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 individual's autonomy.[392] Allowing an individual to have autonomy over her personal information allows her to enjoy "informational privacy". Informational privacy may be broadly understood as the individual's ability to exercise control over the manner in which her information may be collected and used.[393] Second, consent provides a "morally transformative" value as it justifies conduct, which might otherwise be considered wrongful.[394] For instance, seeking consent is what differentiates entering someone's 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 individual's information.[396] Operationalising consent is done through the mechanism of "notice and choice". 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 individuals' data may be used.[397] Seeking consent allows the individual to be responsible for managing her own information, thereby resulting in "privacy self-management"[398].

---

[392] "In democratic societies, there is a fundamental belief in the uniqueness of the individual, in his basic dignity and worth…and in the need to maintain social processes that safeguard his sacred individuality." *See:* Alan Westin, 'Privacy and Freedom', (Atheneum, 1967).
[393] Adam Moore, 'Toward Informational Privacy Rights', 44 San Diego Law Review 809 (2007).
[394] John Kleinig, 'The Nature of Consent' in 'The Ethics of Consent- Theory and Practice', 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*., 'Privacy Harms and the Effectiveness of the Notice and Choice Framework', 11 Journal of Law and Policy for the Information Society, 485, 489, (2015).
[397] Ryan M. Calo, 'Against Notice Skepticism in Privacy (and Elsewhere)', 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, 'Privacy Self-management and the Consent Dilemma', 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 customer's 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, 'Privacy on the Line' (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 organisations' 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 "one-size fits all" model may not be sufficient. It may not be necessary to obtain 'express' consent for certain routine transactions, if these activities do not involve processing sensitive personal information. For routine, low-risk transactions, an individual's 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, 'Privacy Self-management and the Consent Dilemma', 126 Harvard Law Review 1880, 1881, (2013).

[401] Fred H. Cate, 'Failure of Fair Information Principles', in 'Consumer Protection in the Age of Information Economy', (Jane K. Winn *ed.*, Routledge, 2006).

[402] Article 29 Data Protection Working Party, 'Opinion 15/2011 on the Definition of Consent', 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, 'Beyond Consent: A New Paradigm for Data Protection- Discussion Document 2017-03', 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 "contracts of adhesion", where the terms of the notice only provide a "take it or leave it option". 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 "statement or by clear affirmative action". 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 "explicit". However, at present, the manner in which "explicit" consent will be translated into actual practice is not clear.

---

[404] Aleecia M. McDonald and Lorrie Faith Cranor, 'The Cost of Reading Privacy Policies', 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, 'Contract as a Thing', 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:
"*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.*"

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 Canada's PIPEDA, organisations are required to obtain an individual's 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 "graduated consent standard" or a "sliding-scale" for obtaining valid consent. The Digital Privacy Act stipulates that an individual's 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 agency's (government body) or the organisation's (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 individual's 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, 'Highlights of the Canada Digital Privacy Act', 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 entity's 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 consumer's 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 ‘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?

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 "digital age". To this effect, the United Nations Convention on the Rights of the Child (UN CRC) recognises children's rights to protection, including a specific protection against arbitrary or unlawful interference with children's 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 children's 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 children's 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 children's personal information.

2.2 Issues

[418] Sonia Livingstone *et al.*, 'One in Three: Internet Governance and Children's Rights', 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, 'Consent for Processing Children's personal data in the EU: Following in US footsteps?', 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] 'Children's data protection and parental consent: A best practice analysis to inform the EU data protection reform', 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 Opportunities', 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, 'Consent for Processing Children's personal data in the EU: Following in US footsteps?', 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.*, 'One in Three: Internet Governance and Children's Rights', 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, 'Sweep-Children's Privacy' (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 parent's 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 child's 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 parent's 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 parent's 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 child's consent generally with respect to data processing, though the form that the test will take in India's 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 children's 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 "children's website". 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 'non-commercial' 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 child's 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 "may be less aware of risks, consequences, safeguards and their rights in relation to the processing of personal data", especially online.[432] In situations where processing of personal

[426] Article 29 Data Protection Working Party, 'Opinion 15/2011 on the Definition of Consent', 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, 'Consent for Processing Children's personal data in the EU: Following in US footsteps?', 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 "information society services"[433] directly to children under the age of 16.[434] Lack of harmonised general rules on children's 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 "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services." 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, 'Australian Privacy Principles Guidelines: Privacy Act 1988' (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, 'Protection of Children's Privacy in Focus' (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 child's 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 Commissioner's 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 parents' 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, 'Guidelines on Privacy and Online Behavioural Advertising' (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, 'Guidelines for Online Consent' (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, 'Personal Information Online: Code of Practice' (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, 'Peers issue warning over legislation banning children from joining Facebook and Twitter until they are 13', 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 parent's 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 children's 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 child's personal data?

