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed"*.[724] Article 29 Working Party guidance on personal data breach notification notes that there is a difference between a security incident and a personal data breach.[725] A personal data breach is essentially a subset of a security incident. All personal data breaches are security incidents, not all security incidents are necessarily personal data breaches. So, only a security incident that hampers the security, confidentiality or integrity of personal data would result in a ópersonal data breachô

[724] Article 4(12), EU GDPR.
[725] Article 29 Data Protection Working Party, óGuidelines on Personal data breach notification under Regulation 2016/679ô, European Commission (3 October 2017), available at: http://ec.europa.eu/newsroom/document.cfm?doc_id=47741, (last accessed 10 November 2017).

In the US, personal data breaches are defined under sector-specific statutes or specific state laws. Under HIPAA Privacy Rule[726], a breach is, generally, an impermissible use or disclosure that compromises the security or privacy of the protected health information.[727] Privacy Technical Assistance Center (PTAC), established by the US department of education defines a data breach as any instance in which there is an unauthorized release or access of PII or other information not suitable for public release.[728]

Further, the California Security Breach Notification Act, 2016 defines a security breach as an unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the entity. Good-faith acquisition of personal information by an employee or agent of an entity for the purposes of the entity is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.[729]

North Dakota Century Code, Chapter 51-30 Notice of Security Breach for Personal Information defines a security breach as unauthorized acquisition of computerized data when access to personal information has not been secured by encryption or by any other method or technology that renders the electronic files, media, or data bases unreadable or unusable.[730]

It is important to note that although worded differently, US sector specific laws and a comprehensive privacy legislation like the EU GDPR, both recognise the cause and effect relationship between a security incident and a breach that may hamper personal data.

(ii) Data Breach Notifications

Data breach notification refers to the practice of alerting and informing stakeholders including data subjects that a personal data breach has occurred. The nature of notification required depends on the nature of data involved in the breach.

A breach can potentially have a range of significant adverse effects on individuals, which can result in physical, material, or non-material damage. The EU GDPR explains that this can include loss of control over their personal data, limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to

[726] The HIPAA Privacy Rule establishes national standards to protect individualsô medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically. The rule requires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization.
[727] Office for Civil Rights (OCR), óBreach Notification Ruleô, US Department of Health & Human Services (26 July 2013), available at: https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html, (last accessed 20 November 2017).
[728] Privacy Technical Assistance Center, óData Breach Response Checklistô (September 2012), available at: http://ptac.ed.gov/sites/default/files/checklist_data_breach_response_092012.pdf (last accessed 10 November 2017).
[729] Section 1(d), California Security Breach Notification Act, 2016.
[730] North Dakota Century Code, Chapter 51-30 Notice of Security Breach for Personal Information.

reputation, and loss of confidentiality of personal data protected by professional secrecy.[731] It can also include any other significant economic or social disadvantage to those individuals.

In general, the more sensitive the information involved, the more consequences there may be for the data subject. It is important to take note of this relationship between the degree of harm and the sensitivity of the data. Breach of sensitive personal data could have an immediate impact on the individual, which may lead to reputational or monetary damage.

Where there is a likely high risk of these adverse effects occurring, the EU GDPR requires the controller to communicate the breach to the affected individuals as soon as is reasonably feasible.[732] There needs to be an open line of communication between the organisation and its supervisory authority for the purpose of consultation with respect to the risk associated with the category of personal data the organisation is handling and the security safeguards, technical and policy, it has in place to tackle a breach associated with that category of personal data. The supervisory authority may advise the organisation based on the degree of harm for the individual, if and when the individual needs to be notified.

(iii) Breach Detection and Notification Duration

The EU GDPR requires that, in the case of a breach, the controller shall notify the breach without undue delay and, where feasible, not later than 72 hours after having become aware of it.[733] There has been a great debate around whether the stipulated time frame for notification is too short and what does it mean to become ñawareò of a personal data breach.

Becoming aware of a breach implies the detection of a security incident that has consequences for personal data of individuals by the organisation. The process of breach detection is very complex in nature, especially if the organisation has many allied business entities and the engages third party processors.

It is important to specify where this period of becoming aware of the breach begins. Is it when the allied business entities or third parties discover the breach or when the same is notified to the organisation acting as the data controller? It could take months, or even years to find and assess if the breach is in relation to personal data of an individual. The primary issue in relation to detection of breach is the large quantity of data that an organization has to comb through to find anomalies.

[731] Article 29 Data Protection Working Party, ó Guidelines on Personal data breach notification under Regulation 2016/679ô, European Commission (3 October 2017), available at: http://ec.europa.eu/newsroom/document.cfm?doc_id=47741, (last accessed 10 November 2017).
[732] Article 29 Data Protection Working Party, ó Guidelines on Personal data breach notification under Regulation 2016/679ô, European Commission (3 October 2017), available at: http://ec.europa.eu/newsroom/document.cfm?doc_id=47741, (last accessed 10 November 2017).
[733] Article 33(1), EU GDPR.

A research conducted by Ponemon Institute, sponsored by Arbor Networks and found that the average security breach (in North America and EMEA regions) in the retail services sector takes 197 days to detect and 98 days in the financial service sector.[734]

Under Section 6 of the New Mexico Data Breach Notification Act, 2017 (New Mexico Data Breach Act), a person that owns or licenses elements that include personal identifying information of a New Mexico resident shall provide notification to each New Mexico resident whose personal identifying information is reasonably believed to have been subject to a security breach. Notification shall be made in the most expedient time possible, but not later than 45 calendar days following discovery of the security breach**.**

The New Mexico Data Breach Act uses a time frame for notifying the individual in case of breach. It provides that the notification should happen as soon as possible but also provides an upper limit of 45 days for the purpose of notification to the affected individual. This legislation solely provides for one time notification of the individual affected by the breach in the manner prescribed under Section 7 of the said legislation.

This time frame allows the organisation to provide the individual with the information that would help her/him understanding how the incident took place, what is being done in this regard and the person or office to contact in case for following up. An argument in favour of this manner of notification would be that it doesnôt create a situation of panic, which might happen if the individual is informed right at the time of initial detection. At the stage of initial detection, the organisation itself is many times in the dark and wonôt have enough information to answer the individualôs queries and may result in an atmosphere of panic and mistrust. This point needs to be deliberated upon further in the Indian context, where the average individualôs privacy awareness is at a very different level from what it is in the EU or the US.

While fixing a time period for breach notification it is also important to take into consideration the magnitude of the leak. If the number of individuals affected is in millions then would it be prudent to put in a place a notification requirement like we see in the EU GDPR where the data controller has only 72 hours to notify the individuals? It might be within the ability of a large organisation to put automated reporting and breach notification mechanisms in place. But that might not be the case with respect to SME and start-ups across sectors. Building a notification matrix based on the size of the organisations could be a way to tackle this problem, providing different time limits for notifying individuals. This could solve this particular problem but at the risk of complicating the notification mechanism greatly.

[734] Ponemon Institute LLC, óAdvanced Threats in Retail ï A Study of North America & EMEAô, ARBOR Networks, available at: https://pages.arbornetworks.com/Global_Ponemon_Retail.html?utm_source=Ponemon&utm_medium=blog_post&utm_term=AT&utm_content=whitepaper&utm_campaign=Ponemon_Retail, (last accessed 21 November 2017); Ponemon Institute LLC, óAdvanced Threats in Financial Services ï A Study of North America & EMEAô, ARBOR Networks, available at: https://pages.arbornetworks.com/Global_Ponemon_Financial_Services.html?utm_source=Ponemon&utm_medium=blog_post&utm_term=AT&utm_content=whitepaper&utm_campaign=Ponemon_FinServ, (last accessed 21 November 2017).

There is a need to put in place a notification time line that keeps in mind all the above-mentioned factors.

(iv) Notification Requirements

Once a personal data breach is established the organisation must notify the competent authority. In US, the HIPAA demands notification of breach to the affected individuals, and in certain circumstances, to the media. A media notification is required only if a breach affects more than 500 residents of a state or jurisdiction. Reporting to media might put significant burdens on small companies. This option should be carefully weighed. Depending upon the nature of the breach, magnitude of the breach and to whom the notification is addressed, the format of the notification has to be adapted.

(v) Individual Notification

As a best practice, a personal data breach notification should mention; the type of personal data breach, the estimated date of the breach (could be in the form of a range), general description of the security incident in language that is comprehensible for an individual with average technical and legal knowledge. The notification must also inform the individual of his or her rights with respect to the breach and the contact information of the person or office in charge of addressing related grievances. The notification could be done by way of postal mail or electronic mail, as long as the notification is communicated to the affected individual in the stipulated time.

A standard format for notification could be drafted for administrative ease. But the content should reflect type of personal data breach, , the estimated date of the breach (could be in the form of a range), general description of the security incident, the estimated number of individuals affected by the breach, the steps being taken to minimise the impact of the breach and future resolution.

2.12 Provisional Views

1. The law may require that individuals be notified of data breaches where there is a liklelihood that they will suffer privacy harms as a result of data breaches.

2. The law may also require that the data protection authority or any authority be notified immediately on detention of data breaches.

3. Fixing too short a time period for individual notifications may be too onerous on smaller organisations and entities. This may prove to be counter productive as well as an organisation may not have the necessary information about the breach and its likely consequences.

4. The data protection authority may issue codes of practice which prescribe the formats for such notifications.

2.13 Questions

1. What are your views in relation to the above?

2. How should a personal data breach be defined?

3. When should personal data breach be notified to the authority and to the affected individuals?

4. What are the circumstances in which data breaches must be informed to individuals?

5. What details should an breach notification addressed to an individual contain?

6. Are there any alternative views in relation to the above, others than the ones discussed above?

C. CATEGORISATION OF DATA CONTROLLERS

2.14 Issues

Due to the breadth of a data protection law, its effectiveness can come to depend on the ability of a regulatory body to have adequate awareness and monitoring capacity of actual data protection practices so that it can identify and effectively address data protection risks. Not all processing activities pose risks of similar gravity and the nature or volume of the data being processed or the form of the processing operations themselves may require greater scrutiny and oversight. Such differentiation can be seen, for example, in banking regulation where ñsystemically important financial institutionsò seem to require additional forms of regulation.[735]

An example of a general exemption on the basis of the nature of the entity may be found under the (Australian) Privacy Act,[736] where ñsmall businessesò (with an annual turnover AUD 3 million or less) are exempt from obligations under the Privacy Act, though they may, nonetheless, have such duties in certain circumstances such as when the business discloses personal information about another individual for a benefit, service or advantage. Other instances of differentiated regulation within the data protection laws of other jurisdictions are outlined in specific points below regarding the additional obligations for these different entities. Different jurisdictions have categorised data controllers for the purposes of certain additional obligations and have made this categorization on varying criteria.

2.15 Additional Obligations on Data Controllers

(i) Registration

In the context of data protection, there is a need for prior identification and availability for monitoring of data controllers. As a result of this, data protection laws can create a registration requirement for data controllers. However, given the sheer multitude of such entities, it may actually be counterproductive for the requirement to be placed on all of them.

International Practices

In the UK, as per Section 17 of the UK DPA, no processing of personal data can be done by any data controller unless an entry on that entity is included in the register maintained by the Information Commissioner. However, it allows for an exemption from registration for processing that is not harmful, through notification by the Secretary of State and for processing for the sole purpose of maintaining a public register.[737]

---

[735] Financial Stability Board, ôReducing the moral hazard posed by systemically important financial institutions: FSB Recommendations and Time Linesô (20 October 2010), available at: http://www.fsb.org/wp-content/uploads/r_101111a.pdf, (last accessed 28 October 2017).

[736] Sections 6C, 6D and 6E Privacy Act.

[737] More than 400,000 organisations are currently registered: *See* ICO, ôRegister (notify) under the Data Protection Act,ô available at https://ico.org.uk/for-organisations/register/ (last accessed 28 October 2017).

(ii) Data Protection Impact Assessment

A data protection impact assessment (DPIA) is a process centred on evaluating activities that involve high risks to the data protection rights of individuals. The process can become necessary whenever a new project is taken up or a new policy is adopted by a data controller which may involve the use of a new technology or may have a significant impact on the data protection rights of individuals. A DPIA is aimed at describing the details regarding the processing activity, assessing the necessity and proportionality of such an activity, and helping manage the risks that are identified in relation to this activity.[738] The DPIA is carried out before the proposed processing activity is initiated so that the relevant data controller can plan the processing at the outset itself.

International Practices

European Union

Under Article 35 of the EU GDPR, there is a requirement to undertake a compulsory data protection impact assessment prior to data processing where a type of processing is likely to result in a high risk for the rights and freedoms of individuals. Certain kinds of processing activities are identified under the EU GDPR that would require such an assessment[739] and a supervisory authority is permitted to specify certain further activities that would trigger similar obligations.[740] Certain details regarding the contents of the assessment are also laid down. Recital 84 of the EU GDPR makes it clear that the outcome of the DPIA must be taken into account during the actual processing to demonstrate compliance and that where a DPIA indicates risks that cannot be mitigated, a consultation with the supervisory authority should be undertaken.[741]

Australia

Section 33D of the Privacy Act empowers the OAIC to direct an agency to carry out and submit a privacy impact assessment if the relevant activity or function might have a significant impact on the privacy of individuals. The provision also provides a non-exhaustive list of contents of the assessment.

Canada

Further, EU, Canada, Australia and South Africa do not appear to place any requirements for the registration of processing entities.

[738] Article 29 Data Protection Working Party, ―Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is ñlikely to result in a high riskò for the purposes of Regulation 2016/679‖, European Commission (4 April 2017), available at: http://ec.europa.eu/newsroom/document.cfm?doc_id=44137, (last accessed 20 November 2017).

[739] Article 35(3), EU GDPR. A DPIA would be required for ña systematic and extensive evaluation of personal aspectsò through automated processing, large scale processing of special categories of data, and processing of data related to criminal convictions and offences.

[740] Articles 35 (4) and (5), EU GDPR.

[741] It may be noted that the UK DPA and South Africaôs POPI Act do not make DPIAs mandatory.

