CENTRE FOR COMMUNICATION GOVERNANCE AT NATIONAL LAW UNIVERSITY DELHI

COMMENTS ON THE DRAFT PERSONAL DATA PROTECTION BILL, 2018[1]

The Centre for Communication Governance (Centre) is an academic research centre within the National Law University Delhi and is dedicated to working on information law and policy in India. It seeks to embed human rights and good governance within communication policy and protect digital rights in India through rigorous academic research and capacity building.

The protection of the right to privacy, and particularly informational privacy is an integral aspect information law and policy. We welcome the efforts of the Ministry of Electronics and Information Technology (MeitY), Government of India and the Committee of Experts set up by MeitY (Committee), in this direction.

We have provided our comments and feedback to the Draft Personal Data Protection Bill, 2018 (Bill) below. We have referred to the report of the Committee, titled 'A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians' (Report), where necessary to support the understanding of the Bill as put forth by the Committee. In preparing these comments, we have drawn upon existing principles of Indian law, including the Supreme Court's judgment in *Puttaswamy v. Union of India*[2] (Puttaswamy I), and India's experience with data protection and other laws where relevant, as well as international law, and experiences of other jurisdictions where relevant. We have also referred to the comments submitted by CCG and other

[1] With contributions from Smitha Krishna Prasad, Yesha Paul and Aditya Singh Chawla.
[2] *Justice K.S Puttaswamy (Retd.) v. Union of India*, (2017) 6 MLJ 267.

stakeholders to the Committee, earlier this year in response to its white paper (White Paper).

1. Preamble and Principles

1.1. Free and Fair Digital Economy

Paragraph 1 of the preamble to the Bill refers to the fundamental right to privacy, and notes that it is necessary to protect personal data as an essential facet of informational privacy. The second and third paragraphs then go on to note the critical use of data for the growth of the digital economy, and the need for creation of a culture that fosters a free and fair digital economy that respects informational privacy, and ensures empowerment, progress and innovation.

The Report also reflects this two-pronged approach, with even greater emphasis on the idea of a free and fair digital economy.

We note that ensuring growth of the (digital) economy is indeed a part of the State's obligations. However, the question before us here, is the role that this obligation has within the context of a law aiming to protection personal data in order to allow individuals to exercise their constitutionally guaranteed fundamental right to privacy.

At the time of setting up the Committee, MeitY set out terms of reference to govern the Committee's operation via an office memorandum[3]. The introductory paragraph of the office memorandum setting out the terms of reference notes that "(t)he Government of India is cognizant of the growing importance of data protection in India. The need to ensure growth of the digital economy while keeping personal data of citizens secure and protected is of utmost importance." The terms of reference themselves, as set out in part 3 of the office memorandum, simply mention that the Committee is to study various issues relating to data protection in India, and make specific suggestions on principles to be considered for data protection in India, and suggest a draft data protection bill.

[3] Ministry of Electronics and Information Technology, *Office Memorandum No. 3(6)/2017-CLES* (2017), http://MeitY.gov.in/writereaddata/files/MeitY_constitution_Expert_Committee_31.07.2017.pdf (Last visited Oct 10, 2018).

The office memorandum setting up the Committee, and providing these terms of reference was issued on July 31, 2017. In late August 2017, the Supreme Court reaffirmed that the right to privacy is a fundamental right.

Justice Chandrachud in his opinion recommended that the government set up a statutory framework to allow individuals to exercise this right, in its judgment in *Puttaswamy v. Union of India*[4]. He has taken on record the terms of reference (as set out in part 3 of the office memorandum)[5]. The opinion also notes that there is a positive obligation on the State to take all necessary measures to protect the privacy of an individual[6]. In the specific context of informational privacy, it goes on to state that the creation of a robust regime for data protection will require a careful balance between individual interests and legitimate concerns of the state. Some examples of what could constitute such legitimate concerns have been provided, these include: 'protecting national security, preventing and investigating crime, encouraging innovation and the spread of knowledge, and preventing the dissipation of social welfare benefits'[7].

Keeping the above in mind, we submit that while it is indeed within the purview of the State's functions to ensure growth of the economy, this should not be a foundational principle for our data protection laws. The data protection law should be drafted and implemented with the goal of protection of the right to privacy of individuals in India, and enabling them to exercise this right.

The Committee in its Report has referred to the idea that a 'free and fair digital economy' will further empower individuals, and ensure autonomy in protection of their personal data. However, the autonomy that a free economy allows us is only one small part of the protection of our personal data (one that is not reflected adequately in many of the Committee's recommendations, as we see in the context of data localisation and other requirements). It is clear from the *Puttaswamy* judgment, the Committee's White Paper, and the consultations that followed, that

[4] (2017) 6 MLJ 267, Chandrachud J.'s opinion, para 185 and Conclusion, para 5.
[5] *See id.* para 185.
[6] *See id.* para 3(I).
[7] *See id.* para 5.

there is need for a comprehensive data protection law in India. If we are to have a truly comprehensive data protection law that applies across sectors, both horizontally and vertically, the law itself should not be limited in its scope or interpretation, by references to the digital economy alone.

Our concerns regarding the emphasis on the growth of the digital economy and the costs of compliance were also in our initial comments to the white paper.[8]. The Report's focus on the idea of a free and fair digital economy has also been criticised since its publication[9].

We reiterate and echo these concerns again, in the context of the Committee's Report, and particularly the references contained in the Bill itself. The data protection law should regulate and govern the collection and use of personal data of individuals in India, irrespective of the effect such collection and use have on the digital economy or vice versa. We note that not every case of collection and use of personal data is relevant to the digital economy. While personal data has become a core element of the way many businesses within the digital economy work, it would be short-sighted for a law that is meant to be comprehensive, and technology / sector agnostic to be anchored to an undefined idea of a digital economy.

1.2. Fiduciary Relationship

The Bill and the Committee's Report introduce the term 'fiduciary' into data protection discourse in India. The Report discusses the nature of the relationship between persons who are traditionally identified as a 'data processor' and 'data subject' under most data protection laws. The Report notes that there is an element of trust, or a fiduciary nature to such a relationship given that a 'data subject' provides their personal data to a 'data processor' and / or allows them to use this data for certain purposes. In order to address and incorporate this element of the relationship, the

[8] *See* Centre for Communication Governance, *Comments to White Paper of the Committee of Experts on a Data Protection Framework for India* 11 (2018).

[9] Apar Gupta & Ujwala Uppaluri, *A fundamental error*, THE HINDU (2018), https://www.thehindu.com/opinion/lead/a-fundamental-error/article24566374.ece (last visited Oct 9, 2018).

Committee has used the terms 'data fiduciary' (i.e. a traditional data processor) and 'data principal' (i.e. a traditional data subject), in the Report and the Bill.

At the outset, we appreciate the Committee's acknowledgment of the expectation of trust that an individual has from a data processor / data fiduciary, and the Committee's attempt to incorporate this into the law.

However, we note that when discussing this concept, the Report once again focuses on the idea of a free and fair digital economy. Specifically, it states that pursuant to the fiduciary relationship between data principals and data fiduciaries, "data fiduciaries must only be allowed to share and use personal data to fulfil the expectations of the data principal in a manner that furthers the common public good of a free and fair digital economy"[10]. It is submitted that the merging of these two concepts of data fiduciaries, and a 'common public good of a free and fair digital economy' dilutes the fiduciary nature of the relationship that the Report seeks to establish.

In order to understand the impact of the use of the term fiduciary in this Bill better, we look to the way it has been defined under Indian law.

In *Central Board of Secondary Education v. Aditya Bandopadhyay*[11], the Supreme Court discussed the meaning of the word fiduciary, noting that:

> "*21. The term ' fiduciary ' refers to a person having a duty to act for the benefit of another, showing good faith and condour, where such other person reposes trust and special confidence in the person owing or discharging the duty. The term ' fiduciary relationship' is used to describe a situation or transaction where one person (beneficiary) places complete confidence in another person (fiduciary) in regard to his affairs, business or transaction/s. The term also refers to a person who holds a thing in trust for another (beneficiary). The fiduciary is expected to act in confidence and for the benefit and advantage of*

[10] Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* 8 (2018).
[11] *Central Board of Secondary Education v. Aditya Bandopadhyay,* 2011(11) SCR 1028.

the beneficiary, and use good faith and fairness in dealing with the beneficiary or the things belonging to the beneficiary. If the beneficiary has entrusted anything to the fiduciary, to hold the thing in trust or to execute certain acts in regard to or with reference to the entrusted thing, the fiduciary has to act in confidence and expected not to disclose the thing or information to any third party. There are also certain relationships where both the parties have to act in a fiduciary capacity treating the other as the beneficiary."

The definition of a 'fiduciary relationship' was once again discussed by the Supreme Court in *Reserve Bank of India v. Jayantilal N. Mistry*[12]. Here, the court set out rules that govern a fiduciary relationship as follows:

"*56. The scope of the fiduciary relationship consists of the following rules:*

"(i) No Conflict rule - A fiduciary must not place himself in a position where his own interests conflicts with that of his customer or the beneficiary. There must be "real sensible possibility of conflict.

(ii) No profit rule- a fiduciary must not profit from his position at the expense of his customer, the beneficiary;

(iii) Undivided loyalty rule- a fiduciary owes undivided loyalty to the beneficiary, not to place himself in a position where his duty towards one person conflicts with a duty that he owes to another customer. A consequence of this duty is that a fiduciary must make available to a customer all the information that is relevant to the customer's affairs

(iv) Duty of confidentiality- a fiduciary must only use information obtained in confidence and must not use it for his own advantage, or for the benefit of another person."

The Court's interpretation of the term 'fiduciary relationship' as described above is important in the context of the Bill for two reasons. First, it is clear that in many cases, data processors / fiduciaries, particularly those that are privately owned, are

[12] *Reserve Bank of India v. Jayantilal N. Mistry,* 2016 AIR SC 1.

unlikely to meet the criteria set out by the Court in *Jayantilal N. Mistry*. Several data processors collect and process personal data in the interest of the growth of their business, and presumably for profit. There is at the least potential for conflict between a data principal / data subject's interests and that of a person processing their data for such purposes. The concept of a fiduciary relationship as described in the Report[13], where "data fiduciaries must only be allowed to share and use personal data to fulfil the expectations of the data principal in a manner that furthers the common public good of a free and fair digital economy" also does not appear to take into account the Supreme Court's definition of a fiduciary relationship.

Chapter I: Preliminary

1.3. Scope of application of the law

Section 2 of the Bill describes the nature of data processing that the data protection law will apply to:

- *(i) processing of personal data that has been collected, disclosed, shared or processed within India*
- *(ii) processing of personal data by the State, any Indian company, any Indian citizen or any person or body of persons incorporated or created under Indian law.*
- *(iii) processing of personal data by data fiduciaries / processors not present in India, if it is in connection with any business carried on in India, or any systematic activity of offering goods or services to data principals within India*
- *(iv) processing of personal data by data fiduciaries / processors not present in India, if it relates to any activity which involves profiling of data principals within India*

The territorial scope of the Bill has two parts to it, first, processing activities taking place in India, which fall firmly within the jurisdiction of Indian legislative and

[13] Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, *supra* note 9, at 8.

government authorities. The second, is the extra-territorial scope that we see described in section 2(2) of the Bill. The Courts in India have upheld the power of the legislature to enact laws with extra territorial reach, when "such extra-territorial aspects or causes have, or are expected to have, some impact on, or effect in, or consequences for: (a) the territory of India, or any part of India; or (b) the interests of, welfare of, well being of, or security of inhabitants of India, and Indians."[14] In this context, the Bill largely follows this approach, and we recommend that this is maintained in future iterations of the Bill.