2. Should the data protection law have a provision specifically tailored towards protecting children's 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 children's 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 children's 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 "actual knowledge" 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 "notice and choice". 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 "I agree" 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 controller's 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 individual's 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, 'Against Notice Skepticism in Privacy (and Elsewhere)', 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, 'Against Notice Skepticism in Privacy (and Elsewhere)', 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, 'Against Notice Skepticism in Privacy (and Elsewhere)', 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 controller's 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, 'Privacy Self-management and the Consent Dilemma', 126 Harvard Law Review 1880, 1885, (2013).
[447] Florian Schaub *et al*., 'A Design Space for Effective Privacy Notices', 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, 'Failure of Fair Information Principles', in 'Consumer Protection in the Age of Information Economy', 343, 361-62, (Jane K. Winn *ed.*, Routledge, 2006) *citing* Helen Nissenbaum, 'Privacy in Context-Technology, Policy and the Integrity of Social Life' (Stanford University Press, 2010). (discussing a study that only about 20% people read privacy notices "most of the time").
[449] Daniel Solove, 'Privacy Self-management and the Consent Dilemma', 126 Harvard Law Review 1880, 1886, (2013).
[450] Daniel Solove, 'Privacy Self-management and the Consent Dilemma', 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 individual's 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 individual's information is no longer limited to websites and mobile applications. A host of "smart devices", such as fitness trackers, video game systems and speakers collect user's information on a continuous basis. Ordinarily, the privacy notices of such devices are decoupled from the device itself and are posted on the data controller's 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, 'The Cost of Reading Privacy Policies', 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*., 'Privacy Harms and the Effectiveness of the Notice and Choice Framework', 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, 'Privacy Self-management and the Consent Dilemma', 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 "notice" *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 "request for consent" (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 GDPR's 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 individuals' 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, 'Good and Bad Examples of Privacy Notices', 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, 'Privacy Notices, Transparency and Control', 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 "clearly expressed and up to date" 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, 'Guidelines for Online Consent'(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 "clear and conspicuous" 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 organisations' 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 "data trust score" (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 ‘consent dashboard’ 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 ‘data trust score’.
   b. Providing limited safe harbor from enforcement if certain conditions are met.

   If a ‘data trust score’ is 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 "lawful" 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 "public interest", "vital interest" and "legitimate interest".

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 "public interest", "vital interest" and "legitimate interest", 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 India's 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 subject's 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 subject's 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, '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).
[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, '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).

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 individual's 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, '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).
[475] 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).
[476] 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).
[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 "public interest ground" and the "legitimate interest" ground. As the EU GDPR's 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 DPA's 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, '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).
[479] 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).
[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 "reasonably necessary" for one or more of the entity's functions or activities. Determining whether a particular collection of personal information is permitted, involves a two-step process: identifying the entity's 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 customer's 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 "legitimate interest" 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 'lawful purposes' 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 individual's 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, 'Opinion 03/2013 on purpose limitation', 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, '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).
[487] Article 29 Data Protection Working Party, 'Opinion 03/2013 on purpose limitation', 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, '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).