The Treasury Board of Canada Secretariat has released a directive making privacy impact assessments mandatory for all governmental bodies covered under Section 3 of the Canada Privacy Act.[742]

(iii) Data Protection Audit

Data protection audits are processes that can be undertaken by a regulated entity by itself, through an external auditor, or through the regulator to assess whether the entityôs processing activities and overall policies are in line with applicable data protection law and good practice. The development of data protection auditing practices in an industry could well give rise to the establishment of specialised auditing agencies for this purpose and their empanelment under a data protection law may also be considered.

International Practices

European Union

The EU GDPR envisages a role for data protection audits within controller-processor contracts,[743] as a responsibility of a data protection officer,[744] as a mechanism for verification of compliance with binding corporate rules[745] as well as part of the investigative powers of a supervisory authority.[746]

United Kingdom

Under the UK DPA, the Information Commissioner is permitted to conduct audits with the consent of the data controller.[747]

Canada

Section 18 of the PIPEDA enables the Privacy Commissioner to carry out an audit of the ñpersonal information management practices of an organisationò after giving reasonable notice and at a reasonable time.[748]

---

[742] Article 29 Data Protection Working Party, óGuidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is ñlikely to result in a high riskò for the purposes of Regulation 2016/679ô, European Commission (4 April 2017), available at: http://ec.europa.eu/newsroom/document.cfm?doc_id=44137, (last accessed 20 November 2017).

[743] Article 28(3)(h), EU GDPR.

[744] Article 39(1)(b), EU GDPR.

[745] Article 47(1)(j), EU GDPR.

[746] Article 58(1)(b), EU GDPR.

[747] Section 51(7), UK DPA specifically states that the Information Commissioner would óassess any processing of personal data for the following of good practiceô and then óinform the data controller of the results of the assessment.ô

[748] The provision also lays down extensive powers for the purposes of auditing including summoning and enforcing appearance, administering oath, receiving and accepting evidence, entering premises etc. that are along the lines of investigative powers.

Australia

The Privacy Act requires credit rating bodies to ensure that regular audits are carried out by an independent person to ensure that certain agreements with credit providers are being complied with.[749]

South Africa

Under Section 89 of the POPI Act, the Information Regulator is required to assess ñwhether an instance of processing of personal information complies with the provisions of [the] Actò in the prescribed manner. It may do so on its own initiative or on request by or on behalf of the responsible party, data subject or any other person. The provision clarifies the mandatory nature of such assessment, stating that it must be carried out by the Information Regulator ñif it appears to be appropriateò though it may not make the assessment if, on a request, it is unable to identify the requester or the action that must be assessed.[750] Information notices are sent to the relevant organisation towards initiating an assessment.[751] A provision is also made regarding the assessment report resulting from the assessment process.[752] The report is to be given to the responsible party and the Information Regulator may also make any aspect of the assessment public if it is in public interest to do so.

(iv) Data Protection Officer

The designation of a specific individual or officer by a data controller to facilitate compliance through monitoring and advising as well as to act as a point of contact with a data protection authority is a crucial element of data protection laws. These individuals are often called data protection officers (DPOs).[753] It is relevant to note that in the present Indian legal framework, a body corporate is required to designate a grievance officer for grievance redressal purposes with certain details of the same posted on the body corporateôs website.[754]

International Practices

European Union

[749] Sections 20N (3)(b) and 20Q(2)(b), Privacy Act.
[750] Section 89(2), POPI Act. The criteria that the Information Regulator is to keep in mind when determining when it is óappropriateô to make the assessment is also laid down. *See* Section 89(3), POPI Act.
[751] Section 90, POPI Act.
[752] Section 91, POPI Act.
[753] For example, as part of EU GDPRôs accountability-based compliance framework, DPOs will be at the heart of the regulatory scheme, facilitating compliance with the provisions of the EU GDPR as key players: *See* Article 29 Data Protection Working Party, óGuidelines on Data Protection Officers (óDPOsôôô, European Commission (13 December 2016), 4-5, available at: http://ec.europa.eu/newsroom/document.cfm?doc_id=43823, (last accessed 20 November 2017).
[754] Rule 5(9), SPDI Rules.

Under the EU GDPR, only certain data controllers are required to designate a DPO.[755] Some provision is also made to maintain the independence and effectiveness of this officer.[756] The tasks of the DPO include informing and advising on as well as monitoring compliance, advising on and monitoring the performance of DPIAs, cooperating with the supervisory authority and acting as the authoritiesô contact point on all relevant issues.[757]

Canada

Under the PIPEDA, an accountability framework is built around certain individuals who have been designated by an organisation for compliance with accountability provisions[758] and for receiving challenges/complaints regarding compliance.[759] The PIPEDA also states that the designation of such individuals does not relieve organisations of their duty to comply with obligations.[760]

South Africa

The POPI Act adopts the designation of an information officer from the Promotion of Access to Information Act, 2000.[761] Further, it provides for certain additional obligations for the information officer such as encouraging organisational compliance with the relevant law, dealing with requests made to the body under that law, and working with the Information Regulator in relation to investigations.[762]

2.16 Provisional Views

1. The effective enforcement of a data protection law may require some form of differentiated obligations so that certain entities covered under the framework whose processing activities create higher degrees of risk or may cause significant harm can be more readily engaged with and guided in ensuring compliance with relevant obligations.

---

[755] Article 37, EU GDPR. (The provision outlines three situations in which the obligation to appoint a DPO arises: first, for a public authority or body (except a court) carrying out processing; second, where the controller core activities require regular, systematic and large scale monitoring of persons; and third, where such core activities require large scale monitoring of certain special categories of data).

[756] Article 38, EU GDPR. (The DPO may be a staff member or may be on a service contract. It is further mandated that the DPO is to receive adequate support and should not be instructed on his data protection tasks or dismissed or penalised for performing them. Any other tasks he is asked to fulfil should not create any conflict of interest).

[757] Article 39, EU GDPR. Further, there is no provision in the UK DPA for the appointment of a DPO: *See* Anita Bapat and Adam Smith, ôUnited Kingdom: Data Protection 2017,ô International Comparative Legal Guides (ICLG) (15 May 2017), available at: https://iclg.com/practice-areas/data-protection/data-protection-2017/united-kingdom, (last accessed 6 November 2017).

[758] Principle 1 of Schedule 1, PIPEDA (Accountability).

[759] Principle 10 of Schedule 1, PIPEDA (Challenging Compliance).

[760] Section 6, PIPEDA. Further, there is no provision in the Australian (Privacy Act) for for the appointment of a DPO: *See* Melissa Fai and Alex Borowsky, óAustralia: Data Protection 2017ô, International Comparative Legal Guides (ICLG) (15 May 2017), available at: https://iclg.com/practice-areas/data-protection/data-protection-2017/australia, (last accessed 6 November 2017).

[761] Section 1, POPI Act.

[762] Section 55, POPI Act.

2. The following additional obligations mentioned below may find place within the mechanism as appropriate:

(i) Registration

Registration obligations may be placed only for certain kinds of data controllers categorised on the basis of a specified criteria.

(ii) Data protection impact assessment

DPIAs may be required for certain categories of data controllers. Such DPIAs may, however, be undertaken in only specific instances, such as, where processing involves the use of new technology or likelihood of harm to any individual whose data is being processed.

(iii) Data audits

It would be beneficial for data protection law to provide for data protection audits in a regular manner for data controllers whose activities pose higher risks to the protection of personal data. A useful framework need not require the regulator to always carry out such audits itself and the law may provide for the registration of independent external auditing agencies. It may also contain some indication as to what an audit should cover in light of the technical nature of the compliance with certain obligations.

(iv) Data protection officer

There may be a substantial need for designating individuals who are made centres of accountability through their position in the data controllerôs organisation. Such officer may not only play an advisory role in relation to the data controller but must also be its external face in relation to complaints, requests and the requirements of a data protection authority.

2.17 Questions

1. What are your views on the manner in which data controllers may be categorised?

2. Should a general classification of data controllers be made for the purposes of certain additional obligations facilitating compliance while mitigating risk?

3. Should data controllers be classified on the basis of the harm that they are likely to cause individuals through their data processing activities?

4. What are the factors on the basis of which such data controllers may be categorised?

5. What range of additional obligations can be considered for such data controllers?

6. Are there any alternative views other than the ones mentioned above?

Registration

1. Should there be a registration requirement for certain types of data controllers categorised on the basis of specified criteria as identified above? If yes, what should such criteria be; what should the registration process entail?

2. Are there any alternative views in relation to registration?

Data Protection Impact Assessment

1. What are your views on data controllers requiring DPIAs?

2. What are the circumstances when DPIAs should be made mandatory?

3. Who should conduct the DPIA? In which circumstances should a DPIA be done (i) internally by the data controller; (ii) by an external professional qualified to do so; and (iii) by a data protection authority?

4. What are the circumstances in which a DPIA report should be made public?

5. Are there any alternative views on this?

Data Protection Audit

1. What are your views on incorporating a requirement to conduct data protection audits, within a data protection law?

2. Is there a need to make data protection audits mandatory for certain types of data controllers?

3. What aspects may be evaluated in case of such data audits?

4. Should data audits be undertaken internally by the data controller, by a third party (external person/agency), or by a data protection authority?

5. Should independent external auditors be registered / empanelled with a data protection authority to maintain oversight of their independence?

6. What should be the qualifications of such external persons/agencies carrying out data audits?

7. Are there any alternative views on this?

Data Protection Officer

1. What are your views on a data controller appointing a DPO?

2. Should it be mandatory for certain categories of data controllers to designate particular officers as DPOs for the facilitation of compliance and coordination under a data protection legal framework?

3. What should be the qualifications and expertise of such a DPO?

4. What should be the functions and duties of a DPO?

5. Are there any alternative views?

D. DATA PROTECTION AUTHORITY

2.18 Issues

With rapid technological growth, there has been a surge in the processing of individualsô personal data for multiple purposes. The potential for harms to individuals has risen. While a data protection law may be enacted to protect individuals, the implementation and efficacy of such a law may be contingent on the establishment of a robust, independent and technically sound supervisory authority. This is all the more so since issues pertaining to data protection may be highly specialised and may require expertise in several areas such as data analytics, data science, law and associated issues.

Currently, in India, there is no separate authority to ensure compliance with data protection obligations required to be followed by data controllers. The IT Act is limited in its scope and provides for the appointment of adjudicating officers[763] and an appellate mechanism,[764] whose primary mandate is restricted to adjudication of disputes arising under the IT Act. Therefore, a stronger mechanism in the form of a central, oversight authority may be required in India in order to effectuate the effective protection of personal data.

While there is divergence regarding the structure of enforcement and oversight mechanisms in relation to data protection in various jurisdictions, there appears to be strong support for establishing a single centralised regulatory authority when possible.[765] Several countries have moved from a complex multi-agency regulatory structure to a simpler national agency structure.[766] The benefits of a single, centralised regulatory authority, especially in the context of international trade opportunities, appear to be considerable since multinational companies may have a single point of contact and such an authority can ensure consistency by issuing a single set of rules, guidelines or standards. Moreover, it is easier for individuals to seek guidance and direct queries and complaints in relation to a data protection violation from a single, centralised regulatory authority.

2.19 International Practices

(i) Composition and terms of service

European Union

[763] Section 46, IT Act.
[764] Section 48, IT Act.
[765] *See* United Nations Conference on Trade & Development (UNCTAD), ôData Protection Regulations and International Data Flows: Implications for Trade and Developmentô (2016) available at: http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf, (last accessed 25 October 2017).
[766] For example, Japan has moved from 30 regulators to just one. *See* United Nations Conference on Trade & Development (UNCTAD), ôData Protection Regulations and International Data Flows: Implications for Trade and Developmentô (2016) available at: http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf, (last accessed 25 October 2017).

The EU GDPR envisages the establishment of one or more supervisory authorities in each Member State of the EU to ensure compliance with the provisions of the EU GDPR.[767] The EU GDPR provides that Member States shall have the flexibility to choose the qualifications, the eligibility conditions and the rules and procedures for appointment of the members of the supervisory authority.[768] The EU GDPR also prescribes that the duration of service of each member must not be less than four years.[769] The EU GDPR lays down specific provisions for ensuring the independence of the members of the supervisory authorities.[770] Moreover, a member may be dismissed only in cases of serious misconduct if the member no longer fulfills the conditions required for the performance of her duties.[771]

United Kingdom

The UK DPA mandates the establishment of an Information Commissioner responsible for enforcement of the obligations set out under the UK DPA.[772] The Information Commissioner is appointed by Her Majesty by Letters Patent[773] for a maximum term of seven years.[774] To aid in the discharge of her duties, the Information Commissioner can appoint a deputy commissioner and as many officers and staff as she may determine.[775] Removal of the Information Commissioner may happen if she fails to discharge the functions of the office for a continuous period of at least three months, fails to comply with the terms of appointment, is convicted of a criminal offence, declares bankruptcy, or is otherwise unfit to hold office and unable to carry out her functions.[776] The Information Commissioner may be removed from office by Her Majesty with recommendation from both Houses of the Parliament.[777]

Canada

The Privacy Commissioner is responsible for enforcing the provisions of the PIPEDA. The Canada Privacy Act sets out the provisions for appointment, tenure and duties of the Privacy Commissioner. The Privacy Commissioner is appointed by the Governor in Council after consultation with the leader of every recognised party in the Senate and House of Commons

[767] Article 51, EU GDPR.
[768] Article 54, EU GDPR. Further, Article 53, EU GDPR specifies that each Member State shall provide that the appointment of each member of the supervisory authority shall be by means of a transparent procedure by their parliament, their government, their head of State or an independent body entrusted with such appointment.
[769] Article 54, EU GDPR.
[770] Article 52, EU GDPR provides that each member of the supervisory authority shall remain free from external influence, not take instructions from anyone, shall not undertake any action which is incompatible with their duties and not engage in any incompatible occupation during the term of their office. The supervisory authority must have its own staff which shall be subject to the exclusive direction of the members of the supervisory authority. Moreover, each Member State is required to ensure that each supervisory authority is subject to financial control which does not affect its independence and that it has a separate public annual budget, which may be part of the overall state or national budget.
[771] Article 53, EU GDPR.
[772] Section 6 read with Schedule 5, UK DPA.
[773] Section 6(2), UK DPA.
[774] Rule 2(1) of Part I, Schedule 5, UK DPA.
[775] Rule 4(1) of Part I, Schedule 5, UK DPA.
[776] Rule 3A of Part I, Schedule 5, UK DPA.
[777] Rule 2(3) of Part I, Schedule 5, UK DPA.