However, as discussed in our comments to the White Paper, there is a need be certainty about when an entity would be considered as 'offering goods and services' in India. Evidently, the mere availability of an entity's website would not be sufficient, as that would amount to regulating the entirety of the Internet. The Report has discussed this issue as well, and it appears that the use of the term 'systematic' in the Bill is meant to address this problem. There is some Indian jurisprudence on this issue, for instance in relation to trademarks with trans-border reputation, where the courts often look at whether a person / corporation has 'purposefully availed' themselves of the jurisdiction in question by looking at whether they specifically targeted their goods or services to persons in the jurisdiction[15]. We recommend that the language in this section is fortified by the use of criteria that can be identified in Indian jurisprudence on the matter.

2. Chapter II: Data Protection Obligations

2.1. Fair and Reasonable Processing

Section 4 of the Bill provides that any person processing personal data owes a duty to the data principal to process the data in a fair and reasonable manner that respects the privacy of the data principal.

A strong principle-based approach to data protection regulation is welcome, and we acknowledge that any data processing must be undertaken in a 'fair and reasonable

[14] *GVK Industries v. Income Tax Officer*, 2011(4) SCC 36, para 76.
[15] *Banyan Tree Holding (P) Limited vs A. Murali Krishna Reddy & Anr*, 2010(42) PTC 361.

manner that respects the privacy of the data principal'. In this context, we echo the comments made by Professor Graham Greenleaf, and recommend that rather than describing this principle as a duty owed by data fiduciaries to data principals, it is rephrased to reflect that data fiduciaries shall / must undertake data processing in this manner. Such rephrasing would strengthen and mandate compliance with this section.

At the same time, we note that the concepts of 'fair' and 'reasonable' are open to subjective interpretation rather than objective understanding in the way many other obligations under this Chapter are. In several sections where exemptions have been granted, this provision is one of the few that continues to remain applicable where certain types of processing of personal data are exempt from many if not most other provisions of the Bill. While there is theoretical discussion on what 'fair' and 'reasonable' may constitute, they can only be applied in practice on a case-to-case basis. Therefore, we caution against relying on this provision too much to hold up the larger goal of data protection that the Bill works towards.

2.2. Purpose Limitation

Section 5 of the Bill provides that personal data shall only be processed for purposes that are clear, specific and lawful. Purposes incidental to those specified to the data principal must be reasonably expected in the context of the original purpose for which data was collected.

Purpose limitation is an important principle of data protection and the incorporation of this provision in the Bill is welcome. However, the language used in Section 5(2) of the Bill is vague and subjective. We recommend that the reference to incidental purposes be removed given that it may be prone to misinterpretation. For instance, a corporation that processes personal data may consider its 'business purposes' as incidental to the specific purpose that data was collected for. We have in fact seen this in several privacy policies / consent agreements. However, the question of whether the data principal reasonably expects this is open for discussion.

If such language is retained, then proper guidance should be provided to data fiduciaries on how this provision is to be interpreted and used.

2.3. Collection Limitation

Section 6 of the Bill provides that collection of personal data should be limited to such data as is necessary for the purpose of processing.

As with purpose limitation, collection limitation is an important principle of data protection and the incorporation of this provision in the Bill is welcome. However, we note that two types of data processing may be undertaken in this Bill, processing where data is collected from the data principal, and processing by a data processor who does not directly collect the data from the data principal.

In order to avoid any potential for misuse, we recommend that the broader language of data minimization, applicable in general to the holding / storage / processing of data is also incorporated here.

2.4. Lawful processing

Section 7 of the Bill provides that personal data and sensitive personal data may be processed on the grounds described in Chapters III and IV of the Bill respectively.

Please refer to our comments on Chapters III and IV

2.5. Notice

Section 8 of the Bill provides detailed requirements regarding the nature of information that a data fiduciary must provide to a data principal about the processing of their personal data.

We welcome the level of detail incorporated into this section, and have the following recommendations regarding the manner in which the notice requirements should be fulfilled.

First, we note that it is important to read section 8 with section 11 of the Bill which states that data fiduciaries shall not only be responsible for complying with the

provisions of the Bill, but also demonstrating such compliance. In this regard, it will be important to ensure that data fiduciaries have provided independent notice to each individual data principal whose personal data is collected or processed, in addition to any general notice that may be provided on their website / platform.

Second, section 8 should clarify that once such notice is provided, the data fiduciary will comply with the obligations they have set for themselves in the notice document, and will not change these commitments without the specific consent of the data principal. We have also addressed this issue in our comments on section 12 (consent). The standard form of providing notice of data processing in use today is the privacy policy (partly because it is required under the Information Technology Act, 2000, but also because this is the common practice adopted by data processors globally). A look at generic privacy policies available on many websites, will show that typically there is provision made for the data processor to unilaterally amend the privacy policy. In some cases, they will offer to notify users of the amendments before or after the fact, but many policies simply state that by continuing to use the service, the user accepts the amendments. Such actions would no longer meet the notice or consent requirements under the Bill, and it is recommended that the Bill clarifies this position.

2.6. Data storage limitation

Section 10 of the Bill provides that personal data must be retained only as long as it is reasonably necessary for the purpose for which the data is processed.

We recommend that this provision is applicable not only to data fiduciaries but also data processors who act on behalf of data fiduciaries.

2.7. Accountability

Section 11 of the Bill provides that data fiduciaries shall be responsible for complying with the provisions of the Bill, and also demonstrating such compliance.

We note that this provision is applicable to a data fiduciary in relation to processing conducted by the fiduciary itself, or on its behalf, therefore putting the responsibility

on the data fiduciary to ensure compliance by data processors. However, we recommend that in addition to this, data processors be also subject to the accountability requirements under section 11, since data processors may have independent obligations under the Bill.

2.8. General comments on Chapter II

The obligations in Chapter II incorporate important principles of data protection, and are critical to ensuring that the rights of data principals are protected adequately. These obligations must not be derogated from, and any provisions which do allow derogation from these obligations must be limited and necessary for achieving specific goals in accordance with the criteria laid out in *Puttaswamy*[16].

We note that there have been several discussions on the Bill involving multiple stakeholders, since its publication. A common question that has arisen in these discussions relates to the applicability of some or all of these obligations in different situations provided for under the Bill (particularly under the different grounds of processing in Chapter III). For instance, whether the obligations under the Chapter, and specifically under section 8 (Notice) will be applicable where data processing is undertaken on the basis of grounds other than consent.

One reason for this maybe that our existing data protection rules under the Information Technology Act, 2000 (and some versions of the data protection principles as they exist), largely provide for terms which should be included in the consent agreement. However, this has been one of the primary causes for concern in the context of how the consent principle works in practice, and the lack of / inability to provide meaningful consent today. Two broad sets of solutions to this problem have been proposed in contemporary research, first proposals that call for an alternative to consent-based data protection, and the second, proposals that call for strengthening the existing consent-based model with more substantive law[17]. We

[16] (2017) 6 MLJ 267, Chandrachud J.'s opinion, conclusion para 5.

[17] Kritika Bhardwaj, *Preserving Consent Within Data Protection In The Age of Big Data*, 5 NLUD STUDENT LAW JOURNAL, 100–110 (2018), https://nludslj.webs.com/Kritika%20Bhardwaj,%20Preserving%20Consent%20Within%20Data%20Protection%20In%20The%20Age%20Of%20Big%20Data.pdf (last visited Oct 9, 2018).

have previously recommended the second model, and recommended that the data protection principles must be addressed both collectively, and as individual principles that each bring value to the table[18]. Consent, must operate within certain parameters provided by law, thereby allowing individuals the choice and autonomy to consent or not, while also ensuring that data fiduciaries / processors do not contract out of their responsibilities[19]. We note that based on the observations in the Report, and the provisions of the Bill, the Committee has chosen to adopt a similar approach as well.

In order to support this approach, we recommend that clarificatory language is included in the Chapter, to provide that these obligations shall be applicable unless a specific exception is provided for. We also recommend that any such exceptions are limited in nature.

We also recommend that guidance should be provided to data fiduciaries and processors on the manner in which compliance with the law would need to be demonstrated as early as possible once the law is in force.

3. Chapter III: Grounds for Processing of Personal Data

3.1. Processing of personal data on the basis of consent

Section 12 of the Bill provides that personal data maybe processed on the basis of the consent of the data principal. It also provides detailed conditions that any consent obtained by a data fiduciary should meet, including but not limited to contractual standards set out under the Indian Contract Act, 1872 (Contract Act).

The provisions in this section are important given that consent in many instances of processing of personal data is obtained via standard form contracts. Although the Contract Act provides detailed conditions that must be met for any contract to be valid, the validity of standard form contracts remains a grey area decided on a case-to-case basis. The additional requirements for obtaining consent set out in Section 12(2) of the Bill help clarify the position in this regard to some extent.

---

[18] Smitha Krishna Prasad, *Back to Basics: Framing a New Data Protection Law for India* (2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3113536&download=yes (last visited Oct 10, 2018).
[19] *Id.*

The Bill however does not explicitly address the question of incremental consent / change in the terms of the consent agreement. As discussed in the Part 2.5 of these comments above, the standard practice today is for data fiduciaries to state in their privacy policy or terms and conditions (which often also qualify as the consent agreement) that the data processor can unilaterally amend the such document, with or without prior notice to the data principal. Such actions will not meet the notice or consent requirements under the Bill, and rightly so.

In this context, it is recommended that the Bill clarifies this position i.e. that specific consent meeting the criteria set out in Section 12 must be obtained in case of any amendments to the consent / notice documents. It should also be clarified that refusal to consent in such a situation should not adversely affect the rights that a data principal has under the previous terms of consent.

In addition to the above, we note that the language of Section 12 provides some broad guidelines that 'consent' under the Bill must meet. It does not however address the manner in which we can ensure that the consent is informed, or specific to the purpose of processing. In this regard, we reiterate the recommendations made in our comments to the White Paper, and recommend that specific language is included in Section 12 to address the following issues:

(i) Mandatory 'unbundling' of consent[20] in the following contexts: (i) separation of consents for each item requiring consent, not one overall consent[21]; and (ii) separation of consents from the collection of any other information not necessary for the performance of the contract[22].

(ii) Incorporating the language requirements applicable under Section 8 (Notice).

[20] Graham Greenleaf, *Data Protection: A Necessary Part of India's Fundamental Inalienable Right of Privacy – Submission on the White Paper of the Committee of Experts on a Data Protection Framework for India* (2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3102810 (last visited Oct 10, 2018)

[21] Article 7(2), General Data Protection Regulation, Regulation (EU) 2016/679.

[22] *See id.* Article 7(4).

3.2. Processing of personal data for functions of the State

Section 13 of the Bill provides that personal data may be processed if such processing is necessary for:

- *(i) any function of the Parliament or State Legislature*
- *(ii) the exercise of any state function authorized by law for:*
  - *a. the provision of any service or benefit to the data principal from the State*
  - *b. issuance of any certification, license or permit for any action or activity of the data principal*

While it is acknowledged that the State will need to process personal data of individuals in India, for various purposes, it is submitted that this provision is too wide. Many of these activities can in fact be undertaken by the State with the consent of the data principals involved.

The *Puttaswamy* judgment has defined the right to privacy in terms of the autonomy of an individual, and the ability to make choices, decisions, and assert control over their personality[23]. In the context of informational privacy, the subject of the Bill, *Puttaswamy* recognizes that data protection regimes seek to protect the autonomy of the individual[24]. It is submitted here that one of the essential forms of expressing such autonomy in the context of informational privacy and data protection is consent. Therefore any exception to allowing an individual the autonomy of consenting to the processing of their data would need to be measured by the standards of an exception to the protection of the right to privacy and data protection.

The Committee's Report recognizes the primacy of consent in both its discussion on the manner in which consent can be made a more effective tool[25] and on the 'non-consensual grounds for processing'. The Report states that the non-consensual grounds for processing, i.e. the grounds described in sections 13, 14, 15, 16 and 17

[23] (2017) 6 MLJ 267, Chandrachud J.'s opinion, conclusion para 3(F).
[24] *See id.* para 177.
[25] Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, *supra* note 9, at 32.

of the Bill, address situations in which it is not possible to obtain consent or consent may not be an appropriate ground for processing.