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, 'Why Data Minimisation is an important concept in the age of Big Data', 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, 'Big Data for All: Privacy and User Control in the Age of Analytics', 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, 'Discussion Paper on Consent and Privacy' (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 "improving user experience", "IT-security purposes" 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 "specified, explicit and limited" 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, 'Opinion 03/2013 on purpose limitation', 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, 'Opinion 03/2013 on purpose limitation', 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, 'Opinion 03/2013 on purpose limitation', 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, 'Chapter 6: Australian Privacy Principle 6 — Use or disclosure of personal information' (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 individual's 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, 'Guide to Big Data and the Australian Privacy Principles- Consultation Draft', 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, 'Discussion Paper on Consent and Privacy' (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 individual's personality and being. They refer to certain characteristics that define one's essence as a human being and contribute to the individual's dignity, integrity, personal autonomy and independence.[509] These may include aspects such as individual's 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 individual's identity. The harms arise, of course, because information of the individual becomes available to others through a wide range of activities, collectively termed "data processing".[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 one's 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, 'Privacy as an Aspect of Human Dignity- An Answer to Dean Prosser', 36 New York University Law Review 962 (1964).
[510] Data Processing can be understood as "any 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 destruction", Article 4(2), EU GDPR.
[511] Edward J. Bloustein, 'Privacy as an Aspect of Human Dignity- An Answer to Dean Prosser', 36 New York University Law Review 962 (1964).
[512] Robert C Post, 'Three Concepts of Privacy' 89 Texas Law Review 2087 (2001), *citing* Jeffrey Rosen, 'The Unwanted Gaze: The Destruction of Privacy in America' (2000).

specific purposes and under special conditions.[513] Such types of data are termed "sensitive", 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 "sensitive data" 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 "sensitive personal information".[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 "body corporates" 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, 'Advice paper on special categories of data ("sensitive data")', 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 'sensitive personal data or information' 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, 'Comments on the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011', 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 "special categories of data", 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, "sensitive personal data" 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, 'GDPR Conundrums: Processing Special Categories of Data', 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 "special categories" 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 "sensitive" 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, 'Key Definitions of the Data Protection Act', 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 individual's- (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, '6. The Privacy Act: Some Important Definitions: Sensitive Information', 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 "sensitive data" in the US, several sector-specific laws and guidelines implement safeguards where it may be considered necessary. For instance the FTC's 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 "sensitive".[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 , 'FTC Staff Report: Self-Regulatory Principles for Online Behavioural Advertising' (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 , 'FTC Staff Revises Online Behavioural Advertising Principles' (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 "sensitive" 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 India's 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 "sensitive personal data", keeping in mind their unique socio-economic requirements, what categories of information should be included in India's 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 "Personal 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."[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 one's 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 "reasonably necessary" for the purpose for which it was collected. The use of a subjective term such as "reasonably necessary" may affect implementation since it will be difficult to impose a tangible obligation on the organisation. For instance, an organisation

---

[532] 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).

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

[534] 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).

may continue to retain data for long periods of time on vague grounds such as "improving user experience" 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.*, 'The data protection principles under the General Data Protection Regulation', 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, 'Big Data Privacy: Challenges to Privacy Principles and Models', 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 "reasonably necessary/necessary" 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 "reasonably necessary" 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 "individual participation principle" which stipulates that the "processing of personal data must be transparent to, and capable of being influenced by, the data subject".[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, 'Data Privacy Law: An International Perspective' 2 (Oxford University Press, 2014).
[555] 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).
[556] 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).
[557] 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).
[558] Paul M. Schwartz, 'Privacy and Democracy in the Cyber Space', 52 Vanderbilt Law Review 1609 (1999).
[559] CIPP Guide, 'The HEW Report: Defining the Fair Information Practices', available at: https://www.cippguide.org/2012/08/23/the-hew-report-defining-the-fair-information-practices/, (last accessed 26 October 2017).
[560] 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).

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 one's personal data is being processed.
b. The right to access one's 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 one's 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, '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). 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, 'An Introduction to Subject Access Rights', 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, 'An Introduction to Subject Access Rights', 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, '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).

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 "all" 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, 'The Right to be Forgotten and the problems with Unstructured Data' (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, 'The Right to be Forgotten and the problems with Unstructured Data' (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, 'The Right to be Forgotten and the problems with Unstructured Data' (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, 'The Right to be Forgotten and the problems with Unstructured Data' (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.*, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation', 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, 'AI watchdog needed to regulate automated decision-making say experts', 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, "particularly 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 judges".[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, 'Consent, Proportionality and Collective Power, Reinventing Data Protection?', 4, (Springer Link, 2009).
[574] Antonella Galetta *et al.*, 'Mapping the Legal and Administrative Frameworks of Access Rights in Europe – A Cross-European Comparative Analysis' 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.*, 'Mapping the Legal and Administrative Frameworks of Access Rights in Europe – A Cross-European Comparative Analysis' 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, 'The Trouble with European Data Protection Law', 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 one's 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 "National Standard of Canada Entitled Model Code for Protection of Personal Information'.
[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 person's 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 one's 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 individual's family circumstances or professional interests in confidentiality. *See* Paul Voight and Axel Von Dem Bussche, 'The EU General Data Protection Regulation (GDPR): A Practical Guide' (Springer, 2017).