and approval of the appointment by a resolution in the Senate and House of Commons.[778] The Privacy Commissioner holds office for a term of seven years but may be removed for cause by the Governor in Council at any time on address of the Senate and House of Commons.[779] The Canada Privacy Act also lays down specific provisions for ensuring the independence of the Privacy Commissioner.[780]

South Africa

The POPI Act establishes an independent Information Regulator which is tasked with governing the protection of personal information.[781] The Information Regulator is composed of a Chairperson and four members.[782] The POPI Act specifically includes strict instructions on the composition of the Information Regulator, i.e., at least one member of the Information Regulator must be appointed on account of experience as an advocate, attorney, or professor of law.[783] The remainder of the members may be appointed based on any other relevant qualifications.[784] The Chairperson and two regular members must be full-time employees whereas, the other two members may be there in a full-time or part-time capacity.[785] To be appointed within this body an applicant must be a citizen, a public servant, a member of some government body, employee of a political party, mentally fit, without criminal record, and must be chosen by the President on recommendation bythe National Assembly.[786] A committee is created within the National Assembly that nominates a member, who must then be approved by a majority of the Assembly.[787] The members may not be appointed for a period longer than five years, but will be eligible for reappointment at the the end of the term.[788] To ensure the lawful enactment of the duties of the Information Regulator, the POPI Act explicitly states that the Information Regulator must be impartial and perform its functions without fear, favour or prejudice.[789] The members are not permitted to undertake any other remunerative work while they hold office.[790]

Australia

[778] Section 53(1) of the Canada Privacy Act.
[779] Section 53(2) of the Canada Privacy Act.
[780] Section 54 of the Canada Privacy Act stipulates that the Privacy Commissioner shall engage exclusively in the duties of the office of the Privacy Commissioner and shall not engage in any other employment for reward. Further, the Privacy Commissioner shall be paid a salary equal to that of a judge of the Federal Court and shall also be entitled to a pension equivalent of that received by others in public service.
[781] Section 39, POPI Act.
[782] Section 41, POPI Act.
[783] Section 41, POPI Act.
[784] Section 41, POPI Act.
[785] Section 41, POPI Act.
[786] Section 41, POPI Act.
[787] Section 41, POPI Act.
[788] Section 41, POPI Act.
[789] Section 39(b), POPI Act.
[790] Section 41, POPI Act.

The OAIC is mandated to ensure enforcement of the provisions of the Privacy Act.[791] The OAIC is appointed by the Governor-General by a written instrument[792] for a duration of no more than five years.[793] To ensure the lawful enactment of his/her duties by the OAIC, she may not engage in paid employment outside the duties of his or her office without the Ministerôs approval.[794]

(ii) Functions, powers and duties of data protection authorities

European Union

The functions, duties and powers of the supervisory authority under EU GDPR include the following:[795]

a. Monitoring, enforcement and investigation

The supervisory authority must monitor and enforce the application of the EU GDPR. It also has the power to handle complaints lodged by a data subject, duty to investigate the complaint (including obtaining from the data controller access to all personal data as required) and inform the complainant of the progress and outcome of the investigation within a reasonable period. The supervisory authority has the power to order the rectification or erasure of personal data, issue warnings and reprimands, and impose administrative fines on a data controller in case of breach of data protection obligations. The supervisory authority also has the power to carry out data protection audits and impact assessments.

b. Advisory powers

The supervisory authority can advise the Member States and other institutions on legislative and administrative measures relating to protection of natural personsô rights and freedoms about processing.

c. Standard setting powers

The supervisory authority can establish codes of conduct, encourage the establishment of data protection certification mechanisms, data protection seals and marks, and undertake periodic review of issued certifications.

d. Awareness generation

[791] The OAIC is established under Section 5, Australian Information Commissioner Act, 2010 (Australian Information Commissioner Act).
[792] Section 14, Australian Information Commissioner Act.
[793] Section 15, Australian Information Commissioner Act. Per Section 16, Australian Information Commissioner Act, the OAIC is not permitted to engage in paid employment outside the duties of her office without the Ministerôs approval.
[794] Section 16, Australian Information Commissioner Act.
[795] *See* Articles 35, 57, 58, 77 and 83, EU GDPR.

The supervisory authority shall promote awareness of data controllers and processors of their obligations under the EU GDPR and promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing.

United Kingdom

The functions, duties and powers of the Information Commissioner of UK include the following:[796]

a. Monitoring and enforcement

The Information Commissioner has the power to issue an ‘enforcement notice’, ‘assessment notice’ and ‘information notice’ in order to determine whether the data controller has complied with the provisions of the UK DPA.[797]

b. Standard setting powers

The Information Commissioner may encourage trade associations to prepare and to disseminate to their members codes of practices, and where any trade association submits a code of practice to the Information Commissioner for her consideration, notify the trade association whether in her opinion the code promotes the following of good practice.

c. Awareness generation

The Information Commissioner must also provide educational materials to the public so that individuals are aware of their data protection rights. In order to ensure that data controllers are aware of their obligations in relation to processing operations of personal data, the Information Commissioner can disseminate information to data controllers that pertains to the same.

Canada

The functions, duties and powers of the Privacy Commissioner include the following:

a. Monitoring, enforcement and investigation

The Privacy Commissioner’s investigative powers predominantly include the handling of all complaints filed under PIPEDA.[798] While conducting an investigation, the Privacy Commissioner may review evidence, collect relevant records, and enter any premises and prepare a report within one year of filing of the complaint that contains all the findings and recommendations.[799] Where the Privacy Commissioner deems a complaint resolvable without

[796] Section 51, UK DPA.
[797] Sections 40, 41A and 43, UK DPA.
[798] Section 11(1), PIPEDA.
[799] Section 13(1), PIPEDA.

extensive investigation, she may resolve such complaint through dispute resolution mechanisms, such as, mediation and conciliation.[800]

b. Awareness generation

The Privacy Commissioner is required to promote research activities relating to the privacy of individuals and processing of personal information by persons other than by government institutions. [801]

South Africa

The functions, duties and powers of the Information Regulator of South Africa include the following:[802]

a. Awareness generation

This includes advising public and private entities on data protection matters and ensuring no influential actions are taken that risk the protection of personal information.

b. Monitoring, enforcement and investigation

This includes investigation and resolving of complaints arising under the POPI Act. It also includes monitoring developments in information processing and computer technology. Further, the Information Regulator is also required to conduct an assessment of a public or private body in respect of processing of personal information.

c. Laying down codes of conduct and facilitating cross-border cooperation

This includes assisting bodies to develop codes of conduct regarding protection of personal information. Further, it also includes consulting with national and international bodies that are concerned with data protection or information processing.

Australia

The functions, duties and powers of the OAIC include the following:[803]

a. Guidance related functions

It includes making guidelines to adopt best practices in relation to data protection. The OAIC should promote an understanding of APPs.

[800] Section 12.1(2), PIPEDA.
[801] Section 60(1), Canada Privacy Act.
[802] Section 40, POPI Act.
[803] Section 28, 28A, 28B, Privacy Act.

b. Advisory

The functions of the OAIC include providing advice to a Minister or entity regarding data protection. The OAIC must provide reports and recommendations to the Minister regarding protection of the privacy of individuals.

c. Monitoring, enforcement and investigation

The OAIC is required to monitor the accuracy of information held by the entity. It must also ensure no entity is using information for unauthorised purposes. The investigative powers of the OAIC include the power to conduct investigation, obtain information and documents and the power to examine witnesses.[804]

2.20 Provisional Views

1. Based on the above, it follows that a separate and independent data protection authority may be set up in India for enforcement of a data protection legal framework.

2. There are three broad categories of functions, powers and duties which may be performed by a data protection authority: monitoring, enforcement and investigation; standard-setting; and awareness generation.

3. Specifically, the above functions may include:

(i) Monitoring, enforcement and investigation

This may include the power to (a) ensure compliance and enforcement with the provisions of a data protection law; (b) conduct inspection, investigations and collect documents as may be required; (c) adjudicate disputes arising between individuals and data controllers; (d) monitor cross-border transfer of data; (e) monitor security breaches; (f) issue directions to all relevant entities; (g) impose civil penalties for non-compliance; and (h) issue regulations in order to facilitate the enforcement of data protection principles and other ancillary matters relating to data protection.[805]

(ii) Awareness generation

This may include: (a) the ability to conduct research and promote public awareness of data protection; and (b) the power to educate public and private entities.

(iii) Standard setting

[804] *See* Part V, Privacy Act.
[805] The power to issue regulations are standard provisions which are there in the TRAI Act, Securities and Exchange Board of India Act, 2002 (SEBI Act), and the Insurance Regulatory and Development Authority Act, 1999.

This may include the power to: (a) issue codes of conduct/practice; (b) lay down standards for security safeguards; (c) lay down standards for data protection impact assessment; and (d) lay down standards for registration for data controllers as may be required and maintain a database in this regard. Some of these standards relate to data protection issues, e.g., standards for data protection impact assessments; others such as standards for security safeguards are not *per se* related to data protection. The role of the central government in relation to setting of standards for the latter and such analogous categories and organisational measures should be ensured.

2.21 Questions

1. What are your views on the above?

2. Is a separate, independent data protection authority required to ensure compliance with data protection laws in India?

3. Is there a possibility of conferring the function and power of enforcement of a data protection law on an existing body such as the Central Information Commission set up under the RTI Act?

4. What should be the composition of a data protection authority, especially given the fact that a data protection law may also extend to public authorities/government? What should be the qualifications of such members?

5. What is the estimated capacity of members and officials of a data protection authority in order to fulfil its functions? What is the methodology of such estimation?

6. How should the members of the authority be appointed? If a selection committee is constituted, who should its members be?

7. Considering that a single, centralised data protection authority may soon be over-burdened by the sheer quantum of requests/ complaints it may receive, should additional state level data protection authorities be set up? What would their jurisdiction be? What should be the constitution of such state level authorities?

8. How can the independence of the members of a data protection authority be ensured?

9. Can the data protection authority retain a proportion of the income from penalties/fines?

10. What should be the functions, duties and powers of a data protection authority?

11. With respect to standard-setting, who will set such standards? Will it be the data protection authority, in consultation with other entities, or should different sets of

standards be set by different entities? Specifically, in this regard, what will be the interrelationship between the data protection authority and the government, if any?

12. Are there any alternative views other than the ones mentioned above?

CHAPTER 3: ADJUDICATION PROCESS

3.1 Introduction

Adjudication plays an integral role in the enforcement of any law as it ascertains the rights and obligations of parties involved in a dispute and prescribes the corrective actions and remedies. In the context of a data protection law, adjudication entails an assessment of whether and to what extent data protection rights of an individual have been infringed by a data controller, the loss or damage suffered by the individual due to the said infringement, the remedies available to the individual as well as the penal consequences that the data controller may be liable for. Given the technical and specialised nature of the issues that may arise while adjudicating under a data protection law, it is imperative to evaluate the shortcomings of existing adjudicatory mechanisms in India in this field and propose an adjudicatory framework along with the remedies that may be available (the substantive issues relating to ôRemediesô is dealt with in Part IV, Chapter 4 of the White Paper).

3.2 Issues

Under the extant Indian legal framework, specifically the IT Act, a special class of officers called ôadjudicating officersô are appointed for hearing and adjudicating cases pertaining to violations of the provisions of the IT Act or of any rule, regulation, direction or order made thereunder.[806] The IT Act also specifies certain disputes in relation to which the adjudicating officer has the power to adjudicate.[807]

An adjudicating officer is an officer not below the rank of a ôDirectorô to the Government of India or an equivalent officer of a State Government and is required to have such experience in the field of information technology and legal or judicial experience as may be prescribed.[808] Further, an adjudicating officer is required to adjudicate matters in which the claim for injury or damage does not exceed Rs. 5 crores.[809] Moreover, while adjudicating, an adjudicating officer shall have the powers of a civil court.[810]

It is relevant to note that the adjudicatory functions discharged by adjudicating officers primarily relate to fraudulent transactions from bank accounts on account of failure to

[806] Section 46(1), IT Act.
[807] Sections 43 (Penalty and compensation for damage to computer, computer system, etc.), 43A (Compensation for failure to protect data), 44 (Penalty for failure to furnish information, return, etc.) and 45 (Residuary penalty), IT Act.
[808] Section 46(1) and (3), IT Act.
[809] Section 46(1A), IT Act. Please note that jurisdiction in respect of a claim for injury or damage exceeding Rs. 5 crores shall vest with the competent court.
[810] Section 46(5), IT Act. All proceedings before an adjudicating officer shall be deemed to be judicial proceedings within the meaning of Sections 193 and 228, IPC, shall be deemed to be a civil court for the purposes of Section 345 and 346, CrPC and shall be deemed to be a civil court for the purposes of Order XXI, Civil Procedure Code, 1908 (CPC).

maintain reasonable security practices[811] and as such, it appears that such orders may not *per se* relate to other aspects of data protection violation.

So far as the appellate mechanism under the IT Act is concerned, prior to the enactment of the Finance Act, 2017 (Finance Act), appeals from decisions of adjudicating officers lay before the CyAT set up under Section 48 of the IT Act. The CyAT, which started functioning in 2006, was set up with a specific mandate to hear appeals on matters where the jurisdiction of civil courts was barred, i.e. where the claim for injury or damage does not exceed Rs. 5 crores.[812] However, the CyAT has, as of 31 March 2017, passed merely 17 judgments and has passed no judgement after 30 June 2011.[813] Moreover, the chairmanôs position for the CyAT has been lying vacant since July 2011 and consequently, though appointment of members has been carried on, a bench to hear the matters has not been constituted in the absence of a chairman.

In order to bring about rationalisation of tribunals, uniformity in service, efficiency and cost optimisation[814], the IT Act was amended by the Finance Act to confer the powers of the CyAT to hear appeals from the decisions of the adjudicating officers to the Telecom Disputes Settlement and Appellate Tribunal (TDSAT or Appellate Tribunal)[815]. There are concerns on whether the current resources, capacity and infrastructure of the Appellate Tribunal can take on the additional mandate of discharging the functions of the CyAT[816].