To identify these grounds, the Report relies on the illustrative list of permissible exceptions[26], and adds to the list. However, the sections of this chapter that target data fiduciaries in general, i.e. private sector actors (Sections 16 and 17), reflect the idea that consent is the primary ground for processing, and state that if it is not possible to obtain consent, the other grounds may be adopted. It is not clear why the same standard hasn't been applied to the State, the language used in Section 13 avoids any mention of consent, and implies that simply being a State function is in itself a ground for processing of personal data. The Report itself discusses the problems of the asymmetry in power between data principals and data fiduciaries, particularly where the State acts as a data fiduciary. As noted by Amba Kak, this is "*the essence of the debate around consent… However, this argument only demonstrates that additional safeguards, beyond consent, are required—not that consent must be given up on altogether*."[27]

We also note that *Puttaswamy* not only provides a few illustrations of what could be permissible exceptions, it also describes the tests which these exceptions should be subject to. Exceptions / limitations should be prescribed by law, they should be necessary for the purpose of a legitimate state aim, the exception should be proportionate to achieving the object of the law[28].

It is submitted here that this provision is too wide in its ambit, and that simply listing out descriptors of State functions which cover a wide range of State functions would not meet the criteria described above. In order to qualify under the necessity test, each individual function of the State should be tested to see not only if it is necessary for the State to undertake the processing, but also if it is necessary to do so without the consent of the data principals.

---

[26] *See id.* at 106.

[27] Amba Kak, *The Srikrishna committee's data-protection bill does not do enough to hold the government accountable for use of personal data*, THE CARAVAN (2018), http://www.caravanmagazine.in/governance/government-policy/srikrishna-committee-data-protection-government-accountable (last visited Oct 10, 2018).

[28] (2017) 6 MLJ 267, Chandrachud J.'s opinion, conclusion para 180.

In this context, we also note that *Puttaswamy* advocates a three-part test of which the third part focuses on proportionality, a concept that is typically complementary to the test of necessity. However, Section 13 limits itself to applying the test of 'necessity', which is not well defined under Indian law[29]. It is recommended that this provision defines in more detailed manner what would qualify as 'necessary' data processing by the State.

We note that this idea of consent being the primary ground for processing, with other grounds being applicable if consent is not feasible is present in the sections of this chapter that target data fiduciaries in general, i.e. private sector actors (Sections 16 and 17). It is not clear why the same standard hasn't been applied to the State. The Report itself discusses the problems of the asymmetry in power between data principals and data fiduciaries, particularly where the State acts as a data fiduciary. As noted by Amba Kak, this is "*the essence of the debate around consent… However, this argument only demonstrates that additional safeguards, beyond consent, are required—not that consent must be given up on altogether*."[30]

3.3. Processing of personal data in compliance with law or any order of any court or tribunal

Section 14 provides that personal data may be processed if explicitly mandated by any law made by parliament or state legislature or for compliance with any order or judgment of a court or tribunal.

We acknowledge that processing of personal data may be required in both purposes mentioned above. However, we submit that the language used in this section is too broad. It is not clear what circumstances the Committee envisaged where such processing would be mandated by law, without the need for obtaining consent.

[29] Amber Sinha, Nehaa Chaudhari & Smitha Krishna Prasad, *Reading 'Necessity' in India's New Data Protection Bill*, 5 CyFy Journal 201819–30 (2018), https://www.orfonline.org/wp-content/uploads/2018/10/Digital-Debates-Online-Launch.pdf (last visited Oct 10, 2018).
[30] Kak, *supra* note 27.

We recommend that at a minimum, this section is modified to specify that consent will be the primary ground for processing in these cases, unless the law or order of the court / tribunal mandates processing without consent of the data principal.

The same standards of legality, necessity and proportionality as described above should be applicable in the context of Section 14 (a).

3.4. Processing of personal data necessary for the purposes related to employment

Section 16 (1) of the Bill provides certain circumstances in the context of the relationship between an employer and employee where processing of personal data of an employee can be undertaken without the consent of the employee.

Section 16 (2) clarifies that processing may be undertaken without the consent of the employee only where processing on the basis of consent is not appropriate given the relationship between the employer and employee, or obtaining consent would require a disproportionate effort on the part of the employer data fiduciary. The concepts of when it is appropriate to obtain consent, and when it is not, or what would constitute 'disproportionate effort' are not described or defined in the Bill. It is recommended that the Bill defines and describes what actions / circumstances would qualify to meet this criteria.

3.5. Processing of data for reasonable purposes

Section 17 of the Bill provides that data processing may be undertaken without the consent of the data principal for certain reasonable purposes specified by the Data Protection Authority (DPA). The provision specifies the criteria that the DPA must consider before specifying reasonable purposes, and also lists certain activities relating to which such specification could be made.

In this context, we recommend that the language used in Section 17(1) is tightened to clarify that **all** of the criteria from sub-section (a) to (e) must be considered in each case.

With regard to Section 17(2), it is not clear why some of the activities listed have been added to this list. The list consists of the following activities:

(a) prevention and detection of any unlawful activity including fraud;

(b) whistle blowing;

(c) mergers and acquisitions;

(d) network and information security;

(e) credit scoring;

(f) recovery of debt;

(g) processing of publicly available personal data;

Whereas sub-sections (a), (b) and (d), may not require additional justifications, we recommend against adding more commercial activities such as mergers and acquisitions, credit scoring and recovery of debt to this list. Some situations that involve these activities may indeed require data processing without consent, however, adding them to a pre-determined list in the law itself may create a false expectation that all data processing in relation to these activities are exempt from the consent requirements under the Bill. This could add to the burden of the DPA in regulating data processing related to such activities.

We are also concerned about the inclusion of sub-section (g) in this list. Given that persons in India have operated for so many years without a robust data protection law, there is a huge amount of personal data that is currently publicly available, but would not be so if the Bill was enforced. Further, it is not clear what constitutes as publicly available data, and in many cases, publicly available data may come with an expectation of privacy that may even be linked to the purpose for sharing of the data publicly. In such a circumstance, we recommend that publicly available data is approached cautiously under this Bill, and any exceptions to the provisions of this Bill granted in this regard are granted on a case to case basis.

4. Chapter IV: Grounds for processing of Sensitive Personal Data

4.1. Processing of sensitive personal data on the basis of explicit consent

Section 18 of the Bill states that sensitive personal data may be processed on the basis of explicit consent. In order to meet the 'explicit consent' requirement, the

conditions of consent under Section 12 must be met. In addition, the consent must be:

"(a) informed, having regard to whether the attention of the data principal has been drawn to purposes for operations in processing that may have significant consequences for the data principal;
(b) clear, having regard to whether it is meaningful without recourse to inference from conduct in a context; and
(c) specific, having regard to whether the data principal is given the choice of separately consenting to the purposes of, operations in, and the use of different categories of sensitive personal data relevant to processing."

We note that it is important to hold the processing of sensitive personal data to a higher standard, given the heightened risk of harm in the processing of such data. However, while this section aims to provide for such a higher standard, it does not provide much in the way of objective criteria that a data fiduciary can use to see if this standard has been met. As such, it could be prone to different interpretations, and attempts to misuse this provision or the sensitive personal data in itself. We recommend that the section is improved upon by providing language that helps data principals and data fiduciaries understand the standards set forth, by way of objective / illustrative criteria.

We also reiterate our comments in Parts 4.1 and 3.5 above in the context of this section.

4.2. Processing of sensitive personal data for the functions of the State

Section 19 provides that sensitive personal data may be processed by the State for:

- *(i) any function of the Parliament or State Legislature*
- *(ii) the exercise of any state function authorized by law for:*
  - *a. the provision of any service or benefit to the data principal from the State*

We reiterate our submissions in Part 4.2 above regarding the need to provide narrower circumstances, and higher standards of necessity for the application of this provision. Section 19 uses the term 'strictly necessary' rather than 'necessary'. However, in the absence of any definition or criteria that helps understand what 'necessary' means, and then what additional criteria need to be applied for such necessity to qualify as 'strict', this provision remains vague and ambiguous.

4.3. Processing of sensitive personal data in compliance with law or any order of any court or tribunal

Section 20 provides that sensitive personal data may be processed if explicitly mandated by any law made by parliament or state legislature or for compliance with any order or judgment of a court or tribunal.

We reiterate our submissions in Part 4.3 above regarding the need to provide narrower circumstances, and higher standards of necessity for the application of this provision. Section 20 also uses the term 'strictly necessary' rather than 'necessary'. However, as discussed above, in the absence of any definition or criteria that helps understand what 'necessary' means, and then what additional criteria need to be applied for such necessity to qualify as 'strict', this provision remains vague and ambiguous.

4.4. Further categories of sensitive personal data

Section 22 of the Bill provides that additional categories of personal data may be notified as sensitive personal data by the DPA, on the basis of certain criteria identified in the provision. Where required additional safeguards or restrictions on the processing of such categories of sensitive personal data may be prescribed by the authorities. The section also provides that the DPA can specify further grounds on which such categories of sensitive personal data may be processed.

We welcome the Committee's recognition of the need for an ongoing evaluation of the sensitivity of personal data and the safeguards in place for protection of sensitive personal data. However, it is not clear why the DPA has been authorized to specify further grounds on which those categories of sensitive personal data that are notified

by the DPA may be processed. The Report also appears to be silent on this issue. We recommend that this part of the provision is removed from this section.

5. Chapter V: Personal and Sensitive Personal Data of Children

Section 23 of the Bill prescribes additional steps to be taken by data fiduciaries in order to protect any data principals that are children. The age of majority under Indian law, i.e. 18 has been adopted for the purpose of identifying children under this Bill as well.

We appreciate the Committee's efforts to ensure that children whose personal data may be processed are adequately protected under the Bill. We recommend that these measures be finalized after specific consultations with experts who work on issues pertaining to children's use of online spaces, and child rights in general.

6. Chapter VI: Data Principal Rights

6.1. Right to confirmation and access

Section 24 provides that data principals shall have the right to obtain confirmation that a data fiduciary is processing or has processed their personal data, and obtain a summary of such personal data, and the processing activities undertaken.

We recommend that access is not limited to a summary of the personal data held by the data fiduciary, and the processing activities undertaken un relation to such personal data. The rights to confirmation and access are important rights that inform and enable a data principal to exercise other rights under the data protection law. As recognized in the Report, these are 'gateway rights', which must be given a broad scope[31]. The Report has recognized that implementation of this right maybe expensive, and provided for a fee to be levied in some circumstances. However, the Report itself suggests that irrespective of the difficulty or expenses involved in providing confirmation or access, a broad right must be provided which includes in its scope all personal data of a data principal held by a data fiduciary, and information

[31] Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, *supra* note 9, at 70.

regarding various processing activities, including the purpose for processing, disclosure / sharing / transfer of personal data etc.

Accordingly, the right to confirmation and access should provide that a data principal has the right to confirmation about the processing of their personal data by a data fiduciary, access to the full personal data of the data principal that is held by the data fiduciary, and the processing activities undertaken in relation to such personal data.

6.2. Right to data portability

Section 26 of the Bill provides data principals the right to obtain, or have transferred to a different data fiduciary any personal data about them held by a data fiduciary. This includes personal data provided by the data principal to the data fiduciary, obtained by the data fiduciary elsewhere, and generated by the data fiduciary.

The right to data portability is an important and necessary right that should be made available to data principals in order to allow them to exercise their autonomy. We have two comments on the manner in which this provision has been drafted.

First, Section 26(1)(a)(ii), which provides that the personal data that the data principal has a right to in accordance with this section includes personal data 'which has been generated in the course of provision of services or use of goods by the data fiduciary'. It is not clear here why this data has been limited to that generated in the course of provision of services or use of goods by the data fiduciary.