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

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

[598] Australian Law Reform Commission, 'Direct Marketing: Introduction', 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 "the right to be let alone".[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, 'Direct Marketing: Current Coverage by IPPs and NPPs' 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, 'Direct Marketing: Current Coverage by IPPs and NPPs' available at: https://www.alrc.gov.au/publications/26.%20Direct%20Marketing/current-coverage-ipps-and-npps, (last accessed 24 October 2017).
[601] Lexis Nexis, 'Should we rely on automated decision making technologies?' (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, 'AI watchdog needed to regulate automated decision-making say experts', 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, 'AI watchdog needed to regulate automated decision-making say experts', 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, 'Erasure, Restriction and Objection – Rights - Part 3', 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 "provided by" is still unsettled. The Article 29 Working Party Opinion accords a broad interpretation to "provided by" 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 India's 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 forgotten', 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, '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).

[613] 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).

[614] William RM Long and Thomas Fearon, 'WP29 Adopts Final GDPR Guidelines on Data Portability', 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 'direct marketing' 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 "commercial electronic messages" 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 "legal or other significant effects". Such requirements significantly limit the scope of the right since any human involvement in a decision-making process could mean it is not 'automated decision-making'.[617] Similarly, issues could arise *vis-a-vis* the terms like "legal or significant effects" 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.*, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation', 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.*, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation', 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, 'Preventing processing likely to cause damage or distress' 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 individual's 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, 'Delete: The virtue of forgetting in the digital age' (Princeton University Press, 2011).

[631] Frank La Rue, 'Report of the Human Rights Council's Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression', 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*., 'I regretted the minute I pressed share: A Qualitative Study of Regrets on Facebook', Symposium on Usable Privacy and Security, Pittsburgh, (July 20–22, 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, 'The End of Privacy' 221 (1999, Macmillan); Jonathan Zittrain, 'The Future of the Internet-and How to Stop It' (Yale University Press, 2008); Jeffrey Rosen, 'The Web Means the End of Forgetting', 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, 'Shamans, Software, and Spleens: Law and the Construction of the Information Society' (Harvard University Press, 1996); Helen Nissenbaum, 'Privacy in Context-Technology, Policy, and the Integrity of Social Life', 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, "*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.*"[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 'shackles of unadvisable past things' on 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. "If I post something online, do I have the right to delete it?"
b. "If I post something, and someone else copies it and re-posts it on their own site, do I have the right to delete it?"
c. "If someone else posts something about me, do I have a right to delete it?"

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 – 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 "shall have the obligation to erase personal data without undue delay", unless the retention of the data is necessary for exercising "the right of freedom of expression."[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, 'The Resistance of memory: Could the European Union's Right to be Forgotten exist in the United States?' 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, 'The Right to be Forgotten' 64 Stanford Law Review 90 (February 2012).
[642] Article 17, EU GDPR.

remove data for "the processing of personal data for journalistic purposes, or for the purposes of academic, artistic or literary expression."[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 information—eg: search engines—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 Spain's highest court, AudienciaNacional, to Google requiring it to delete information concerning a Spanish citizen's 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 'right to be forgotten'.

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, 'In Europe you will need a VPN to see real search results', 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, 'Reconceptualising the right to be forgotten to enable transatlantic data flow', 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, 'Schedule 1, Principle 5 of PIPEDA; Personal Information Retention and Disposal: Principles and Best Practices' (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, 'You'd better forget the right to be forgotten in Canada' (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, 'Submissions received for the consultation on Online Reputation', 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 "inaccurate, irrelevant, excessive, out-of-date, incomplete, misleading or obtained unlawfully." 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 India's 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 controller's possession?

---

[653] Section 24, POPI Act.
[654] Section 24, POPI Act.
[655] Andrew Weeks, 'The Right to Be Forgotten in South Africa', 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 subject's 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?