Upon adjudication, the adjudicating officer under the IT Act has the power to give remedies in the form of either a civil penalty imposed upon the defaulter or grant compensation to the aggrieved individual. Section 43A of the IT Act stipulate that any person who commits the acts specified under the said provision shall be liable to pay damages by way of compensation to the person so affected.[817] Given that there does not appear to be any specific limit on the amount of compensation payable under this provision, it follows that a person affected by an infringement may assess the damages on her own so long as the amount assessed does not

---

[811] Sreenidhi Srinivasan and Namrata Mukherjee, ôBuilding An Effective Data Protection Regimeö, Vidhi Centre For Legal Policy 19 (January 2017). *Also see Ram Techno Park v. State Bank of India*, Complaint No. 9 of 2012, Adjudicating Officer (Maharashtra) Order dated 22 February 2013, available at: https://it.maharashtra.gov.in/Site/Upload/ACT/DIT_Adjudication_RamTechno_Vs_SBI-22022013.pdf, (last accessed 23 October 2017) and *M/s Shreenivas Signs Pvt. Ltd. v. IDBI Bank Ltd.*, Complaint No. 12 of 2013, Adjudicating Officer (Maharashtra) Order dated 18 February 2014, available at: https://it.maharashtra.gov.in/Site/Upload/ACT/DIT_Adjudication_SreenivasSigns_Vs_IDBI-18022014.PDF, (last accessed 23 October 2017).

[812] Section 61, IT Act.

[813] *See* ôJudgmentsö, Cyber Appellate Tribunal, available at http://cyatindia.gov.in/Judgement.aspx (last accessed 22 October 2017).

[814] Radhika Merwin, ôMerger of tribunals to rationalize workingö, Hindu Business Line (23 March 2017), available at: http://www.thehindubusinessline.com/economy/policy/merger-of-tribunals-to-rationalise-working/article9598534.ece, (last accessed 22 October 2017).

[815] The TDSAT is established under Section 14 of the TRAI Act. An appeal from the TDSAT lies with the Supreme Court of India (as per Section 18, TRAI Act).

[816] It is relevant to note that in 2004, the TDSATôs jurisdiction was extended to cover broadcasting services. Moreover, per the Finance Act, the mandate of the Airports Economic Regulatory Authority Appellate Tribunal has also been transferred to the TDSAT (in addition to that of the CyAT).

[817] Similar provision is contained in Section 43, IT Act.

exceed Rs. 5 crores.[818] Furthermore, in case of a contravention of the provisions of the IT Act for which no penalty has been prescribed separately, the defaulting person shall be liable to pay a penalty not exceeding Rs. 25,000 or compensation not exceeding Rs. 25,000.[819]

Compensation, as a remedy under Section 43A of the IT Act is extremely limited and is applicable where a body corporate fails to maintain and implement reasonable security practices and procedures. Moreover, for any other violation of the provisions of the IT Act (for which no separate penalty is prescribed), the amount of compensation that may be claimed is limited to Rs. 25,000. In the context of adjudication of disputes pertaining to data protection violation, it may be relevant to consider the extent to which adjudicatory bodies may grant compensation to an aggrieved party and consequently, determine the jurisdiction and powers of adjudicatory bodies in this regard.

3.3 International Practices

European Union

Under the EU GDPR, the supervisory authority set up in every Member State has the power to investigate complaints relating to the breach of any of the rights of the data subject.[820] The supervisory authority has a wide range of investigative powers[821] and corrective powers.[822] A data subject may file a complaint with the supervisory authority where she considers that the processing of personal data related to her infringes the EU GDPR.[823] The supervisory authority has the power to impose an administrative penalty on the data controller where the latter has breached the provisions of the EU GDPR.[824] The data subject, however, also has the right to bring an appeal or seek a remedy from the competent courts of the Member States where the supervisory authority is established where the said authority does not handle the complaint or does not inform the data subject about the progress or outcome of the complaint within the prescribed time limit.[825]

United Kingdom

Under the UK DPA, the Information Commissioner has several powers including the power to issue ‘enforcement notices’ to data controllers in case of contravention of the provisions of the UK DPA.[826] The Information Commissioner also has the power to issue ‘assessment

[818] Please note that for a claim above Rs. 5 crores, the claim will be filed with a civil court having competent territorial and pecuniary jurisdiction. In other words, when such a claim is filed with a civil court, then the special adjudicatory mechanism of the IT Act will no longer be the procedural law and the process will be governed by the provisions of the CPC. *See* Apar Gupta, ‘Commentary on Information Technology Act’, 184 (Lexis Nexis, 2013).
[819] Section 45, IT Act. Section 44, IT Act only prescribes a penalty for failure to furnish information, return, etc.
[820] Article 57(1)(f), EU GDPR.
[821] Article 58(1), EU GDPR.
[822] Article 58(2), EU GDPR.
[823] Article 77(1), EU GDPR.
[824] Article 83, EU GDPR.
[825] Article 78, EU GDPR.
[826] Section 40, UK DPA.

noticesô[827] and áinformation noticesô in order to determine whether the data controller has complied with the provisions of the UK DPA.[828] Where a data controller fails to comply with any of the notices, then it may be considered as an offence under the UK DPA.[829] The Information Commissioner may impose a monetary penalty upon the data controller for contravention of data protection principles.[830] A data controller on whom any type of notice under the UK DPA has been served by the Information Commissioner, has the right to file an appeal with the First-tier Tribunal.[831]

Australia

Under the Privacy Act, in case of a breach of the privacy principles, an individual can file a complaint with the OAIC.[832] Where it is not feasible to conciliate between the parties, the OAIC may undertake an investigation and upon finding of a substantiated complaint, can direct the respondent to not repeat such a conduct or perform a reasonable act to redress the loss suffered by the individual.[833] On an application by the OAIC, if the prescribed court is satisfied that the respondent has contravened the provisions of the Privacy Act, it may order the respondent to pay a penalty.[834] The OAIC may also undertake the above on the basis of a *suo moto* action.[835] Moreover, an application for review of an order made by the OAIC lies with the Administrative Appeals Tribunal.[836]

Canada

In Canada, under the PIPEDA, the Privacy Commissioner may take cognizance of a complaint filed by an individual or on its own.[837] Upon filing of a complaint, the Privacy Commissioner may conduct an investigation.[838] Upon completion of investigation, the Privacy Commissioner is required to prepare a report consisting of its findings and recommendations.[839] On receiving the report, the individual may apply to the court for a hearing in respect of the matter in relation to which the complaint was made or that is referred to in the Privacy Commissionerôs report.[840] The court may direct the organization to correct its practices and award damages to the complainant.[841]

---

[827] Sections 41A, 41B, 41C and 42, UK DPA.
[828] Section 43, UK DPA.
[829] Section 47, UK DPA.
[830] Sections 55A-55E, UK DPA.
[831] Section 48, UK DPA read with ICO, ñInformation Commissionerôs guidance about the issue of monetary penalties prepared and issued under section 55C(1) of the Data Protection Act 1998ò, 3 (December 2015), available at: https://ico.org.uk/media/for-organisations/documents/1043720/ico-guidance-on-monetary-penalties.pdf, (last accessed 20 October 2017).
[832] Section 36, Privacy Act.
[833] Section 52, Privacy Act.
[834] Section 80W, Privacy Act.
[835] Section 52(1A) read with Section 40(2), Privacy Act.
[836] Section 96, Privacy Act.
[837] Section 11, PIPEDA.
[838] Section 12, PIPEDA.
[839] Section 13, PIPEDA.
[840] Section 14, PIPEDA.
[841] Section 16, PIPEDA.

Under the POPI Act, the Information Regulator may undertake investigation into a complaint submitted by a person for, *inter alia*, breach of the conditions of lawful processing of personal information.[842] The Information Regulator may also, on its own initiative, commence investigation.[843] On receipt of a complaint, the Information Regulator may conduct a pre-investigation[844], act as a conciliator, conduct a full investigation or refer the complaint to its enforcement committee[845]. Where the Information Regulator is satisfied with the organization has interfered with the protection of personal information of the complainant, the Information Regulator may issue a notice directing the organization to take corrective steps accordingly.[846] A penalty may also be imposed on the organization.[847] A right of appeal against the direction/notice of the Information Commissioner lies with the High Court having the requisite jurisdiction.[848]

3.4 Provisional Views

1. Given that under a data protection legal regime, government bodies and public authorities may be considered as data controllers, an adjudicating officer appointed under the IT Act, who is an officer of the government, may not be the appropriate body to adjudicate disputes which involve violation of data protection obligations by such government bodies and public authorities. Therefore, it may be appropriate for a separate, independent body, such as, a data protection authority to adjudicate on disputes arising between an individual and a data controller due to breach of any data protection obligation.

2. It follows that an individual whose data protection rights have been violated may, at the outset, first approach the data controller or a specific grievance redressal officer of the data controller identified in this regard.

3. Where the data controller fails to resolve the complaint of the individual in a satisfactory and expeditious manner, the individual may be given the right to file a complaint with the data protection authority. Moreover, where the data protection authority observes any violation by a data controller of any of the provisions of a data protection law, it may initiate action against such data controller on a *suo motu* basis.

4. The data protection authority may be conferred with the power to appoint an adjudicating officer who may have the requisite qualifications and expertise to inquire into the facts of the complaint and adjudicate accordingly.

[842] Sections 73 and 74, POPI Act.
[843] Section 76(3), POPI Act.
[844] Section 79, POPI Act.
[845] Section 92, POPI Act.
[846] Section 95, POPI Act.
[847] Section 109, POPI Act.
[848] Section 97, POPI Act.

5. Given that the Appellate Tribunal has already been provided with the mandate to hear appeals from adjudicating officers under the IT Act, it may be worthwhile to propose the Appellate Tribunal as an appellate forum for any decision passed by a data protection authority. This, of course, will be subject to suitable amendments to the TRAI Act along with the constitution of specialised benches having the requisite technical knowledge and expertise as required to achieve this purpose.

6. In addition to the powers described in the previous section on ôData Protection Authorityô (Part IV, Chapter 2 of the White Paper), the data protection authority may be given the power to impose civil penalties as well as order the defaulting party to pay compensation.

7. Specifically, in case of compensation claims, the consumer fora set up under the Consumer Protection Act, 1986 (COPRA) typically act as avenues for filing such claims. However, it is relevant to note that given the vast number of data controllers operating in the Indian market and the number of potential data protection violation claims that may be brought by individuals, the consumer fora, especially at the district and state levels, may not have the requisite capacity as well as the technical knowledge and expertise to adjudicate on compensation claims arising from such violations. Moreover, if all compensation claims lie with the consumer fora, it may not incentivise individuals to file complaints with the data protection authority for enforcement and instead file claims relating to compensation with the consumer fora.

8. Consequently, it may be proposed that matters in which compensation claims for injury or damage does not exceed a prescribed threshold, may lie with the data protection authority. Further, an appeal from an order of the data protection authority granting such compensation and matters in which compensation claims for injury or damage exceeds such threshold may lie with the National Commission Disputes Redressal Commission (National Commission). This may be undertaken pursuant to requisite amendments to the COPRA and by setting up benches with the requisite technical skills and expertise.

3.5 Questions

1. What are your views on the above?

2. Should the data protection authority have the power to hear and adjudicate complaints from individuals whose data protection rights have been violated?

3. Where the data protection authority is given the power to adjudicate complaints from individuals, what should be the qualifications and expertise of the adjudicating officer appointed by the data protection authority to hear such matters?

4. Should appeals from a decision of the adjudicating officer lie with an existing appellate forum, such as, the Appellate Tribunal (TDSAT)?

5. If not the Appellate Tribunal, then what should be the constitution of the appellate authority?

6. What are the instances where the appellate authority should be conferred with original jurisdiction? For instance, adjudication of disputes arising between two or more data controllers, or between a data controller and a group of individuals, or between two or more individuals.

7. How can digital mechanisms of adjudication and redressal (e.g. e-filing, video conferencing etc.) be incorporated in the proposed framework?

8. Should the data protection authority be given the power to grant compensation to an individual?

9. Should there be a cap (e.g. up to Rs. 5 crores) on the amount of compensation which may be granted by the data protection authority? What should be this cap?

10. Can an appeal from an order of the data protection authority granting compensation lie with the National Consumer Disputes Redressal Commission?

11. Should any claim for compensation lie with the district commissions and/or the state commissions set under the COPRA at any stage?

12. In cases where compensation claimed by an individual exceeds the prescribed cap, should compensation claim lie directly with the National Consumer Disputes Redressal Commission?

13. Should class action suits be permitted?

14. How can judicial capacity be assessed? Would conducting judicial impact assessments be useful in this regard?

15. Are there any alternative views other than the ones mentioned above?

CHAPTER 4: REMEDIES

A. PENALTIES

In the context of a data protection law, civil penalties may be calculated in a manner to ensure that the quantum of civil penalty imposed not only acts as a sanction but also acts as a deterrence to data controllers, which have violated their obligations under a data protection law.

4.1 Issues

The IT Act does not appear to prescribe civil penalty provisions specifically for violation of data protection obligations.[849] The provisions of the IT Act are limited in their applicability and do not appear to take into account the wide range of instances of data protection violation which may occur due to advancement in technology used towards processing of personal data. Moreover, the quantum of penalty prescribed under the provisions of the IT Act appear to be inadequate and may not act as a deterrence to emerging e-commerce and other technology based players in India. Therefore, the critical issue in relation to civil penalties under a data protection legal framework pertains to the manner in which such penalties may be determined or calculated and the quantum of such penalties which may act as adequate deterrence.

4.2 International Practices

European Union

The EU GDPR mandates that the administrative fines imposed by a supervisory authority in each individual case must be effective, proportionate and dissuasive.[850] For specific violations, the EU GDPR prescribes an administrative fine of up to EUR 20,000,000, or in the case of an undertaking, up to four percent of the total worldwide turnover of the preceding financial year, whichever is higher. [851] In other words, administrative penalty that may be imposed on a data controller under the EU GDPR is linked to the total worldwide turnover of the preceding financial year of the defaulting data controller.