We note that as per current practices, reports suggest that many data fiduciaries generate or process personal data beyond the specific services or goods that they provide a data fiduciary. There could be two reasons for not including this within the scope of this sub-section (a) processing or holding of such personal data would not be permissible under the purpose limitation and other obligations under Chapter II of the Bill, and (b) in many cases, any additional personal data (over that required or generated in the course of provision of service or goods) held by a data fiduciary would fall within Section 26(1)(a)(iii) (data which forms a part of any profile of the data principal). However, given the amount of personal data that would already be held by many data fiduciaries at the time when this law comes into force, and the

pervasive nature of data processing undertaken today, we recommend that Section 26(1)(a)(ii) is expanded. This provision should cover all personal data generated by a data fiduciary. Such expansion of the scope of Section 26 would serve an additional purpose. Without the expansion of the right to confirmation and access, section 26 is the only provision in this Bill which would allow a data principal access to all data about them held by a data principal, and should be as expansive as possible. It may well be that a data principal is only able to recognize or identify any contraventions of the Bill by the data fiduciary, once they have access to such data.

Second, Section 26(2) limits the scope of this right to personal data processed by automated means. Section 48 of the Bill already provides a wide exemption from the provisions of this Bill for small entities that process personal data manually. The sub-sections of Section 26(2) provide other exceptions to the rights in Section 26(1) that may be considered reasonable. In such a case, there is no reason why these rights should be further limited to personal data processed by automated means. Further, we note that there is no other definition or qualification to describe what constitutes automated means here. This limitation would only serve to add ambiguity to the rights of the data principal, allowing data fiduciaries the discretion to deny data principals their rights, for instance in situations where processing is undertaken by a combination of human and automated means. We recommend that this limitation to personal data processed by automated means is removed.

6.3. Conditions for the exercise of rights under Chapter VI

Section 28 provides certain general conditions applicable to the exercise of rights under this Chapter.

We note here, that the Report in its discussion of the right to confirmation and access, emphasizes the importance of this right and states that data fiduciaries should not be able to refuse requests under this right. We agree with the Report in this context, and recommend that Section 28 is amended to reflect this position.

6.4. Other rights

The Bill has omitted several other rights that we see incorporated in other legislations such as the GDPR and are integral to the rights of data principals in the digital age. These rights include the right to object to processing and the right to deletion of personal data, the right to object to processing for purpose of direct marketing, the right to not be subject to a decision based solely on automated processing, and the right to restrict processing.

The White Paper discussed these rights, and expressed some concerns about the applicability and use of these rights in the Indian ecosystem. As mentioned in our comments to the White Paper, these rights described are important rights that allow individuals to fully exercise their right to informational privacy in the context of the way technology operates and functions today. We recommend that these rights are incorporated in the Bill.

The right to restrict processing, object to processing and processing for the purpose of direct marketing are contemporary, relevant rights that are being incorporated in data protection laws in many jurisdictions today[32].

On the right to object to processing, the sole concern expressed in the White Paper is that it is applicable in contexts that are not currently recognised as grounds of processing in India. It was not clear however, why this should prevent us from incorporating this right if it is otherwise considered relevant. With grounds other than consent now being recognised as lawful grounds for processing of personal data, we do not believe that this concern, even if it were valid, holds anymore. The efforts undertaken by the Committee in any case constitute a study of comparative or international laws on data protection, which have then been modified to apply in India. In this context we note that in the absence of any right to object to processing, restrict processing, or request deletion of personal data, the rights of data principals are limited significantly. The ability to ensure that a data principal's personal data is

[32] *See* Greenleaf, Graham, *'European' Data Privacy Standards Implemented in Laws Outside Europe,* 149 PRIVACY LAWS & BUSINESS INTERNATIONAL REPORT 21-23 (2017), https://ssrn.com/abstract=3096314 (last visited Oct 10, 2018).

not being processed against their will, is limited to the ability to withdraw consent[33] or rely on the data fiduciary's compliance with the storage limitation obligations[34]. However, this means that where data is processed on grounds other than consent, there is essentially no right to deletion of data or object to the processing of personal data until the purpose is fulfilled, even if the data principal is willing to face the consequences of not having such purpose fulfilled.

The Committee seems to recognise the importance of these rights in the context of individual autonomy. However, they have inexplicably decided that the curbing of autonomy in this particular case is necessary for the greater public good of a 'free and fair digital economy'. Our comments on the manner in which the Committee has valued the economy over individual rights are available in Part 1.1 of these comments.

Accordingly, we recommend that the right to restrict and object to processing, and obtain the deletion of personal data held by a data fiduciary is also granted to individuals.

With regard to the right to object to processing for the purpose of direct marketing, we agreed with the views expressed in the White Paper, that there is a need for a framework which provides for direct and unsolicited marketing across sectors / means of communication. It is not clear why this framework is not provided under this law[35].

The right not to be subject to a decision solely based on automated decision making is also an important right, the denial of which could adversely impact individuals. The right is important, considering the potential issues that individuals could face as a result of inaccurate decision making – ranging from receiving promotional material for services you are not interested in, to unjustified discrimination on the basis of

[33] The Personal Data Protection Bill, s.12 (2018).
[34] *Id.* at s.10.
[35] We note that the TRAI has in July 2018 published the new Telecom Commercial Communication Customer Preference Regulations, 2018. However, these regulations are not comprehensively applicable across sectors.

social factors[36]. Again, there is no proper justification provided by the Committee for the exclusion of this right. The Committee recognises the legitimate rationale behind the inclusion of these rights in the GDPR i.e. curbing harms due to prejudice and discrimination in output data owing to evaluative determinations without human review[37]. The Report then suggests that human review could also be biased, and a better solution (than granting individuals the autonomy to object to these biases), is to ensure that systemic changes, such as the incorporation of privacy by design principles and adequate accountability frameworks. The Committee suggests that 'processes that weed out discrimination' are a constituent element of 'privacy by design' that is mandated in Section 29 of the Bill. However, we note that section 29 of the Bill includes a somewhat detailed description of these elements, and we do not believe that any of them directly address the problems posed by automated decision making.

The right to object to a decision solely based on automated decision making is important not only to ensure that no discriminatory decisions are made about the data principal, but also allow data principals the right to know how decisions about them are being made. In situations where even the makers of these automated systems often do not understand or are unable to explain the decision making processes, the rights of individuals are significantly impaired by the absence of this right. A forward thinking law, which aims to continue to be relevant and govern the processing of personal data in a future which promises to only build on automated processes must ensure that individuals are adequately protected from these processes where required.

We recommend that the right to object to a decision solely based on automated decision making is provided for in this Bill in order to ensure that the data principal is able to exercise their autonomy in full.

---

[36] Article 29 Data Protection Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679* (2017), http://ec.europa.eu/newsroom/document.cfm?doc_id=47742 (last visited Oct 10, 2018).

[37] Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, *supra* note 9, at 74.

7. Chapter VII: Transparency and Accountability Measures

7.1. Privacy by design

Section 29 requires data fiduciaries to incorporate privacy by design principles described in the provision.

We note here that although the section is titled privacy by design, the provision itself is prescriptive and limited to the 7 principles described in the section. We recommend that the provision mandates incorporation of 'Privacy by Design' as a concept, in order to ensure that the law takes into account any evolution of these principles.

We also recommend that Professor Greenleaf's suggestions of incorporating a privacy by default standard in this section are adopted[38].

7.2. Personal data breach

Section 32 of the Bill provides measures to be undertaken by data fiduciaries in case of a breach of personal data in the context of notification of the breach to the DPA.

We note that this section only provides for notification of a breach to the DPA, and then states that the DPA will decide whether data principals need to be notified of the breach. It in fact, seems to bar data fiduciaries from notifying data principals of the breach, except where required by the DPA.

The underlying idea behind data breach notification provisions is that a security breach must be notified, and cannot be kept secret by the data controller and/or processor, and must inform at three levels: the data protection authority, individuals and the public, where needed.

In this context whereas a strict liability approach is recommended in the case of notification of breaches by data processors / fiduciaries to the DPA, the question is what approach should be adopted for notification to the data principal / public. We

[38] Graham Greenleaf, *GDPR-Lite and Requiring Strengthening – Submission on the Draft Personal Data Protection Bill to the Ministry of Electronics and Information Technology (India)* (2018), https://ssrn.com/abstract=3252286 (last visited Oct 10, 2018).

refer to our comments to the White Paper on this subject, and recommend that the data fiduciary must provide a written assessment to the data protection authority of its determination of 'harm' to the data subjects, arising out of the data breach. The authority may then come to an independent conclusion as to whether, in such instances, there exists a risk of harm to data subjects.

However, the data fiduciary need not wait for the data protection authority's independent determination of 'risk of harm' in order to notify data subjects of the breach. Such a determination by the authority may occur *post-facto*. In cases where the magnitude of the leak is high, the fiduciary should, in addition to, communicating individually to every data subject, issue a public communication containing details regarding the nature of the breach, the estimated number of data subjects affected, the measures taken to reestablish data security, etc.

A guide maybe provided to data fiduciaries on what constitutes harm or the risk of harm in order to arrive at the determination of whether notification needs to be provided to data principals / the public. The GDPR provides one example of how this approach can be incorporated into law. Adopting this approach would increase the responsibility of the data fiduciary towards a data principal in the protection of their data, and also reduce the burden on the DPA in assessing each breach to determine whether notification to data principals is required.

Further, we recommend that in no case should a data fiduciary be precluded from notifying a data principal of a breach should they wish to do so. We acknowledge that unnecessary or large numbers of public notifications of breach may cause panic. However, notification of breaches to individual data principals with sufficient explanations regarding the consequences of the breach would work towards empowering the data principal.

7.3. Classification of data fiduciaries

Section 38 of the Bill provides that the DPA may classify certain data fiduciaries as significant data fiduciaries, and provides criteria for consideration by the DPA in making such a decision. The criteria include:

(a) volume of personal data processed;

(b) sensitivity of personal data processed;

(c) turnover of the data fiduciary;

(d) risk of harm resulting from any processing or any kind of processing undertaken by the fiduciary;

(e) use of new technologies for processing; and

(f) any other factor relevant in causing harm to any data principal as a consequence of such processing.

This section also provides that the requirements in relation to data protection impact assessments, record-keeping, data audits and appointment of data protection officers will only be applicable to significant data fiduciaries as determined by the DPA.

It is submitted that the language used in this section, and the discretion granted to the DPA under this provision is too wide. First, whereas the DPA is provided with certain criteria to consider when determining whether a data fiduciary is a significant data fiduciary or not, there is no threshold or consistency requirement set forth in this provision. The DPA has the discretion to make this determination on a case to case basis. It is submitted that this is too wide a discretionary power to give to the DPA, and should be limited. The concerns regarding the application of this section are exacerbated by the questions on the independence of the DPA.

Second, the criteria for consideration itself is limited. For instance, while the inclusion of turnover betrays a focus on the private sector in the drafting of this section, the absence of any 'public interest' criteria is conspicuous. Such criteria should necessarily be included in any such determination. Given the kind of personal data processing that is undertaken by the State, and the lack of accountability that is seen in many cases[39], it is important to ensure that any State agency (that meets a bare

[39] For detailed examples or discussions, *See* Gopal Sathe, *The Indian Railways Is Sitting on a Giant Trove Of Your Digital Data. The Modi Govt Wants To Sell it, And Experts Are Worried*, HUFFPOST (July 7, 2018), https://www.huffingtonpost.in/2018/07/18/the-indian-railways-is-sitting-on-a-giant-trove-of-your-travel-data-the-modi-govt-wants-to-sell-it-and-experts-are-worried-dek_a_23484279/ (last visted Oct 9, 2018); Centre for Communication

minimum threshold criteria) should be considered a significant data fiduciary. All transparency and accountability measures should be made applicable to these State agencies.

Third, we note that four obligations of data fiduciaries, in relation to data protection impact assessments, record-keeping, data audits and appointment of data protection officers, would essentially not be applicable to those data fiduciaries that the DPA does not consider to be significant data fiduciaries. In this context, we recommend that record-keeping is removed from this list. Record-keeping is an important function of any data fiduciary and directly related to the data fiduciary's obligations under Section 11(Accountability), and the exercise of the data principal's rights under Chapter VI of the Bill. As such, all data fiduciaries should be required to maintain records of all data processing activities.

8. Chapter VIII: Restrictions on cross border data transfer

The Bill places two different types of restrictions on cross border transfer of personal data, the first in the form of data localization[40] and the second in the form of conditions on the permissible transfers of personal data[41]. Our comments on these sections are below.

8.1. Data localization requirements

Section 41 of the Bill provides that one serving copy of all personal data that is governed by the data protection law must be served on a server or data centre in India. Certain categories of personal data (but not sensitive personal data) may be exempt from this requirement based on necessity or strategic interests of the State.

It also provides that the critical personal data (to be identified by the central government) should be stored and processed only in India.

Governance, *Comments to White Paper of the Committee of Experts on a Data Protection Framework for India* 11 (2018).

[40] The Personal Data Protection Bill, s. 40 (2018).

[41] The Personal Data Protection Bill, s. 41 (2018).

In addition to this Bill, it has been noted with some concern that there are several other law / policy making processes running parallelly which seek to impose data localization requirements in different sectors. For example, the Reserve Bank of India issued a notification directing that payment system providers must 'ensure that the entire data relating to payment systems operated by them are stored in a system only in India'[42]. Payment system providers and others have raised a number of questions about what this means practically for these companies[43].

Similarly, in the draft of the e-commerce policy states that steps would be taken to develop capacity for and incentivize domestic data storage in India, and post a two-year sunset period, data localization would become mandatory.[44] The draft provides that 'community data collected by IoT devices in public spaces', and data generated by users in India from various sources including e-commerce platforms, social media, search engines etc' would need to be mandatorily stored exclusively in India. The government of India will have access to this data for national security and public policy objectives, subject to 'rules related to privacy, consent etc.' The data stored in India will also be shared with start-ups meeting certain criteria (there is no limitation here regarding application of the above-mentioned rules related to privacy, consent etc.).

While these policies / sector specific regulations are not the subject of this submission, they are relevant, since the Bill is meant to provide a comprehensive overview of how personal data is protected and processed in India.

---

[42] Storage of Payment System Data, RBI/2017-18/153 (2018).

[43] Aditi Shah & Aditya Kalra, *Exclusive: India Proposes Easing Local Data Storage Rules For Foreign Payment Firms-Document*, REUTERS (July 12, 2018), https://in.reuters.com/article/india-data-localisation-exclusive/exclusive-india-proposes-easing-local-data-storage-rules-for-foreign-payment-firms-document-idINKBN1K20K6 (last visted Oct.9, 2018); Mihir Sharma, *How Data Localisation limits Posssibilities for India's Startups, Consumers*, BUSINESS STANDARD (Sept.14, 2018), https://www.business-standard.com/article/current-affairs/how-data-localisation-limits-possibilities-for-india-s-startups-consumers-118091400087_1.html (last visited Oct.3, 2018).

[44] Aroon Deep, *Draft National E-Commerce Policy : Data Localisation And Priority To Domestic Companies*, MEDIANAMA (Aug.7, 2018), https://www.medianama.com/2018/08/223-draft-national-e-commerce-policy-data-localisation-and-priority-to-domestic-companies/ (last visited Oct. 3, 2018).

The Report accompanying the Bill discusses the reasons why data localization is required / recommended in India. The White Paper also discussed some of these ideas while assessing whether data localization should be provided for under Indian law. These reasons are discussed and addressed below.

1. Enforcement of domestic law, and data protection law: This section of the Report aims to address two issues, first, domestic law enforcement, and second providing individuals with higher data protection standards available under Indian law.

   On the first, the Report notes that law enforcement authorities often need to gain access to information held and controlled by data fiduciaries. It argues that local storage of personal data would limit jurisdictional problems that these authorities face, and assist in obtaining this information easily.

   The Committee is right in noting that the processes that law enforcement authorities are currently required to follow to access data held in foreign jurisdictions is difficult and slow. However, as submitted previously in our comments to the White Paper (attached), mandating localization purely to ensure access to data for law enforcement appears to be an overbroad measure. In this context, the language used in the Report about the kind of data law enforcement authorities need to access is key: data that **held** and **controlled** by data fiduciaries. If the issue at hand is access to data controlled by data fiduciaries that do not fall under Indian jurisdiction, then data localization may not be the best way to tackle the problem. It may be more appropriate to avail other alternatives, such as incorporating investigative jurisdiction which shifts focus away from the location of the data to the nationality and location of the target data fiduciary[45].

   The U.N. Special Rapporteur on the Right to Privacy has proposed that "negotiation and legislation are the most appropriate means of developing mechanisms by which a state may efficiently obtain access to cloud data."[46]

[45] DAN SVANTESSON, LAW ENFORCEMENT CROSS-BORDER ACCESS TO DATA (2016).
[46] *Microsoft Corporation v. United States of America*, No. 14-2985 (2d Cir. 2016).

Given the failure of the MLAT process, new processes must be operationalized. The Report itself also acknowledges that in the future, nation states should work towards harmonization to create an effective information sharing regime for law enforcement. An example, previously endorsed by the Rapporteur,[47] could be an international framework that allows for the grant of an 'international data access warrant.'[48] Another example would be the kind of bilateral negotiations that the recently passed Clarifying Lawful Overseas Use of Data Act (CLOUD Act) in the United States of America[49], subject however, to adequate transparency, accountability and oversight mechanisms[50]. We note in this context, that although the Report contains some discussion on the nature of laws that would permit law enforcement authorities to access personal data, the Bill leaves this question open. The Bill simply provides that all law enforcement access to data will largely be exempt from the requirements under the Bill in so far as they are authorized by law, necessary and proportionate. It is submitted that in the absence of a clear law providing for such access in such manner, it is premature to discuss the need for data localization in order to allow law enforcement access to data.

On the second issue, although the Report makes mention of it initially, there is no substantial discussion explaining why local storage of data (whether entirely, or in a copy form), would afford better data protection. Effective regulation of cross-border transfer of personal data should be sufficient to ensure that personal data of individuals in India is protected adequately.

---

[47] Joseph A. Cannataci (Special Rapporteur on the Right to Privacy), *Report of the Special Rapporteur on the Right to Privacy, Joseph A. Cannataci*, 18 A/HRC/34/60 (Feb.24, 2017).

[48] *Microsoft Corporation v. United States of America*, No. 14-2985 (2d Cir. 2016).

[49] S.2383, 115th Cong. (2018).

[50] The CLOUD Act has been subject to criticism from several civil society and human rights organisations for failing to provide adequate transparency, accountability and oversight mechanisms. *See* David Ruiz , *Responsibility Deflected, Cloud Act Passes*, ELECTRONIC FRONTIER FOUNDATION (Mar.22, 2018), https://www.eff.org/deeplinks/2018/03/responsibility-deflected-cloud-act-passe(last visited Oct.9, 2018); Neema Singh Guliani & Naureen Shah, *The Cloud Act Does Not Help Privacy and Human Rights: It Hurts Them*, LAWFARE (Mar. 16, 2018), https://www.lawfareblog.com/cloud-act-doesnt-help-privacy-and-human-rights-it-hurts-them (last visited Oct. 9, 2018).

2. Building an Artificial Intelligence (AI) ecosystem: The Report notes that there is great economic potential of an AI ecosystem, and development of such an ecosystem is integral to the digital economy.

   In this regard, the Report appears to provide two separate sets of arguments: (i) that growth of AI is dependent on harnessing data, and (ii) data localization policies would ensure that processing of data is done within the country using local infrastructure, and create an ecosystem with local presence of skilled professionals.

   It is not clear how local storage of data would translate into harnessing of this data by the local industry. While the Report discusses this idea of building an ecosystem, the Bill does not seem to reflect this goal. The Bill, **rightly**, does not provide for any overt circumstances where personal data of Indian individuals must be shared with the Indian industry, simply for the purpose of building this AI ecosystem. Data sharing may be permitted in limited circumstances, provided the conditions set forth in the Bill are complied with.

   However, the draft e-commerce policy mentioned above provides some worrying insight into the approach that some appear to be taking in this context. The policy simply states that data stored in India will be shared with local start-ups meeting certain criteria. It is not clear how consent, purpose limitation or any other requirements under the Bill will play into this.

   Subsequent developments have suggested that the draft e-commerce policy will be revised, and is being discussed at different levels within the Government. However, the underlying issue raised by the reliance of the Report (and the e-commerce policy), on data localization as a means of building India' AI industry by way of sharing of personal data held in India is still cause for concern. The growth of an AI based economy, as well as the use of AI for good are much discussed subjects today. However, as discussed above in Part 1.1, the economic growth and related benefits available to the Indian industry must be subject to the protection of the privacy and data protection rights of individuals and not vice versa.

3. Preventing foreign surveillance: The Report argues that storage of personal data in different jurisdictions increases the risk of foreign surveillance, citing the example of US foreign surveillance laws and actions.

   However, as we have discussed in our comments to the White Paper, it has been argued that localization may be an ineffective remedy. First, localization laws such as Russia's, that merely mandate the storage of local copies of data, only increase the risk of unlawful surveillance by domestic authorities, while maintaining the same degree of exposure abroad[51]. Second, reports suggest that foreign governments routinely employ surveillance tactics overseas, along with the use of malware[52]. This implies that physical access to data storage or processing is not technically necessary, and relocating the data would not serve the purpose of protecting it.

   Even if the Committee's argument is accepted, it is not clear how mandating local storage of a copy of data in India will prevent or limit foreign surveillance.

On a general note, it has been suggested that localization may make data more vulnerable to security attacks as well as natural disasters[53]. Typically, data is partitioned and stored over multiple physical locations, in a process known as sharding. Mandating localization would preclude such practices[54]. Localization also creates a 'jackpot' problem, with vast quantities of data centralized within a jurisdiction as a compelling target for unauthorized access.[55]

Scholars have also suggested that data localization may be contrary to the values enshrined in the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, which protect the freedom to seek, receive and impart information of all kinds, regardless of frontiers[56]. The right to access the

---

[51] Neha Mishra, *Data Localization laws in a Digital World*, THE PUBLIC SPHERE 137, 143 (2016).
[52] *Id.*
[53] Mishra, *supra* note 51 at 143.
[54] *Id.*
[55] Anupam Chander and Uyên Lê*, Data Nationalism*, 64 EMORY L.J. 677, 717 (2015).
[56] CHRISTOPER KUNER, TRANSBORDER DATA FLOWS AND DATA PRIVACY LAW, 66 (2013).

internet has also been recognized as a fundamental human right by the United Nations Human Rights Council[57]. The Indian Supreme Court has also made observations to this effect[58]. An example of the immediate impact that one could see from a consumer perspective is the availability of services provided by smaller foreign service providers. Not all services on the internet are backed by large companies with deep pockets, or targeted specifically at Indian users. If smaller service providers who see India as one of many potential markets are forced to store local copies of personal data in India, when it is not economically viable for them, this may result in service providers choosing not to make their services available in India at all. It is also not clear how these data localization requirements will be enforced with respect to all persons who collect or process any personal data on the internet, that segments of the Indian population may wish to engage with.

On the basis of the above, it is submitted that data localization as envisaged by Section 40(1) of the Bill does not address the concerns raised by the Committee adequately, and is an over broad measure that may have a negative impact on the rights of Indian data principals. If data localization is required to protect certain sensitive information, then adequate rules may be made specific to certain sectors or categories of information. However, it is premature to consider a broad data localization requirement in the sense of Section 40(1) of the Bill.