[849] Under the IT Act, civil penalty provisions are limited to instances where any person fails to furnish any document, return or report, or fails to maintain books of accounts or records as may be prescribed (Section 44, IT Act). Moreover, there is a residuary penalty clause which is applicable to instances for which no separate penalty is prescribed and limits the amount of penalty leviable to a maximum of Rs.25,000 (Section 45, IT Act). It may be noted that the IT Act prescribes fines (along with imprisonment) for offences involving breach of privacy and confidentiality under Section 72 and disclosure without consent or in breach of lawful contract under Section 72A.

[850] Article 83(1), EU GDPR.

[851] Per Article 83(5), EU GDPR, this includes instances where the data controller or data processor has infringed the basic principles for processing (including conditions for consent), data subjectsô rights, and transfer of personal data to a recipient in a third country or an international organization pursuant to Articles 44-49, EU GDPR. Similar administrative fine is also prescribed where the data controller or data processor does not comply with an order of the supervisory authority. Moreover, for certain other types of infringements, Article 83(4) of the EU GDPR prescribes an administrative fine of up to EUR 10,000,000, or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

Given that only an upper limit is prescribed in relation to the quantum of administrative penalty that may be imposed on a data controller or data processor, the EU GDPR further stipulates the criteria that a supervisory authority may consider while determining the quantum of such administrative penalties. These factors include[852]:

(i) the nature, gravity and duration of the infringement taking into account the nature, scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;

(ii) the intentional or negligent character of the infringement;

(iii) any action taken by the data controller or data processor to mitigate the damage suffered by the data subjects;

(iv) the degree of responsibility of the data controller or data processor taking into account the technical and organizational measures implemented by them; and

(v) any relevant previous infringement by the data controller or data processor.

It is pertinent to note that the obligations set out under the EU GDPR are also applicable where public authorities/government bodies are acting as data controllers or data processors. However, the EU GDPR mandates each Member State to lay down rules on whether and to what extent administrative fines may be imposed on such public authorities and bodies.[853]

United Kingdom

Under the UK DPA, the Information Commissioner has the power to impose monetary penalty up to the prescribed amount upon the data controller in case of a serious contravention of the data protection principles set out under the UK DPA.[854] The Information Commissioner must be satisfied that the contravention was of a kind likely to cause substantial damage or substantial distress, and either (i) the contravention was deliberate or (ii) the data controller knew or ought to have known that there was a risk that the contravention would occur and that such a contravention would be of a kind likely to cause substantial damage or substantial distress but failed to take reasonable steps to prevent the contravention.[855] The Information Commissioner is also required to take into account the

[852] Article 83(2), EU GDPR.
[853] Article 83(7), EU GDPR.
[854] Sections 55A-55E, UK DPA. The amount of the monetary penalty determined by the Information Commissioner cannot exceed GBP 500,000. The monetary penalty imposed must be sufficiently meaningful to act both as a sanction and also as a deterrent to prevent non-compliance of similar seriousness in the future by the contravening person and by others. *See* ICO, ñInformation Commissionerôs guidance about the issue of monetary penalties prepared and issued under section 55C(1) of the Data Protection Act 1998ò, 3 (December 2015), available at: https://ico.org.uk/media/for-organisations/documents/1043720/ico-guidance-on-monetary-penalties.pdf, (last accessed 20 October 2017).
[855] Section 55A, UK DPA.

sector, size, financial and other resources of a data controller as the purpose of a monetary penalty is not to impose undue financial hardship on an otherwise responsible entity.[856]

Australia

As per the Privacy Act, the OAIC may apply to the prescribed court for an order that an entity which has infringed any provisions of the Privacy Act shall be liable to pay a pecuniary penalty.[857] If the court is satisfied that the entity has contravened certain provisions of the Privacy Act, then it may order the entity to pay a pecuniary penalty as it determines.[858]

South Africa

Under the POPI Act[859], an administrative fine not exceeding R10 million may be imposed on the defaulting organization. Moreover, while determining an appropriate fine, the Information Regulator may consider the following factors:

(i) nature of personal information involved;

(ii) duration and extent of contravention;

(iii) number of data subjects affected or potentially affected by such contravention;

(iv) likelihood of substantial distress or damage, including injury to feelings or anxiety suffered by data subjects;

(v) whether the responsible party could have prevented the contravention from occurring; and

(vi) failure to carry out risk assessment or a failure to operate good policies, procedures and practices to protect personal information.

4.3 Provisional Views

1. Based on a review of the extant Indian legal and regulatory framework as well as the international best practices set out above, the following models for calculation of civil penalties may be possible:

---

[856] ICO, ñInformation Commissionerôs guidance about the issue of monetary penalties prepared and issued under section 55C(1) of the Data Protection Act 1998ò, 3 (December 2015), available at: https://ico.org.uk/media/for-organisations/documents/1043720/ico-guidance-on-monetary-penalties.pdf, (last accessed 20 October 2017).
[857] Section 80W, Part VIB, Privacy Act.
[858] From a reading of Section 80W(5), Privacy Act, it appears that the pecuniary penalty is capped at five times the amount stipulated for violation of a specific provision under the Privacy Act, in case of a body corporate and otherwise, it is the amount of pecuniary penalty contemplated for violation of a specific provision under the Privacy Act.
[859] Section 109, POPI Act.

(i) Per day basis

A data protection law may stipulate that for a violation of a data protection obligation, a civil penalty of a specific amount may be imposed on the data controller for each day such violation continues, which may or may not be subject to an upper limit.[860] An upper limit may be a fixed amount or may be linked to a variable parameter, such as, a percentage of the annual turnover of the defaulting data controller.

(ii) Discretion of adjudicating body subject to a fixed upper limit

A data protection law may stipulate that for a violation of a data protection obligation, an adjudicating authority may decide the quantum of civil penalty leviable subject always to a fixed upper limit as prescribed under applicable law. This model of penalty determination is common to the Indian context[861] and appears to be so from an international perspective as well.

(iii) Discretion of adjudicating body subject to an upper limit linked to a variable parameter

A data protection law may stipulate that for a violation of a data protection obligation, an adjudicating authority may decide the quantum of civil penalty leviable subject always to an upper limit which is linked to a variable parameter. There are instances in Indian law where such a standard has been adopted.[862] In the context of a data protection law, the EU GDPR adopts a similar standard and sets the upper limit of a civil penalty that may be imposed on a defaulting data controller as a percentage of the total worldwide turnover of the preceding financial year of the defaulting data controller.

2. In relation to the penalty models set out above, it may be relevant to note that while civil penalty leviable on a daily basis (i.e., model (i)) may act as a deterrent, it may lead

[860] In the Indian context, typically, per day civil penalty that may be leviable is capped to an upper limit. For instance, Section 91(2), Companies Act, 2013 provides that civil penalty for closure of register of members or debenture holders without prescribed notice is Rs. 5,000 for every day of such violation subject to a maximum of Rs. 1 lakh. Similarly, per Section 15C, SEBI Act, if any listed company or any registered intermediary fails to redress grievances of investors within the prescribed time, then such company or intermediary shall be liable to penalty which not be less than Rs. 1 lakh but which may extend to Rs. 1 lakh for each day during which such failure continues subject to a maximum of Rs. 1 crore. However, there are instances in the IT Act, such as, Section 44(b) (as cited above) which prescribes a per day civil penalty of Rs. 5,000 which is not capped.

[861] For instance, per Section 105, Insurance Act, 1938, if any director, managing director, manager or other officer or employee of an insurer wrongfully obtains possession of any property or wrongfully applies to any purposes of the said Act, then such person shall be liable to a penalty not exceeding Rs. 1 crore. Further, per Section 50, Food Safety and Standards Act, 2006, any person who sells to the purchaserôs prejudice any food which is not in compliance with the provisions of the FSSA or of the nature, substance or quality demanded by the purchaser shall be liable to a penalty not exceeding Rs. 5 lakhs.

[862] For instance, per Section 15G, SEBI Act, the penalty for insider trading is provided as a minimum of Rs. 10 lakhs which may extend to Rs. 25 crores or three times the amounts of profit made out of insider trading, whichever is higher. Similarly, under Section 27, Competition Act, 2002, where after any enquiry, it is found that any agreement or action of an enterprise in a dominant position is in contravention of Sections 3 or 4, as the case may be, a penalty may be imposed which shall not be more than 10% of the average of the turnover for the last three preceding financial years upon each of such person or enterprise which are parties to such agreement or abuse.

to an overly adverse impact on small data controllers/ start-up entities who are in the process of setting up businesses or may be in their teething period. In such a case, a per day civil penalty may not be feasible and the quantum of penalty that may be imposed may be left to the discretion of an adjudicating body subject to an upper limit, where such an upper limit may be a fixed amount or may be linked to a variable parameter, such as, a percentage of the annual turnover of the defaulting data controller

3. Where models (ii) or (iii) are proposed to be adopted, it may leave sufficient room for discretion on the part of the adjudicating authority. Consequently, it may be necessary to set out the factors that an adjudicating authority may consider while determining the appropriate quantum of civil penalty that may be imposed. This may include, nature and extent of violation of the data protection obligation, nature of personal information involved, number of individuals affected, whether infringement was intentional or negligent, measures taken by data controller to mitigate the damage suffered and previous track record of the data controller in this regard.

4. To ensure that civil penalty imposed constitutes adequate deterrence, any of the above models or a combination thereof may be adopted. An upper limit of civil penalty which may be linked to the total worldwide turnover of the defaulting party, as is the case under the EU GDPR, brings within its ambit those data controllers which handle large volumes of personal data, or who have a high turnover due to their data processing operations, or whose operations involve the use of new technology for processing and therefore may have a higher likelihood of causing harms to individuals.

5. Consequently, the highest form of deterrence in relation to civil penalties may be where a per day civil penalty is imposed subject to a fixed upper limit or a percentage of the total worldwide turnover of the defaulting data controller of the previous financial year, whichever is higher.

4.4 Questions

1. What are your views on the above?

2. What are the different types of data protection violations for which a civil penalty may be prescribed?

3. Should the standard adopted by an adjudicating authority while determining liability of a data controller for a data protection breach be strict liability? Should strict liability of a data controller instead be stipulated only where data protection breach occurs while processing sensitive personal data?

4. In view of the above models, how should civil penalties be determined or calculated for a data protection framework?

5. Should civil penalties be linked to a certain percentage of the total worldwide turnover of the defaulting data controller (of the preceding financial year as in EU GDPR) or should it be a fixed upper limit prescribed under law?

6. Should the turnover (referred to in the above question) be the worldwide turnover (of preceding financial year) or the turnover linked to the processing activity pursuant to a data protection breach?

7. Where civil penalties are proposed to be linked to a percentage of the worldwide turnover (of the preceding financial year) of the defaulting data controller, what should be the value of such percentage? Should it be prescribed under the law or should it be determined by the adjudicating authority?

8. Should limit of civil penalty imposed vary for different categories of data controllers (where such data controllers are categorised based on the volume of personal data processed, high turnover due to data processing operations, or use of new technology for processing)?

9. Depending on the civil penalty model proposed to be adopted, what type of factors should be considered by an adjudicating body while determining the quantum of civil penalty to be imposed?

10. Should there be a provision for blocking market access of a defaulting data controller in case of non-payment of penalty? What would be the implications of such a measure?

11. Are there any alternative views on penalties other than the ones mentioned above?

B. COMPENSATION

Awarding of compensation constitutes an important remedy where an individual has incurred a loss or damage as a result of a data controllerôs failure to comply with the data protection principles as set out under law.

4.5 Issues

The IT Act, albeit in a limited manner, in Section 43A, recognizes the right of an individual to claim compensation in case of a failure to protect sensitive personal data. Section 43A of the IT Act specifically stipulates that where a body corporate possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates is negligent in implementing and maintaining reasonable security practices and procedures[863] and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.[864]

Moreover, while adjudging the quantum of compensation payable under the IT Act, the adjudicating officer shall have due regard to the following factors, namely:[865]

(i) the amount of gain of unfair advantage, wherever quantifiable, made as a result of the default;

(ii) the amount of loss caused to any person as a result of the default; and

(iii) the repetitive nature of the default.

From a plain reading of the above, it follows that Section 43A of the IT Act is triggered in cases of negligence in maintaining and implementing reasonable security practices and procedures and that such negligence has caused a wrongful loss or wrongful gain[866] to any person.

---

[863] As per Section 43A, IT Act, órreasonable security practices and proceduresô may be specified in an agreement between the parties or may be specified under law or in the absence of such agreement or any law, such reasonable security practices and procedures as may be prescribed by the central government in consultation with such professional bodies or associations as it may deem fit.

[864] It is relevant to note that under Section 43, IT Act, if any person without the permission of the owner or any other person who is in charge of a computer, computer system or computer network accesses or secures access to such computer, computer system or computer network, downloads, copies or extracts any data or information from the same, or provides any assistance to any person to facilitate access to the same in contravention to the provisions of the IT Act shall be liable to pay damages by way of compensation to the person so affected.

[865] Section 47, IT Act.

[866] While there is no specific definition of the terms órwrongful lossô or órwrongful gainô under the IT Act, reliance may be placed on Section 23, IPC which states as follows:

ñ*ìWrongful gainî is gain by unlawful means of property to which the person gaining is not legally entitled. ìWrongful lossî.ñìWrongful lossî is the loss by unlawful means of property to which the person losing it is legally entitled.*ò

Compensation as a remedy as stipulated under Section 43A of the IT Act appears to be rather limited in its nature and scope.[867] In this regard, it is relevant to note that first, this provision is applicable only where a body corporate[868] fails to maintain and implement reasonable security practices and procedures. Consequently, Section 43A of the IT Act does not appear to impose any liability to pay compensation on a government body/public authority in case of breach of data protection obligations by such entities.

Second, Section 43A of the IT Act appears to be applicable only when a body corporate has failed to maintain reasonable security practices and procedures as provided in an agreement between the parties concerned or as may be specified under any law for the time being in force, i.e., the SPDI Rules. It is unclear whether ñreasonable security practices and proceduresò referred to in Section 43A of the IT Act includes the various obligations under the SPDI Rules or only the security practices and procedures specified in Rule 8 of the SPDI Rules.[869] Concomitantly, even where one or more other obligations under the IT Act is breached but there is no gain or loss in financial terms, Section 43A of the IT Act would not be attracted.[870]

4.6 International Practices

European Union

Under the EU GDPR[871], an individual who has suffered ñmaterial or non-materialò damage as a result of the infringement of the EU GDPR shall have the right to receive compensation from the data controller or data processor for the damage suffered. It has been specified that a data controller shall be liable for the damage caused by processing which infringes the EU GDPR and that a data processor shall only be liable where it has acted in violation of any obligation specifically applicable to data processors or has acted outside or contrary to any lawful instruction provided by the data controller. Further, court proceedings for exercising the right to receive compensation shall be brought before the competent courts in the Member States.

---

[867] The use of Section 43A, IT Act appears to be rather limited. A majority of the jurisprudence in this regard appears to stem from orders passed by adjudicating officer in Maharashtra where cases pertain to fraudulent transactions from bank accounts on account of failure to maintain reasonable security practices and compensation may range from Rs. 5,000 to Rs. 40 lakhs. *See* Sreenidhi Srinivasan and Namrata Mukherjee, ôBuilding An Effective Data Protection Regimeõ, Vidhi Centre For Legal Policy 19 (January 2017) and *also see Chander Kalani & Anr. v. State Bank of India & Ors.*, Complaint No. 1 of 2014, Adjudicating Officer (Maharashtra) Order dated 12 January 2015, available at: https://it.maharashtra.gov.in/Site/Upload/ACT/DIT_Adjudication_Chander%20Kalani_Vs_SBI_Ors-12012015.PDF, (last accessed 21 November 2017) and *Amit Dilip Patwardhan v. Bank of Baroda*, Complaint No. 15 of 2013, Adjudicating Officer (Maharashtra) Order dated 30 December 2013, available at: https://it.maharashtra.gov.in/Site/Upload/ACT/DIT_Adjudicaton_AmitPatwardhan_Vs_BankOfBaroda-30122013.PDF, (last accessed 21 November 2017).

[868] Explanation (i) to Section 43A, IT Act defines ñbody corporateò as any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities.

[869] Sreenidhi Srinivasan and Namrata Mukherjee, ôBuilding An Effective Data Protection Regimeõ, Vidhi Centre For Legal Policy 19 (January 2017).

[870] Sreenidhi Srinivasan and Namrata Mukherjee, ôBuilding An Effective Data Protection Regimeõ, Vidhi Centre For Legal Policy 19 (January 2017).

[871] Article 82, EU GDPR.

United Kingdom

As per the guidance[872] issued by the ICO, if an individual suffers damage where a data controller has breached the provisions of the UK DPA, the individual is entitled to claim compensation from the data controller. If an individual claims a certain amount as compensation, she will be required to demonstrate how the data controllerôs failure to comply with the UK DPA has resulted in her incurring that amount of damage or loss. This right can only be enforced through the courts. Moreover, a claim for compensation may be defended on the basis that the data controller took reasonable care in the circumstances to avoid breach. However, there are no guidelines on the level of compensation to be payable in this regard.

Australia

Under the Privacy Act, if the OAIC, upon investigation makes a finding of substantiated complaint that the organization has engaged in conduct that amounts to an interference with privacy, then the OAIC may, *inter alia*, declare that the complainant is entitled to a specified amount by way of compensation for any loss or damage suffered by reason of the act or practice which forms the subject matter of the complaint.[873] Further, any loss or damage as referred above includes injury to the feelings of the individual and humiliation suffered by the individual.[874] However, a determination made by the OAIC above is not binding or conclusive between the parties to the determination and separate proceedings are required to be initiated by the individual or the OAIC to enforce the latterôs determination.[875]

Canada

Under PIPEDA, the court (to which the complainant has applied for hearing in respect of any matter in respect of which complaint was made to the Privacy Commissioner) may, *inter alia*, award damages to the complainant including damages for any humiliation that the complainant has suffered.[876]

South Africa

Under the POPI Act, a data subject or on the request of the data subject, the Information Regulator may institute a civil action for damages in a court having jurisdiction against the responsible organization for breach of the provisions of the POPI Act, whether or not there was intent or negligence on the part of the responsible party. The court may award payment which is just and equitable, including payment of damages as compensation for patrimonial

[872] ICO, ócompensationô available at https://ico.org.uk/for-organisations/guide-to-data-protection/principle-6-rights/compensation/ (last accessed 20 October 2017).
[873] Section 52, Privacy Act.
[874] Section 52(1AB), Privacy Act.
[875] Section 52(IB), Privacy Act.
[876] Section 16(c), PIPEDA.

and non-patrimonial loss suffered by the data subject, aggravated damages, interest and cost of suit on such scale as may be determined by the court.[877]

4.7 Provisional Views

1. An individual may be given the right to seek compensation from a data controller in case she has suffered any loss or damage due to a violation of the data controllerôs obligations under a data protection legal framework.

2. A claim for compensation may be filed in accordance with the provisions set out in the previous chapter on óAdjudication Processô (Part IV, Chapter 3 of the White Paper).

3. It may be considered whether an obligation should be cast upon a data controller to grant compensation on its own to an individual upon detection of significant harm caused to such individual due to violation of data protection rules by such data controller (without the individual taking recourse to the adjudicatory mechanism).

4.8 Questions

1. What is the nature, type and extent of loss or damage suffered by an individual in relation to which she may seek compensation under a data protection legal regime?

2. What are the factors and guidelines that may be considered while calculating compensation for breach of data protection obligations?

3. What are the mitigating circumstances (in relation to the defaulting party) that may be considered while calculating compensation for breach of data protection obligations?

4. Should there be an obligation cast upon a data controller to grant compensation on its own to an individual upon detection of significant harm caused to such individual due to data protection breach by such data controller (without the individual taking recourse to the adjudicatory mechanism)? What should constitute significant harm?

5. Are there any alternative views other than the ones mentioned above?

[877] Section 99, POPI Act.

C. OFFENCES

There are certain types of breaches of data protection obligations, which, by their very nature and the impact they create, are extremely serious and may cause significant harm to individuals. In these instances, it may be imperative to prescribe criminal sanctions in the form of punishment and severe fines on the data controller.

4.9 Issues

The IT Act deals extensively with several types of offences or cybercrimes and prescribes penalty in the form of fines or imprisonment or both.[878] Specifically in the context of data protection, Sections 72[879] and 72A[880] of the IT Act offer some redress. Section 72 of the IT Act is limited in scope as it prescribes a penalty only against those persons who have been given the power under the IT Act or the rules and regulations made thereunder to access any electronic resource. As such, it may be limited to functionaries who have been granted specific powers under the provisions of the IT Act.[881] Section 72A of the IT Act is broader in scope as it imposes a penalty on any person, whether a private or public entity, for the disclosure of personal information without the consent of the person concerned. However, Section 72A of the IT Act is triggered only in those instances where the person (who has disclosed the personal information) has secured access to such personal information while providing services under the terms of a lawful contract.

Rapid growth of technological advancements which may be utilised towards processing of personal information increases the risk of data protection violations. Consequently, provisions in a data protection legal framework may be required to carefully set out criminal liability in cases of data protection violation. Moreover, criminal sanction in the form of imprisonment and fines may be prescribed to ensure that it adversely affects the data controller financially and reputationally thereby serving some deterrent value.

---

[878] This includes Section 65 (tampering with computer source documents), Section 66 (computer related offences), Section 66B (punishment for dishonestly receiving stolen computer resource or communication device), Section 66C (punishment for identity theft), Section 66D (punishment for cheating by personation by using computer resource), Section 66E (punishment for violation of privacy), Section 66F (punishment for cyber terrorism) and Section 67 (punishment for publishing or transmitting obscene material in electronic form).

[879] Section 72, IT Act provides as follows:

ñ*Save as otherwise provided in this Act or any other law for the time being in force, if any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.*ò

[880] Section 72A, IT Act provides as follows:

ñ*Save as otherwise provided in this Act or any other law for the time being in force, any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person, shall be punished with imprisonment for a term which may extend to three years, or with fine which may extend to five lakh rupees, or with both.*ò

[881] Apar Gupta, Commentary on Information Technology Act, 269 (Lexis Nexis, 2013).

4.10 International Practices

European Union

Under the EU GDPR, it appears that Member States shall have the discretion to decide rules in relation to criminal sanctions for infringements of the EU GDPR.[882]

United Kingdom

The UK DPA makes it an offence for a person who either knowingly or recklessly without the consent of the data controller obtains or discloses personal data or the information contained in the personal data, or procures the disclosure to another person of the information contained in the personal data.[883]

Australia

Under the Privacy Act, a person commits an offence if personal information (that relates to another individual) is disclosed to her and such person subsequently discloses the personal information.[884]

Canada

Under PIPEDA[885], every person who knowingly contravenes, *inter alia*, Section 8(8)[886] of the PIPEDA is guilty of an offence punishable on summary conviction and liable to a fine not exceeding CAD10,000, or an indictable offence and liable to a fine not exceeding CAD100,000.

South Africa

Under the POPI Act, fine or imprisonment (for a period not exceeding 10 years) or both for certain types of offences[887] and fine or imprisonment (for a period not exceeding 12 months) or both for certain other types of violations[888] of the POPI Act has been prescribed.[889]

---

[882] Lucy Lyons, "Enforcement and sanctions under the GDPR", Taylor Wessing (April 2016) available at: https://www.taylorwessing.com/globaldatahub/article-enforcement-sanctions-under-gdpr.html, (last accessed 20 October 2017). Please note that as per Article 84, EU GDPR, Member States may lay down rules on other penalties applicable to infringements of the EU GDPR, especially those infringements, which are not subject to administrative fines.

[883] Section 55, UK DPA. Per Section 60 of the UK DPA, a fine capped at a particular amount is prescribed as penalty.

[884] Section 80Q, Privacy Act. The penalty is 60 penalty units or imprisonment for one year or both.

[885] Section 28, PIPEDA.

[886] Per Section 8(8), PIPEDA, an organization that has personal information that is the subject of a request shall retain the information for as long as is necessary to allow the individual to exhaust any recourse under the PIPEDA that she may have.

[887] For instance, for failure to comply with any enforcement notices (Section 103, POPI Act) or obstructing the functioning of the Information Regulator (Section 100, POPI Act).

4.11 Provisional Views

1. The law may treat certain actions of a data controller as an offence and impose criminal liability. This may include instances where any person recklessly obtains or discloses, sells, offers to sell or transfers personal data to a third party without adhering to relevant principles of the data protection law, particularly without the consent of the data subject.

2. The quantum of penalty and term of imprisonment prescribed may be enhanced as compared to the provisions of the IT Act.

3. A more stringent penalty may be prescribed where the data involved is sensitive personal data.

4. The power to investigate such an offence may lie with a police officer not below the rank of Inspector.[890]

4.12 Questions

1. What are the types of acts relating to the processing of personal data which may be considered as offences for which criminal liability may be triggered?

2. What are the penalties for unauthorised sharing of personal data to be imposed on the data controller as well as on the recipient of the data?

3. What is the quantum of fines and imprisonment that may be imposed in all cases?

4. Should a higher quantum of fine and imprisonment be prescribed where the data involved is sensitive personal data?

5. Who will investigate such offences?

6. Should a data protection law itself set out all relevant offences in relation to which criminal liability may be imposed on a data controller or should the extant IT Act be amended to reflect this?

7. Are there any alternative views other than the ones mentioned above?

---

[888] For instance, per Section 54, POPI Act, any person acting on behalf of or under the direction of the Information Regulator must treat as confidential the personal information which comes to his or her knowledge in the course of performing her official duties.
[889] Section 107, POPI Act.
[890] As reflected in Section 78, IT Act.

PART V
SUMMARY

Key Principles of a Data Protection Law

A data protection framework in India must be based on the following seven principles:

1. Technology agnosticism- The law must be technology agnostic. It must be flexible to take into account changing technologies and standards of compliance.

2. Holistic application- The law must apply to both private sector entities and government. Differential obligations may be carved out in the law for certain legitimate state aims.

3. Informed consent- Consent is an expression of human autonomy. For such expression to be genuine, it must be informed and meaningful. The law must ensure that consent meets the aforementioned criteria.

4. Data minimisation- Data that is processed ought to be minimal and necessary for the purposes for which such data is sought and other compatible purposes beneficial for the data subject.

5. Controller accountability- The data controller shall be held accountable for any processing of data, whether by itself or entities with whom it may have shared the data for processing.

6. Structured enforcement- Enforcement of the data protection framework must be by a high-powered statutory authority with sufficient capacity. This must coexist with appropriately decentralised enforcement mechanisms.

7. Deterrent penalties- Penalties on wrongful processing must be adequate to ensure deterrence.

In order to achieve these principles, the Committee requests your views on the White Paper. The key issues analysed in the White Paper and questions raised for consultation under each head are summarised below for convenience. We would be grateful if your answers are brief and targeted to the questions asked. Any other views on the subject will also be appreciated.

SCOPE AND EXEMPTIONS

1. Territorial and Personal Scope

The power of the State to prescribe and enforce laws is governed by the rules of jurisdiction in international law. Data protection laws challenge this traditional conception since a single act of processing could very easily occur across jurisdictions. In this context, it is necessary to determine the applicability of the proposed data protection law.

For a fuller discussion, see page 24 above.

Questions

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

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 the extra-territorial application of a data protection law in India , other than the ones considered above?

2. Other Issues of Scope

There are three issues of scope other than territorial application. These relate to the applicability of the law to data relating to juristic persons such as companies, differential application of the law to the private and the public sector, and retrospective application of the law.

For a fuller discussion, see page 30 above.

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 person; (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:

   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?

3. Definition of Personal Data

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. Thus, it is important to accurately define personal information or personal data which will trigger the application of the data protection law.

For a fuller discussion, see page 34 above.

Questions

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

2. For the purpose of a data protection law, should the term ópersonal dataô or ópersonal informationôbe used?

   Alternatives:

   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 óidentifiedô, óidentifiableô or óreasonably identifiableô 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 ópersonal dataô and ópersonal informationô, which have not been considered?

4. Definition of Sensitive Personal Data

While personal data refers to all information related to a personôs identity, there may be certain intimate matters in which there is a higher expectation of privacy. Such a category widely called ósensitive personal dataôrequires precise definition.

For a fuller discussion, see page 41 above.

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?