As discussed above, Section 40(2) of the Bill provides that the Central Government will notify categories of personal data that are 'critical personal data', which may only be processed in a server or data centre located in India. The Report is not clear on what these categories of data may be. While it may be accepted that in certain circumstances such localization measures may be appropriate, it is submitted that the discretion granted to the Central Government under this Section is too wide, and must be limited by specific criteria for recognition of such categories.

[57] Human Rights Council, A/HRC/32/L.20 (2016).
[58] Krishnadas Rajagopal, *Right to Access Internet Cannot be Curtailed, Says SC*, THE HINDU (Apr..13, 2017), https://www.thehindu.com/news/national/right-to-access-internet-cannot-be-curtailed-says-sc/article17994420.ece (last visited Oct.9, 2018).

It is also submitted that a detailed study of India's obligations under the World Trade Organisation agreements[59], and the impact that localization requirements may have in this context, is undertaken before mandating localization in any form.

8.2. Conditions for cross-border data transfer

The Bill provides that personal data can be transferred outside India in the following circumstances:

- *If the transfer is made with the consent[60] of the data principal, and subject to standard contractual clauses or intra-group schemes that have been approved by the Data Protection Authority (DPA); or*
- *If the transfer is made with the consent[61] of the data principal, to a country / sector within a country / international organization that has been pre-approved by the Central Government. Section 41(2) lists out the criteria for such pre-approval: The Central Government must find that the relevant personal data will be subject to an adequate level of protection, on the basis of the applicable laws and international agreements, and the effectiveness of the enforcement by authorities with appropriate jurisdiction. The Central Government must also monitor the circumstances applicable to such data in order to review its decision.*
- *If the transfer / set of transfers has been approved by the DPA.*

This section reflects the approach recommended in our comments to the White Paper. However, we submit that it may be useful to strengthen the provisions under Section 41 of the Bill. As it stands currently, the Bill places a high burden on the DPA, requiring approval of either all contractual clauses or intra-group schemes that data can be transferred through, or countries (or sectors within a country), or international organizations that data can be transferred to.

---

[59] *Legal Texts: The WTO Agreements*, WORLD TRADE ORGANISATION, https://www.wto.org/english/docs_e/legal_e/final_e.htm (last visited Oct.9, 2018). https://www.wto.org/english/docs_e/legal_e/final_e.htm.

[60] Consent must be explicit where the data is sensitive personal data.

[61] Consent must be explicit where the data is sensitive personal data.

The DPA should also be empowered to adopt standard clauses or rules that can then be used by data fiduciaries, for instance as provided for in the EU's GDPR. As recommended in our comments to the White Paper, the DPA could place reliance on adequacy assessments by other regulators and international data protection authorities, whose standards are considered sufficiently rigorous[62]. A harmonized approach could reduce the burden on the regulator. As recommended by Professor Graham Greenleaf, the European Union would be a primary contender for such an alignment, entailing that there would already be 43 jurisdictions where data may flow freely[63].

9. Chapter IX: Exemptions

9.1. Security of the state, and prevention, detection, investigation and prosecution of contraventions of law

Sections 42 and 43 of the Bill provide exemptions from the application of large parts of the Bill where personal data is required to be processed in the interests of the security of the State, and prevention, detection, investigation and prosecution of any offence or contravention of law, respectively. Such processing will only be permitted if it is authorized pursuant to a law, is in accordance with the procedure established by such law made by Parliament (and State Legislature in the case of Section 43), and is necessary for and proportionate to achieving the interests in question.

In cases, which fall under such a category, the processing will be exempt from all provisions of the Bill other than Section 4 (which requires data processing to be fair and reasonable), and Section 31 (which requires certain minimum security standards to be adopted by data fiduciaries).

Given that the two sections are largely similar in nature, we address our concerns regarding both sections together in these comments.

---

[62] Graham Greenleaf, *Data Protection: A Necessary Part of India's Fundamental Inalienable Right of Privacy – Submission on the White Paper of the Committee of Experts on a Data Protection Framework for India*, 6 UNSWLRS 1,11 (2018).
[63] *Id.*

The broad exemptions granted to intelligence and law enforcement authorities under these sections has sparked a debate about the extent to which the Bill should address surveillance activities. The Committee itself has acknowledged in its Report that there is an immediate need for better legal provisions to govern surveillance activities, noting that a large amount of surveillance taking place in India today happens outside the remit of the law[64]. The Committee notes that these activities would be illegal as per the Supreme Court's judgment in *Puttaswamy*. It recommends, not only that surveillance activities should be conducted under law (and not executive order), but also be subject to oversight, and transparency requirements. However, it stops short of providing for this under the Bill itself, noting that typically, data protection and surveillance are regulated under separate laws, and such independent surveillance laws are outside the scope of the Committee's mandate. The Committee argues that the tests of lawfulness, necessity and proportionality provided for under Sections 42 and 43 are sufficient to meet the standards set out under the Puttaswamy judgment.

This raises three questions - first, what the broader contours of a law regulating intelligence and law enforcement authorities' surveillance activities should be. Second, whether this can be achieved under a data protection law. Third and more specifically, the nature of data protection, oversight and transparency regulations that processing of personal data for such activities should be subject to.

First, we look at the need for laws governing surveillance activities, and the principles that should be adopted in such laws.

It is clear from the Puttaswamy judgment that *any collection and use of personal information by government agencies would therefore impact a fundamental right available under the Constitution*. Each such use will need to be measured against standards set for permissible restrictions to such fundamental rights, to examine whether such rights have been violated or not. We have limited laws and regulations on how this right to privacy is actually protected, especially against the government's use of personal data. The Information Technology Act, 2000 has some provisions

[64] Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, *supra* note 9, at 124.

and rules on the interception and monitoring of information[65], as does the Telegraph Act, 1885[66]. However, these regulations are limited in scope.

In addition to the Indian Constitution, international human rights laws and principles also recognise the right to privacy. In the absence of specific case law or legislation dealing with such issues, the contents of international conventions and norms are significant for the interpretation of rights guaranteed under the Constitution[67]. These conventions and norms are helpful in identifying India's obligations under international law. They also provide established global principles and practices that can guide India in formulating a data protection framework that meets such obligations. Regional conventions and regulations such as the GDPR could be looked at for guidance on how government use of data can be regulated.

The Universal Declaration of Human Rights (UDHR) adopted by the United Nations General Assembly in 1948, and the International Convention on Civil and Political Rights (ICCPR), to which India is a state party[68] both recognize the right to privacy. Article 12 of the UDHR and Article 17 of the ICCPR both state as follows:

> *"1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.*
> *2. Everyone has the right to the protection of the law against such interference or attacks."*

The standards for what actions would be considered 'unlawful' or 'arbitrary' can be drawn from principles of international human rights law as well. In this context, the Human Rights Committee has explained that "*the term "unlawful" means that no interference can take place except in cases envisaged by the law. Interference*

---

[65] Information Technology Act, No.21 of 2000, INDIA CODE (2000) s.69; Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.
[66] Section 5, Telegraph Act, No.XIII of 1885 (1885) s.5; Indian Telegraph Rules, 1951.
[67] *Vishaka v. State of Rajasthan*, AIR 1997 SC 3011.
[68] UN General Assembly, *International Covenant on Civil and Political Rights*, 999 UNTS 171 (Adopted on December 16, 1966).

authorized by States can only take place on the basis of law, which itself must comply with the provisions, aims and objectives of the Covenant"[69].

The (then) United Nations High Commissioner for Human Rights has addressed these issues in her 2014 report on 'The right to privacy in the digital age'[70] (OHCHR Report).

The OHCHR Report states that the right to privacy under the ICCPR may only be limited if the following criteria are met[71]:

1. Any limitations must be provided for by law;
2. Such law must be sufficiently accessible, clear and precise. An individual should be able to look to the law and ascertain who is authorized to conduct data surveillance and circumstances under which surveillance is permissible;
3. the limitation must be necessary for reaching a legitimate aim, and must be in proportion to the aim;
4. Such limitation must be the least intrusive option available;
5. the limitation must be shown to have some chance of achieving its goal (the authorities seeking to limit the right have the onus to prove this)
6. any limitation must not render the essence of the right (to privacy) meaningless; and
7. Limitations must also be consistent with other human rights, such as the prohibition of discrimination.

The OHCHR Report also notes that even where there are laws that act as limitations or exceptions to the right to privacy, they must be further supported by effective procedural safeguards, and adequately resourced and effective institutional arrangements to support these safeguards[72]. It also states that independent civilian

[69] UNHRC, General Comment No. 16, HRI/GEN/1/Rev.9 (Vol. I) (1988).
[70] UNHRC, Report of the Office of the United Nations High Commissioner for Human Rights, *The right to privacy in the digital age*, A/HRC/27/37 (2014) available at http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf (last visited Oct 10, 2018).
[71] *Id.* at para 23.
[72] UNHRC, *supra.* note 70.

oversight agencies, as well as the involvement of all branches of government in the oversight of surveillance programmes are essential[73].

In this context, it may be helpful to take note of the restrictions allowed under the GDPR as an example of the restrictions that may be considered reasonable in India.

Under the GDPR, states may restrict obligations of data protection to safeguard national security, public security and the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security[74]. However, such a restriction must respect the essence of the fundamental rights and freedoms, must be a necessary and proportionate measure in a democratic society. In particular it must contain provisions regarding[75]:

(i) the purposes of the processing or categories of processing;
(ii) the categories of personal data;
(iii) the scope of the restrictions introduced;
(iv) the safeguards to prevent abuse or unlawful access or transfer;
(v) the specification of the controller or categories of controllers;
(vi) the storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing;
(vii) the risks to the rights and freedoms of data subjects; and
(viii) the right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction.

The recent judgment of the European Court of Human Rights in the case of Big Brother Watch and Ors. v. The United Kingdom[76] provides even more detailed

[73] *Id.* at para 37.
[74] Article 23, General Data Protection Regulation, Regulation (EU) 2016/679.
[75] *Id.* at Article 23(2).
[76] *Big Brother Watch and Others v. the United Kingdom* (applications nos. 58170/13, 62322/14 and 24960/15)

insight into the kind of oversight and transparency requirements any surveillance activities / law should meet. This case was brought before the European Court of Human Rights after the Snowden revelations showing the existence of surveillance and intelligence sharing programmes operated by the intelligence services of the United States and the United Kingdom. It was alleged that these practices were in violation of Article 8 of the European Convention on Human Rights.

In this case, the UK's bulk interception practices were found to be illegal due to lack of independent oversight of the selection and search processes involved. Specifically, the court stated that there was no independent oversight or safeguards in the process for: selecting the Internet bearers for interception, choosing the selectors and search criteria used to filter and select intercepted communications for examination, and the selection of related communications data for examination, even though this data could reveal a great deal about a person's habits and contacts.

Second, we look at whether the above-mentioned principles and guidelines can be incorporated into the Bill itself, to regulate processing of personal data by intelligence and law enforcement authorities. The Committee's Report has noted that in many jurisdictions examined, there are separate laws regulating data protection and surveillance activities. Accordingly, while the Committee has made recommendations on what laws governing data processing by intelligence and law enforcement authorities should contain, the Bill itself does not undertake such regulation. It is submitted here that simply because it is common practice in some other jurisdictions, India does not need to refrain from regulating surveillance in the data protection law. In fact, earlier versions of the privacy / data protection law that were being considered by the government did contain provisions addressing surveillance. We also acknowledge that including provisions that regulate surveillance activities by intelligence and law enforcement authorities in this Bill might entail longer or more complicated internal processes for the government, requiring coordination among different ministries as well as central and state governments.

However, it is not clear how the provisions of Section 42 and 43, which provide that data processing in the interests of security of the state and prevention, detection,

investigation and prosecution of any offence or any other contravention of law will be enforced, should this law come into force in the absence of the other laws referred to in these sections. Therefore, we recommend that even if a separate law is required for this purpose, the government should undertake this law-making process simultaneously, as it considers the Bill, to provide individuals in India the highest standards of privacy data protection at the earliest possible time.