5. Definition of Processing

Data protection laws across jurisdictions have defined the term óprocessingô in various ways. It is important to formulate an inclusive definition of processing to identify all operations, which may be performed on personal data, and consequently be subject to the data protection law.

For a fuller discussion, see page 44 above.

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:

   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?

6. Definition of Data Controller and Processor

The obligations on entities in the data ecosystem must be clearly delineated. To this end a clear conceptual understanding of the accountability of different entities which control and process personal data must be evolved.

For a fuller discussion, see page 48 above.

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 ódata controllerô or should it additionally define ódata processorõ?

   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 ódata controllerô (entity that determines the purpose of collection of information) and attribute primary responsibility for privacy to it.
   c. Use the two concepts of ódata controllerôand ódata processorô(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 owner and making them accountable.
   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 or processors which have not been considered above?

7. Exemptions

A data controller may be exempted from certain obligations of a data protection law based on the nature and purpose of the processing activity eg. certain legitimate aims of the state. The scope of such exemptions, also recognised by the Supreme Court in *Puttaswamy* needs to be carefully formulated.

For a fuller discussion, see page 52 above.

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?

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 ódomesticô or ôhousehold purposeô 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 ójournalistô and ójournalistic purposeô 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 óliteraryô or óartisticô 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 the 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 ǵprevention of crimeôbe 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?

8. Cross Border Flow of Data

Given the advent of the Internet, huge quantities of personal data are regularly transferred across national borders. Providing strong rules to govern such data flows is vital for all entities in the data eco-system.

For a fuller discussion, see page 62 above.

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, 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 which have not been considered?

9. Data Localisation

Data localisation requires companies to store and process data on servers physically located within national borders. Several governments, driven by concerns over privacy, security, surveillance and law enforcement, have been enacting legislations that necessitate localisation of data. Localisation measures pose detrimental effects for companies may, harm Internet users, and fragment the global Internet.

For a fuller discussion, see page 69 above.

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?

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. These laws operate in various sectors, such as, the financial sector, health sector and the information technology sector. Consequently, such laws may need to be examined against a new data protection legal and regulatory framework as and when such framework comes into existence in India.

For a fuller discussion, see page 76 above.

Questions

Comments are invited from stakeholders on how each of these laws may need to be reconciled with the obligations for data processing introduced under a new data protection law.

GROUNDS OF PROCESSING, OBLIGATION ON ENTITIES AND INDIVIDUAL RIGHTS

1. Consent

Most jurisdictions treat consent as one of the grounds for processing of personal data. However, consent is often not meaningful or informed, which raises issues of the extent to which it genuinely expresses the autonomous choice of an individual. Thus, the validity of consent and its effectiveness needs to be closely examined.

For a fuller discussion, see page 78 above.

Questions

1. What are your views on relying on consent as a primary ground for processing personal data?

   Alternatives:

   a. Consent will be the primary ground for processing.
   b. Consent will be treated at par with other grounds for processing.
   c. Consent may not be a ground for processing.

2. What should be the conditions for valid consent? Should specific requirements such as ‘unambiguous’, ‘freely given’ etc. as in the EU GDPR be imposed? Would mandating such requirements be excessively onerous?

3. How can consent fatigue and multiplicity of notices be avoided? Are there any legal or technology-driven solutions to this?

4. Should different standards for consent be set out in law? Or should data controllers be allowed to make context-specific determinations?

5. Would having very stringent conditions for obtaining valid consent be detrimental to day-to-day business activities? How can this be avoided?

6. Are there any other views regarding consent which have not been explored above?

2. Child's Consent

It is estimated that globally, one in three Internet users is a child under the age of 18. Keeping in mind their vulnerability and increased exposure to risks online, a data protection law must sufficiently protect their interests.

For a fuller discussion, see page 85 above.

Questions

1. What are your views regarding the protection of a childôs personal data?

2. Should the data protection law have a provision specifically tailored towards protecting childrenôs personal data?

3. Should the law prescribe a certain age-bar, above which a child is considered to be capable of providing valid consent? If so, what would the cut-off age be?

4. Should the data protection law follow the South African approach and prohibit the processing of any personal data relating to a child, as long as she is below the age of 18, subject to narrow exceptions?

5. Should the data protection law follow the Australian approach, and the data controller be given the responsibility to determine whether the individual has the capacity to provide consent, on a case by case basis? Would this requirement be too onerous on the data controller? Would relying on the data controller to make this judgment sufficiently protect the child from the harm that could come from improper processing?

6. If a subjective test is used in determining whether a child is capable of providing valid consent, who would be responsible for conducting this test?

   Alternatives:

   a. The data protection authority
   b. The entity which collects the information
   c. This can be obviated by seeking parental consent

7. How can the requirement for parental consent be operationalised in practice? What are the safeguards which would be required?

8. Would a purpose-based restriction on the collection of personal data of a child be effective? For example, forbidding the collection of childrenôs data for marketing, advertising and tracking purposes?

9. Should general websites, i.e. those that are not directed towards providing services to a child, be exempt from having additional safeguards protecting the collection, use and disclosure of childrenôs data? What is the criteria for determining whether a website is intended for children or a general website?

10. Should data controllers have a higher onus of responsibility to demonstrate that they have obtained appropriate consent with respect to a child who is using their services? How will they have ñactual knowledgeò of such use?

11. Are there any alternative views on the manner in which the personal data of children may be protected at the time of processing?

3. **Notice**

Notice is an essential prerequisite to operationalise consent. However, concerns have been raised about notices being ineffective because of factors such as length, use of complex language, etc. Thus, the law needs to ensure that notices are effective, such that consent is meaningful.

For a fuller discussion, see page 92 above.

Questions

1. Should the law rely on the notice and choice mechanism for operationalising consent?

2. How can notices be made more comprehensible to individuals? Should government data controllers be obliged to post notices as to the manner in which they process personal data?

3. Should the effectiveness of notice be evaluated by incorporating mechanisms such as privacy impact assessments into the law?

4. Should the data protection law contain prescriptive provisions as to what information a privacy notice must contain and what it should look like?

   Alternatives:

   a. No form based requirement pertaining to a privacy notice should be prescribed by law.
   b. Form based requirements may be prescribed by sectoral regulators or by the data protection authority in consultation with sectoral regulators.

5. How can data controllers be incentivised to develop effective notices?

Alternatives:

a. Assigning a ódata trust scoreô.
b. Providing limited safe harbour from enforcement if certain conditions are met.

If a ódata trust scoreôis assigned, then who should be the body responsible for providing the score?

6. Would a consent dashboard be a feasible solution in order to allow individuals to easily gauge which data controllers have obtained their consent and where their personal data resides? Who would regulate the consent dashboard? Would it be maintained by a third party, or by a government entity?

7. Are there any other alternatives for making notice more effective, other than the ones considered above?

4. Other Grounds of Processing

It is widely recognised that consent may not be sufficient as the only ground for lawful processing of personal data. Several other grounds, broadly conforming to practical requirements and legitimate state aims, are incorporated in various jurisdictions. The nature and remit of such grounds requires determination in the Indian context.

For a fuller discussion, see page 99 above.

Questions

1. What are your views on including other grounds under which processing may be done?

2. What grounds of processing are necessary other than consent?

3. Should the data protection authority determine residuary grounds of collection and their lawfulness on a case-by-case basis? On what basis shall such determination take place?

Alternatives:

a. No residuary grounds need to be provided.
b. The data protection authority should lay down ólawful purposesô by means of a notification.
c. On a case-by-case basis, applications may be made to the data protection authority for determining lawfulness.
d. Determination of lawfulness may be done by the data controller subject to certain safeguards in the law.

4. Are there any alternative methods to be considered with respect to processing personal data without relying on consent?

5. **Purpose Specification and Use Limitation**

Purpose specification and use limitation are two cardinal principles in the OECD framework. The principles have two components- first, personal data must be collected for a specified purpose; second, once data is collected, it must not be processed further for a purpose that is not specified at the time of collection or in a manner incompatible with the purpose of collection. However the relevance of these principles in the world of modern technology has come under scrutiny, especially as future uses of personal data after collection cannot always be clearly ascertained. Its relevance for the Indian context will thus have to be assessed.

For a fuller discussion, see page 105 above.

Questions

1. What are your views on the relevance of purpose specification and use limitation principles?

2. How can the purpose specification and use limitation principles be modified to accommodate the advent of new technologies?

3. What is the test to determine whether a subsequent use of data is reasonably related to/ compatible with the initial purpose? Who is to make such determination?

4. What should the role of sectoral regulators be in the process of explicating standards for compliance with the law in relation to purpose specification and use limitation?

   Alternatives:

   a. The sectoral regulators may not be given any role and standards may be determined by the data protection authority.
   b. Additional/ higher standards may be prescribed by sectoral regulators over and above baseline standards prescribed by such authority.
   c. No baseline standards will be prescribed by the authority; the determination of standards is to be left to sectoral regulators.

5. Are there any other considerations with respect to purpose specification and use limitation principles which have not been explored above?

6. **Processing of sensitive personal data**

If ósensitive personal dataô is to be treated as a separate category, there is a concomitant need to identify grounds for its processing. These grounds will have to be narrower than grounds for general processing of personal data and reflect the higher expectations of privacy that individuals may have regarding intimate facets of their person.

For a fuller discussion, see page 111 above.

Questions

1. What are your views on how the processing of sensitive personal data should be done?

2. Given that countries within the EU have chosen specific categories of ñsensitive personal dataò, keeping in mind their unique socio-economic requirements, what categories of information should be included in Indiaôs data protection law in this category?

3. What additional safeguards should exist to prevent unlawful processing of sensitive personal data?

   Alternatives:

   a. Processing should be prohibited subject to narrow exceptions.
   b. Processing should be permitted on grounds which are narrower than grounds for processing all personal data.
   c. No general safeguards need to be prescribed. Such safeguards may be incorporated depending on context of collection, use and disclosure and possible harms that might ensue.
   d. No specific safeguards need to be prescribed but more stringent punishments can be provided for in case of harm caused by processing of sensitive personal information.

4. Should there be a provision within the law to have sector specific protections for sensitive data, such as a set of rules for handling health and medical information, another for handling financial information and so on to allow contextual determination of sensitivity?

5. Are there any alternative views on this which have not been discussed above?

7. Storage Limitation and Data Quality

Related to the principle of purpose specification is the principle of storage limitation which requires personal data to be erased or anonymised once the purpose for which such data was collected is complete. Personal data in the possession of data controllers should also be

accurate, complete and kept up-to-date. These principles cast certain obligations on data controllers. The extent of such obligations must be carefully determined.

For a fuller discussion, see page 117 above.

Questions

1. What are your views on the principles of storage limitation and data quality?

2. On whom should the primary onus of ensuring accuracy of data lie especially when consent is the basis of collection?

   Alternatives:

   a. The individual
   b. The entity collecting the data

3. How long should an organisation be permitted to store personal data? What happens upon completion of such time period?

   Alternatives:

   a. Data should be completely erased
   b. Data may be retained in anonymised form

4. If there are alternatives to a one-size-fits-all model of regulation (same rules applying to all types of entities and data being collected by them) what might those alternatives be?

5. Are there any other views relating to the concpets of storage limitation and data quality which have not been considered above?

8. Individual Participation Rights-1

One of the core principles of data privacy law is the ñindividual participation principleò which stipulates that the processing of personal data must be transparent to, and capable of being influenced by, the data subject. Intrinsic to this principle are the rights of confirmation, access, and rectification. Incorporation of such rights has to be balanced against technical, financial and operational challenges in implementation.

For a fuller discussion, see page 122 above.

Questions

1. What are your views in relation to the above?

2. Should there be a restriction on the categories of information that an individual should be entitled to when exercising their right to access?

3. What should be the scope of the right to rectification? Should it only extend to having inaccurate date rectified or should it include the right to move court to get an order to rectify, block, erase or destroy inaccurate data as is the case with the UK?

4. Should there be a fee imposed on exercising the right to access and rectify oneôs personal data?

   Alternatives:

   a. There should be no fee imposed.
   b. The data controller should be allowed to impose a reasonable fee.
   c. The data protection authority/sectoral regulators may prescribe a reasonable fee.

5. Should there be a fixed time period within which organisations must respond to such requests? If so, what should these be?

6. Is guaranteeing a right to access the logic behind automated decisions technically feasible? How should India approach this issue given the challenges associated with it?

7. What should be the exceptions to individual participation rights?
   [For instance, in the UK, a right to access can be refused if compliance with such a request will be impossible or involve a disproportionate effort. In case of South Africa and Australia, the exceptions vary depending on whether the organisation is a private body or a public body.]

8. Are there any other views on this, which have not been considered above?

9. **Individual Participation Rights-2**

In addition to confirmation, access and rectification, the EU GDPR has recognised other individual participation rights, viz. the right to object to processing (including for Direct marketing), the right not to be subject to a decision solely based on automated processing, the right to restrict processing, and the right to data portability. These rights are inchoate and some such as those related to Direct Marketing overlap with sectoral regulations. The suitability of incorporation of such rights must be assessed in light of their implementability in the Indian context.

For a fuller discussion, see page 129 above.

Questions

1. What are your views in relation on the above individual participation rights?

2. The EU GDPR introduces the right to restrict processing and the right to data portability. If India were to adopt these rights, what should be their scope?

3. Should there be a prohibition on evaluative decisions taken on the basis of automated decisions ?

   Alternatives:

   a. There should be a right to object to automated decisions as is the case with the UK.
   b. There should a prohibition on evaluative decisions based on automated decision-making.

4. Given the concerns related to automated decision making, including the feasibility of the right envisioned under the EU GDPR, how should India approach this issue in the law?

5. Should direct marketing be a discrete privacy principle, or should it be addressed via sector specific regulations?

6. Are there any alternative views in relation to the above which have not been considered?

10. Individual Participation Rights-3: Right to be forgotten

The right to be forgotten has emerged as one of the most emotive issues in data protection law. The decision of the European Court of Justice in the *Google Spain* case and the repeated reference to this right in *Puttaswamy* necessitates a closer look at its contours, scope and exceptions, particularly as it raises several vexed questions relating to the interface between free speech, privacy and the right to know.

For a fuller discussion, see page 137 above.