Third we look at some of the data protection, oversight and transparency provisions in this Bill that such surveillance activities could be made subject to, irrespective of any additional laws. The Bill currently provides that data processing in the interests of security of the state and prevention, detection, investigation and prosecution of any offence or any other contravention of law is exempt from all but two provisions of the Bill. The Report argues that the criteria for data processing set forth in Section 42 and 43 provide sufficient safeguards:

(i) data processing must be undertaken in pursuant to a law
(ii) the processing must be done in accordance with the procedure established by such law made by Parliament (or State Legislature in the case of section 43)
(iii) the processing must be necessary for and proportionate to the interests being achieved
(iv) processing must be fair and reasonable in accordance with Section 4 of the Bill
(v) adequate security standards must be implemented in accordance with section 31 of the Bill

It is submitted here that this exemption granted under sections 42 and 43 is too wide, and several other provisions of the Bill can be made applicable to such processing, albeit in a modified manner where required. Some of these provisions are described below:

(i) The purpose limitations provided under section 5
(ii) The collection limitations provided under section 6

(iii) The notice requirements under Section 8 could be made applicable in a limited manner, where notice is required to be given post-facto (such measures are recommended in the OHCHR Report and provided for in the GDPR)

(iv) The data quality requirements under Section 9 – it is acknowledged that asking the data principal itself may not be a reasonable option if the aim of the surveillance activity is to be met. The intelligence / law enforcement authorities should however be required to take the utmost care to ensure that data quality is maintained, given that the decisions likely to be made about a data principal on the basis of surveillance activities could lead not only to an infringement of the right to privacy, but also other fundamental rights.

(v) The data storage limitation under section 10. This provision has been made applicable to some extent in the case of Section 43 (4), we recommend that a similar provision is included under section 42 as well.

(vi) The accountability requirements under section 11, as well as the transparency and accountability measures under sections 29, 30 (in a limited manner, where general notice of data practices is made publicly available), 33, 34, 35, and 36. It is noted in this context that it may not be feasible to have data audits and impact assessments conducted by external agencies / persons, however, capacity should be built internally (for instance within the office of the data protection officer) to undertake such exercises.

In addition to the above, specific protection should also be granted where the personal data of minors is processed in accordance with existing laws such as the Juvenile Justice (Care and Protection of Children) Act, 2015.

Additional transparency / reporting requirements should be made applicable to private data fiduciaries, regarding the number / nature and other information about requests for data by intelligence / law enforcement authorities.

9.2. Processing for the purpose of legal proceedings

Section 44 of the Bill exempts any data processing for the purpose of enforcing any legal right or claim, seeking any relief, defending any charge, opposing any claim, or obtaining any legal advice, as well as any processing by a court or tribunal that is necessary for the exercise of any judicial function from all compliances under the Bill except:

(i) Section 4 (which requires data processing to be fair and reasonable),
(ii) Section 31 (which requires certain minimum security standards to be adopted by data fiduciaries)
(iii) *Chapter VIII which deals with cross border transfers of personal data*.

We acknowledge that there is need for a reasonable exemption in the interest of protecting and enabling judicial proceedings. However, it is submitted again, that the exemption granted in this section is too wide, and that appropriate rules should be framed for the processing of data in these circumstances in a manner that balances the right to privacy and data protection of individuals. In addition, it is recommended that the provisions in this section are clarified to ensure that where such rules already exist, the Bill does not override the rules to provide for a lower standard, for instance in relation to the Juvenile Justice (Care and Protection of Children) Act, 2015, or restrictions against publication of the names of survivors of sexual assault. A broad provision in the nature of Section 46 (2) (a) which states that the exemption will not apply in case of disclosure of personal data to the public may be made applicable in relation to Section 44 (1), which is applicable to parties to a legal proceeding rather than the courts / tribunals.

Further, it may be beneficial to apply separate standards to parties directly involved in any judicial proceedings, and others such as witnesses, in a manner similar to the provisions of section 43(3).

9.3. Research, archiving or statistical purposes

Section 45 of the Bill provides that the DPA may exempt categories of research, archiving or statistical work from provisions of the Bill in certain circumstances. Data

fiduciaries cannot however be exempt from compliance with sections 4, 31 and 33 of the Bill. The DPA may exempt different categories of these activities from different provisions of the law.

It is acknowledged that these are important categories of work that need to be undertaken in the public interest, and that certain limited exceptions from data protection compliances may be required in some such cases. However, as discussed in our comments to the White Paper, we recommend that these broad exemptions are limited to research that is undertaken for non-commercial purposes, preferably by educational institutions, scientific and research institutions in order to ensure that the exemption is used for bonafide purposes only i.e. in the public interest.

In addition, it is submitted that additional provisions of the Bill, such as the collection limitation, purpose limitation, and storage limitation requirements, along with the transparency and accountability requirements should be added to the list of provisions from which there can be no derogation. The rights of data principals as provided for under Chapter VI of the Bill should also be available in the context of these activities. These additional safeguards would limit the misuse of this provision for purely profit making undertakings, and ensure that the interests of individual data principals and the public interest[77] are balanced. There is also an added benefit of reducing the burden on the DPA in making decisions about the provisions from which different categories of research may be exempt under the Bill.

There is a lot of literature available on the ethics of research itself. For instance, the concept of differential privacy came up as a tool for researchers who collect and analyze privacy-sensitive personal data and make decisions whether and how to share their research data and results with others[78]. It is recommended that this provision is finalized after consultations with experts in this field.

[77] In this context, we refer back to our discussion in Section 1.1 of these comments to clarify that economic growth of corporations in the digital area alone would not constitute public interest for this purpose.

[78] Nissim, K., Steinke, T., Wood, A., Altman, M., Bembenek, A., Bun, M., Gaboardi, M., O'Brien, D.R. and Vadhan, S., 2017. Differential Privacy: A Primer for a Non-technical Audience. *Working Group Privacy Tools Sharing Res. Data, Harvard Univ., Boston, MA, USA, Tech. Rep. TR-2017-03*.

9.4. Journalistic purposes

Section 47 of the Bill provides for exemptions to be available from several parts of the Bill where processing is undertaken for journalistic purposes.

We refer back to our comments to the questions in the White Paper on the exemptions that should be granted in the case of processing of personal data for journalistic purposes. Noting that many jurisdictions have often provided for wide exemptions, except perhaps that of maintaining technical security standards[79], we recommended that India adopt a higher standard.

We recommend that in addition to retaining security obligations, the law also clarifies that these exemptions are only available for the purpose of information that is required to be reported, written about, or referred to in some manner in the journalistic work. This would ensure that should the individuals undertaking such works be affiliated with commercial / for profit organisations, the exemption doesn't enable these organisations to undertake data processing that would otherwise be governed by the law, using such an exemption. We also recommend that principles such as storage limitation, collection limitation, which do not unduly restrict the actions of the individuals undertaking such works may continue to be applicable.

10. Chapter X: Data Protection Authority of India

Chapter X of the Bill provides for the setting up of a 'Data Protection Authority' for the purposes of the Bill. The Committee's initial approach to regulation, as discussed in the White Paper, was to put in place a co-regulation model. The White Paper also discussed self-regulation and command and control, as alternate options. In this regard, we welcome the Committee's move towards a regulatory regime based on responsive regulation[80]. The Report of the Committee discusses the concept of responsive regulation, and its application in the context of a DPA in some detail.

[79] Ministry of Electronics and Information Technology, Chapter 7, *White Paper of the Committee of Experts on a Data Protection Framework for India* (2017), http://MeitY.gov.in/white-paper-data-protection-frameworkindia-public-comments-invited (last visited Oct 10, 2018).

[80] Centre for Communication Governance, *supra.* note 7.

However, concerns have been raised regarding the application of these principles in the Bill itself.

We have not provided comments to each section in this Chapter, however, we address three main concerns in this regard below.

10.1. Independence of Committee

Section 50 of the Bill addresses the composition and qualifications for appointment of members.

The Selection Committee consists of the Chief Justice of India (or a CJI-nominated SC Justice) as Chairperson, the Cabinet Secretary, and "one expert of repute" chosen by the other two members from a list of five experts approved by the Central Government.

The powers of the Committee are limited to recommending names to the Central Government, who has the final say in appointing members of the DPA.

There is a lack of clear qualifications for appointment – with the Bill only requiring that the persons appointed must have specialised knowledge of, and at least ten years professional experience in the field of data protection, information technology, data management, data science, data security, cyber and internet laws, and related subjects, in addition to being '*persons of ability, integrity and standing'*. This opens up potential for predominance of bureaucrats who may technically meet these ambiguous qualifications but could compromise independence of the DPA.

Additionally, there is no explicit provision for a wide range of stakeholders to be represented in the DPA. This lack of representation is particularly important in light of the stipulation that any defect in the appointment of a chairperson or member will not invalidate the proceedings of the DPA (section 55 of the Bill), and the considerable discretionary powers that the DPA has been endowed with, which include the power to specify reasonable purposes for which personal data and sensitive personal data may be processed (section 60(2)).

Section 51 provides the terms and conditions of appointment of members of the DPA.

Some measures have been taken to avoid regulatory capture by data fiduciaries, however:

1. While the chairperson and members of the DPA are barred from working in any capacity with a significant data fiduciary during and two years after their tenure at the DPA, there is no bar on a member having worked with a significant data fiduciary (which is to be classified as such by the government) immediately *prior* to appointment –could make complete independence more difficult to monitor and enforce.

2. There are insufficient safeguards in place to ensure the independence of the DPA from government interference in appointments.

This is further highlighted by Section 107, which empowers the Central Government to make rules on procedure to be followed by the selection Committee for the DPA under Section 50(3), its salaries and allowances under Section 51(2), the selection, qualifications, terms of employment of the Adjudicating Officer under Section 68(2) and the Appellate Tribunal under Sections 80(1), 81, and 82(3).

In addition to the above, Section 98 provides that:

1. *The Central Government can issue directions to the DPA as it may consider necessary for the sovereignty and integrity of India, the security of the State, friendly relations with foreign States or public order, which provides ample scope for interpretation.*
2. *While the DPA can express its views on the same, it is bound by government directions on matters that the government determines to be relating to policy.*

Such a wide scope for government interference significantly undermines the independence of the DPA.

10.2. Transparency in appointment and proceedings

1. There are no provisions to make the deliberations and process of appointing the members of the DPA public and transparent, despite the stated push for transparency and accountability.
2. Minutes of the meetings of the DPA should also be made public (subject to reasonable security/ privacy concerns).
3. The DPA is to advise Parliament and the Central and State governments on measures required to guarantee data protection [Section 60(2)]. This should be supported by mandating that these measures (laws, rules, regulations or otherwise) which impact privacy should be approved by the DPA after a public consultation.
4. The Bill is unclear on whether the adjudicatory body set up can be approached directly or whether complaints should first be addressed to the data fiduciary.

The idea of centralisation, i.e. one DPA for the entire country is also questionable since state agencies and private sector companies throughout the country will all be considered data fiduciaries. Almost all, if not all individuals residing in India will effectively be considered data principals under this Bill, and will need to have access to the DPA in order to enforce their rights. Under these circumstances, a network of regional DPAs would be more effective than a hub and spoke model.

10.3. Responsive Regulation

The Report concludes that responsive regulation via an enforcement pyramid is the preferred option of enforcement, an approach also suggested in our comments to the White Paper[81].