Questions

1. What are your views on the right to be forgotten having a place in Indiaôs data protection law?

2. Should the right to be forgotten be restricted to personal data that individuals have given out themselves?

3. Does a right to be forgotten add any additional protection to data subjects not already available in other individual participation rights?

4. Does a right to be forgotten entail prohibition on display/dissemination or the erasure of the information from the controllerôs possession?

5. Whether a case-to-case balancing of the data subjectôs rights with controller and public interests is a necessary approach for this right? Who should perform this balancing exercise? If the burden of balancing rests on the data controller as it does in the EU, is it fair to also impose large penalties if the said decision is deemed incorrect by a data protection authority or courts?

6. Whether special exemptions (such as the right to freedom of expression and information) are needed for this right? (over and above possible general exemptions such as national security, research purposes and journalistic or artistic expression)?

7. Are there any alternative views to this .

REGULATION AND ENFORCEMENT

1. Enforcement Models

Once the substantive obligations of a data protection law are formalised, provisions regarding enforcement must be structured so as to ensure compliance with substantive provisions. Effective enforcement requires the consideration of certain aspects of institutional design and overall approach before we can develop and align individual elements of the framework. This may be in terms of the extent of burden placed on entities covered under such framework, the structure and functions of any enforcement agency, or the tools at its disposal. Enforcement models consist of: (i) ócommand and controlô; (ii) self-regulation; and (iii) co-regulation.

For a fuller discussion, see page 143 above.

Questions

1. What are your views on the above described models of enforcement?

2. Does co-regulation seem an appropriate approach for a data protection enforcement mechanism in India?

3. What are the specific obligations/areas which may be envisaged under a data protection law in India for a (i) ócommand and controlô approach; (ii) self-regulation approach (if any); and (iii) co-regulation approach?

4. Are there any alternative views to this?

2. Accountability and Enforcement Tools

Accountability

A data protection law must reflect the principle of accountability. Accountability should not only be enforced for breach of data protection obligations through the adoption and implementation of standards by data controllers, but also in certain well defined circumstances, it could be extended to hold data controllers liable for the harms that they cause to individuals without further proof of violation of any other obligation. The data protection law should appropriately identify such harms for which the data controller should be held liable in this manner.

For a fuller discussion, see page 147 above.

Questions

1. What are your views on the use of the principle of accountability as stated above for data protection?

2. What are the organisational measures that should be adopted and implemented in order to demonstrate accountability? Who will determine the standards which such measures have to meet?

3. Should the lack of organisational measures be linked to liability for harm resulting from processing of personal data?

4. Should all data controllers who were involved in the processing that ultimately caused harm to the individual be accountable jointly and severally or should they be allowed mechanisms of indemnity and contractual affixation of liability inter se?

5. Should there be strict liability on the data controller, either generally, or in any specific categories of processing, when well-defined harms are caused as a result of data processing?

6. Should the data controllers be required by law to take out insurance policies to meet their liability on account of any processing which results in harm to data subjects? Should this be limited to certain data controllers or certain kinds of processing?

7. If the data protection law calls for accountability as a mechanism for protection of privacy, what would be impact on industry and other sectors?

8. Are there any other issues or concerns regarding accountability which have not been considered above?

Enforcement Tools

A number of regulatory tools and mechanisms may be simultaneously utilised to achieve different enforcement objectives such as flexibility and rigour in compliance. It needs to be determined which regulatory tools and mechanisms will find place in a data protection law for India.

A. Codes of Practice

For a fuller discussion, see page 157 above.

Questions

1. What are your views on this?

2. What are the subject matters for which codes of practice may be prepared?

3. What is the process by which such codes of conduct or practice may be prepared? Specifically, which stakeholders should be mandatorily consulted for issuing such a code of practice?

4. Who should issue such codes of conduct or practice?

5. How should such codes of conduct or practice be enforced?

6. What should be the consequences for violation of a code of conduct or practice?

7. Are there any alternative views?

B. Personal Data Breach Notification

The aggregation of data in the hands of public and private entities leaves them vulnerable to data breaches. Data breaches can take many forms including; hackers gaining access to data through a malicious attack; lost, stolen, or temporary misplaced equipment; employee negligence; and policy and/or system failure. It is important to identify these threats and establish processes to deal with these breaches.

For a fuller discussion, see page 161 above.

Questions

1. What are your views in relation to the above?

2. How should a personal data breach be defined?

3. When should personal data breach be notified to the authority and to the affected individuals?

4. What are the circumstances in which data breaches must be informed to individuals?

5. What details should an breach notification addressed to an individual contain?

6. Are there any alternative views in relation to the above, others than the ones discussed above?

C. Categorisation of Data Controllers

Given the complexity and breadth of application of a data protection law, it may be difficult for a regulator to effectively ensure compliance on the part of all data controllers. Further, a data protection law can entail heavy compliance burdens. As a result, it may be necessary,

both for principled and practical reasons to differentiate between data controllers, depending on factors that give rise to greater risks or threats to individual data protection rights.

For a fuller discussion, see page 167 above.

Questions

1. What are your views on the manner in which data controllers may be categorised?

2. Should a general classification of data controllers be made for the purposes of certain additional obligations facilitating compliance while mitigating risk?

3. Should data controllers be classified on the basis of the harm that they are likely to cause individuals through their data processing activities?

4. What are the factors on the basis of which such data controllers may be categorised?

5. What range of additional obligations can be considered for such data controllers?

6. Are there any alternative views other than the ones mentioned above?

Registration

1. Should there be a registration requirement for certain types of data controllers categorised on the basis of specified criteria as identified above? If yes, what should such criteria be; what should the registration process entail?

2. Are there any alternative views in relation to registration?

Data Protection Impact Assessment

1. What are your views on data controllers requiring DPIAs or Data Protection Impact Assessments?

2. What are the circumstances when DPIAs should be made mandatory?

3. Who should conduct the DPIA? In which circumstances should a DPIA be done (i) internally by the data controller; (ii) by an external professional qualified to do so; and (iii) by a data protection authority?

4. What are the circumstances in which a DPIA report should be made public?

5. Are there any alternative views on this?

Data Protection Audit

1. What are your views on incorporating a requirement to conduct data protection audits, within a data protection law?

2. Is there a need to make data protection audits mandatory for certain types of data controllers?

3. What aspects may be evaluated in case of such data audits?

4. Should data audits be undertaken internally by the data controller, a third party (external person/agency), or by a data protection authority?

5. Should independent external auditors be registered / empanelled with a data protection authority to maintain oversight of their independence?

6. What should be the qualifications of such external persons/agencies carrying out data audits?

7. Are there any alternative views on this?

Data Protection Officer

1. What are your views on a data controller appointing a DPO?

2. Should it be mandatory for certain categories of data controllers to designate particular officers as DPOs for the facilitation of compliance and coordination under a data protection legal framework?

3. What should be the qualifications and expertise of such a DPO?

4. What should be the functions and duties of a DPO?

5. Are there any alternative views?

D. Data Protection Authority

The effective enforcement of data protection law may necessitate a separate, independent regulatory authority. Such an authority may discharge the following types of functions, powers and duties: (i) Monitoring, enforcement and investigation; (ii) Standard-setting; and (iii) Awareness generation.

For a fuller discussion, see page 175 above.

Questions

1. What are your views on the above?

2. Is a separate, independent data protection authority required to ensure compliance with data protection laws in India?

3. Is there a possibility of conferring the function and power of enforcement of a data protection law on an existing body such as the Central Information Commission set up under the RTI Act?

4. What should be the composition of a data protection authority, especially given the fact that a data protection law may also extend to public authorities/government? What should be the qualifications of such members?

5. What is the estimated capacity of members and officials of a data protection authority in order to fulfil its functions? What is the methodology of such estimation?

6. How should the members of the authority be appointed? If a selection committee is constituted, who should its members be?

7. Considering that a single, centralised data protection authority may soon be over-burdened by the sheer quantum of requests/ complaints it may receive, should additional state level data protection authorities be set up? What would their jurisdiction be? What should be the constitution of such state level authorities?

8. How can the independence of the members of a data protection authority be ensured?

9. Can the data protection authority retain a proportion of the income from penalties/fines?

10. What should be the functions, duties and powers of a data protection authority?

11. With respect to standard-setting, who will set such standards? Will it be the data protection authority, in consultation with other entities, or should different sets of standards be set by different entities? Specifically, in this regard, what will be the interrelationship between the data protection authority and the government, if any?

12. Are there any alternative views other than the ones mentioned above?

3. **Adjudication Process**

Adjudication plays an integral role in enforcement of any law as it ascertains the rights and obligations of parties involved in a dispute and prescribes corrective actions and remedies. In the context of a data protection law, adjudication entails an assessment of whether and to

what extent data protection rights of an individual have been infringed by a data controller, the loss or damage suffered by the individual due to the said infringement, the remedies available to the individual as well as the penal consequences that the data controller may be liable for.

For a fuller discussion, see page 184 above.

Questions

1. What are your views in relation to an adjudication process envisaged under a data protection law in India?

2. Should the data protection authority have the power to hear and adjudicate complaints from individuals whose data protection rights have been violated?

3. Where the data protection authority is given the power to adjudicate complaints from individuals, what should be the qualifications and expertise of the adjudicating officer appointed by the data protection authority to hear such matters?

4. Should appeals from a decision of the adjudicating officer lie with an existing appellate forum, such as, the Appellate Tribunal (TDSAT)?

5. If not the Appellate Tribunal, then what should be the constitution of the appellate authority?

6. What are the instances where the appellate authority should be conferred with original jurisdiction? For instance, adjudication of disputes arising between two or more data controllers, or between a data controller and a group of individuals, or between two or more individuals.

7. How can digital mechanisms of adjudication and redressal (e.g. e-filing, video conferencing etc.) be incorporated in the proposed framework?

8. Should the data protection authority be given the power to grant compensation to an individual?

9. Should there be a cap (e.g. up to Rs. 5 crores) on the amount of compensation which may be granted by the data protection authority? What should be this cap?

10. Can an appeal from an order of the data protection authority granting compensation lie with the National Consumer Disputes Redressal Commission?

11. Should any claim for compensation lie with the district commissions and/or the state commissions set under the COPRA at any stage?

12. In cases where compensation claimed by an individual exceeds the prescribed cap, should compensation claim lie directly with the National Consumer Disputes Redressal Commission?

13. Should class action suits be permitted?

14. How can judicial capacity be assessed? Would conducting judicial impact assessments be useful in this regard?

15. Are there any alternative views other than the ones mentioned above?

4. Remedies

A. Penalties

In the context of a data protection law, civil penalties may be calculated in a manner so as to ensure that the quantum of civil penalty imposed not only acts as a sanction but also acts as a deterrence to data controllers, which have violated their obligations under a data protection law. Further, there may be three models (or a combination thereof) possible for the calculation of civil penalties, which are as follows:

(i) Per day basis;
(ii) Discretion of the adjudicating body subject to a fixed upper limit;
(iii) Discretion of adjudicating body subject to an upper limit linked to a variable parameter (such as a percentage of the total worldwide turnover of the preceding financial year of the defaulting data controller).

For a fuller discussion, see page 191 above.

Questions

1. What are your views on the above?

2. What are the different types of data protection violations for which a civil penalty may be prescribed?

3. Should the standard adopted by an adjudicating authority while determining liability of a data controller for a data protection breach be strict liability? Should strict liability of a data controller instead be stipulated only where data protection breach occurs while processing sensitive personal data?

4. In view of the above models, how should civil penalties be determined or calculated for a data protection framework?

5. Should civil penalties be linked to a certain percentage of the total worldwide turnover of the defaulting data controller (for the preceding financial year) or should it be a fixed upper limit prescribed under law?

6. Should the turnover (referred to in the above question) be the worldwide turnover (of preceding financial year) or the turnover linked to the processing activity pursuant to a data protection breach?

7. Where civil penalties are proposed to be linked to a percentage of the worldwide turnover (of the preceding financial year) of the defaulting data controller, what should be the value of such percentage? Should it be prescribed under the law or should it be determined by the adjudicating authority?

8. Should limit of civil penalty imposed vary for different categories of data controllers (where such data controllers are categorised based on the volume of personal data processed, high turnover due to data processing operations, or use of new technology for processing)?

9. Depending on the civil penalty model proposed to be adopted, what type of factors should be considered by an adjudicating body while determining the quantum of civil penalty to be imposed?

10. Should there be a provision for blocking market access of a defaulting data controller in case of non-payment of penalty? What would be the implications of such a measure?

11. Are there any alternative views on penalties other than the ones mentioned above?

B. Compensation

Awarding of compensation constitutes an important remedy where an individual has incurred a loss or damage as a result of a data controllerôs failure to comply with the data protection principles as set out under law.

For a fuller discussion, see page 197 above.

Questions

1. What is the nature, type and extent of loss or damage suffered by an individual in relation to which she may seek compensation under a data protection legal regime?

2. What are the factors and guidelines that may be considered while calculating compensation for breach of data protection obligations?

3. What are the mitigating circumstances (in relation to the defaulting party) that may be considered while calculating compensation for breach of data protection obligations?

4. Should there be an obligation cast upon a data controller to grant compensation on its own to an individual upon detection of significant harm caused to such individual due to data protection breach by such data controller (without the individual taking recourse to the adjudicatory mechanism)? What should constitute significant harm?

5. Are there any alternative views other than the ones mentioned above?

C. Offences

The law may treat certain actions of a data controller as an offence and impose a criminal liability. This may include instances where any person recklessly obtains or discloses, sells, offers to sell or transfers personal data to a third party without adhering to relevant principles of the data protection law, particularly without the consent of the data subject. It may be considered whether other acts should create criminal liability.

For a fuller discussion, see page 201 above.

Questions

1. What are the types of acts relating to the processing of personal data which may be considered as offences for which criminal liability may be triggered?

2. What are the penalties for unauthorised sharing of personal data to be imposed on the data controller as well as on the recipient of the data?

3. What is the quantum of fines and imprisonment that may be imposed in all cases?

4. Should a higher quantum of fine and imprisonment be prescribed where the data involved is sensitive personal data?

5. Who will investigate such offences?

6. Should a data protection law itself set out all relevant offences in relation to which criminal liability may be imposed on a data controller or should the extant IT Act be amended to reflect this?

7. Are there any alternative views other than the ones mentioned above?

****