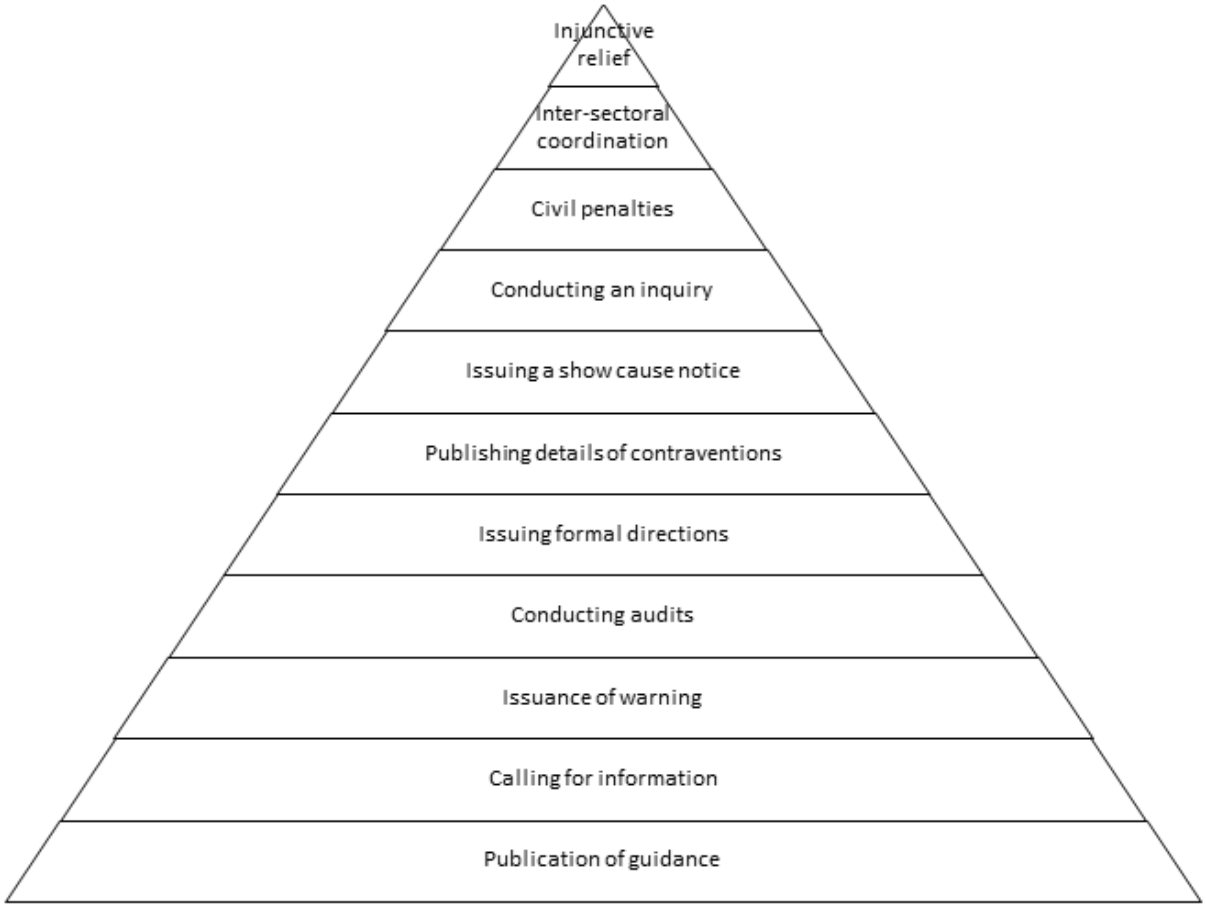
Adopting a responsive regulation mechanism would introduce tripartism to regulation, and involve a multi-stakeholder approach to ensure compliance and avoid regulatory capture[82]. An enforcement pyramid consists of regulatory strategies in the

[81] Centre for Communication Governance, *supra.* note 7 at 5

[82] John Braithwaite, *Responsive Regulation*, http://johnbraithwaite.com/responsive-regulation/ (last visited Oct 3, 2018).

form of proactive and reactive sanctions that can be conceptually arranged in the form of a pyramid, with the bottom layers being less coercive, less intrusive and less costly[83]. In using responsive regulation, it is advisable to lay out an explicit enforcement pyramid (i.e. clearly map out regulatory responses to each potential action) in order to ensure higher compliance.

An enforcement pyramid that could potentially be utilised by the DPA, that ranges from capacity building to deterrence and incapacitation could include the following escalating stages:



1. Publication of guidance in the form of responses to queries by data fiduciaries/ processors which can also be made available to the public on its website
2. Calling for information from data fiduciaries/ processors in case of possible violation of the Act

[83] *Id.*

3. Issuance of warning to the concerned data fiduciary/ processor if any of its activities is likely to cause a violation of the Act
4. Conducting audits to check whether the activities of the data fiduciary/ processor are compliant with the provisions of the Act
5. Issuing formal directions to data fiduciaries/ processors to ensure compliance with the Act
6. Publishing details of contraventions by data fiduciaries/ processors on its website for access to the public
7. Issuing a show cause notice to the concerned data fiduciary/ processor prior to initiating an inquiry into its practices
8. Conducting an inquiry of the concerned data fiduciary/ processor if there is a reasonable belief that the Act is being violated
9. Levying a civil penalty on the data fiduciary/ processor if it is found guilty of violating the Act, the quantum of which will be determined by the gravity of the violation as well as any history of previous violations
10. Consulting with other regulators and ensuring inter-sectoral coordination in case of concurrent jurisdiction in a particular matter
11. Injunctive relief in the form of temporarily suspensions, and cease and desists to data fiduciaries who have been found guilty of violating the Act

As per Chapter 9(b) of the Report, this enforcement pyramid will consist of the following stages[84]:

1. Issuance of direction
2. Power to call for information
3. Publication of guidance
4. Issuance of public statement
5. Codes of practice
6. Conducting inquiries

[84] The Report finds substantial basis for this in the White Paper by Dvara Research. *See* Beni Chugh et al., Effective Enforcement of a Data Protection Regime: A Model for Risk-Based Supervision Using Responsive Regulatory Tools (2018), https://www.dvara.com/blog/wp-content/uploads/2018/07/Effective-Enforcement-of-a-Data-Protection-Regime.pdf (last visited Oct 10, 2018).

7. Injunctive relief
8. Inter-sectoral coordination

While the Bill itself does not explicitly mention responsive regulation, it enumerates a number of the principles of responsive regulation mentioned in the Report. However, it is submitted that the responsive regulation model incorporated in the Bill could be modified to include certain stages that could be mobilised before a potential breach in order to avoid climbing up the pyramid to inquiries and sanctions.

Moreover, notwithstanding the powers granted to the DPA, it must be kept in mind that Section 98 empowers the Central Government to issue any directions it deems fit and "necessary in the interest of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States or public order", which the DPA is bound to abide by.

The Bill under Section 60(2)(l) mandates that the DPA shall publish codes of practice under Section 61 on its website, however, it does not require that it publish responses to clarifications sought by data fiduciaries/ processors and other such public guidance. This would be a helpful measure to ensure that there is no ambiguity regarding the Act and Rules that would later have to be dealt with through escalation up the pyramid.

Section 63 of the Bill states that the DPA may order a data fiduciary/ processor to provide any information required to discharge its functions, pursuant to any other provisions.

Section 65(1)(a) states that the DPA may issue a warning to the data fiduciary/ processor after conducting an inquiry. However, it may be worthwhile to include this stage *before* the inquiry stage if a prima facie investigation into the information provided under Section 62 indicates that any potential violations might occur, thus allowing the entity the opportunity to correct this error before commencing an inquiry and avoiding unnecessary costs.

Annual data audits conducted by independent auditors in the manner specified by the DPA under Section 35 of the Bill will help ensure compliance and avoid

unnecessary intervention by the DPA when avoidable. However, the effectiveness of this provision depends on the DPA ensuring that designated data auditors are sufficiently qualified and independent, which will have to be reinforced in the Rules for their appointment. Section 60(2)(f) helps in this regard by stating that the data trust scores of every significant data fiduciary must be published on the DPA website.

The powers of the DPA to issue formal directions have been enumerated throughout the Bill in some detail. Section 62 specifically empowers the DPA to issue directions in the course of its duties after giving data fiduciaries/ processors reasonable opportunity to be heard. This power is expanded further in specifying reasonable purposes for processing of data (Section 17), what constitutes sensitive personal data, the grounds under which they may be processed, and additional safeguards that may be required for processing of personal data (Section 22), and the mandate that the DPA issue directions for processing of personal and sensitive personal data of children (Section 23).

It is important that instances of contraventions by data fiduciaries be documented and made available to the public. This serves to not only inform the public of the safety of their data, but also acts as a possible deterrent to violating the Act. This has been covered by Section 60(2)(m), which aims to promote public awareness.

Section 64 mandates that the Inquiry Officer shall first issue written notice to the concerned data fiduciary/ processor, subsequent to which it can conduct an inquiry, especially where it believes the interests of a data principal may be compromised because the data fiduciary/ processor is acting detrimental to their interest, or that a data fiduciary/ processor has violated the data protection law. For instance, in the case of a personal data breach (Section 32), the data fiduciary is to inform the DPA in the prescribed manner. However, considerable power is given to the DPA in determining whether to inform the data principal of the breach of their data, as the clause does not mandate that the DPA must inform the data principal in all circumstances.

The decision to incorporate an adjudicatory wing within the DPA under Section 68 highlights potential questions of regulatory burden[85] as well as potential conflict of interest. In a similar instance, the Telecom Regulatory Authority of India was initially envisaged to exercise both regulatory and adjudicatory functions. However, the resulting regulatory burden imposed on TRAI did not allow it to adequately perform its regulatory functions, leading to a 1997 amendment that established the Telecom Disputes Settlement and Appellate Tribunal. The aim of the establishment of a separate and independent dispute settlement wing was "bringing about functional clarity, strengthening the regulatory framework and the disputes settlement mechanism" which was achieved by "bringing about a clear distinction between the recommendatory and regulatory functions of Telecom Regulatory Authority of India (TRAI) by making it mandatory for Government to seek recommendations of TRAI in respect of specified matters and by the setting up of a separate dispute settlement mechanism."[86] Burdening the newly formed DPA with the dual tasks of regulation and dispute resolution will only serve to undermine its own efficiency and increase costs and procedural complexity. In contrast, an independent adjudicatory body (in the same form as the TDSAT) would ensure no conflict of interest and maximise efficiency in dealing with disputes, which is of particular importance in cases of data breaches.

11. Others

11.1. Penalties, Offences and Compensation

We appreciate the Committee's call for different approaches in the event of violation of the provisions of the Bill in the form of penalties, remedies, and criminal offences. One of the reasons that the Data Protection Rules under the IT Act, have not been enforced properly, is the lack of appropriate mechanisms to deter and prevent violations.

---

[85] Regulatory burden is the administrative cost of a regulation in terms of dollars, time and complexity What is compliance burden? -*See* SEARCHCOMPLIANCE, https://searchcompliance.techtarget.com/definition/compliance-burden (last visited Oct 3, 2018).

[86] TELECOM DISPUTES SETTLEMENT APPELLATE TRIBUNAL, https://web.archive.org/web/20120508223006/http://www.tdsat.nic.in/profile2.htm (last visited Oct 3, 2018).

In this regard, we have some concerns about the way the provisions of the Bill dealing with compensation to be provided to data principals who are affected by a violation under the Bill, under Section 75.

A significant difference in situations that call for a penalty vis-à-vis those that call for compensation to be paid to a data principal is the need to prove harm. The Bill also provides a definition for such harm[87], under which harm includes:

(i) bodily or mental injury;
(ii) loss, distortion or theft of identity;
(iii) financial loss or loss of property,
(iv) loss of reputation, or humiliation;
(v) loss of employment;
(vi) any discriminatory treatment;
(vii) any subjection to blackmail or extortion;
(viii) any denial or withdrawal of a service, benefit or good resulting from an evaluative decision about the data principal;
(ix) any restriction placed or suffered directly or indirectly on speech, movement or any other action arising out of a fear of being observed or surveilled; or
(x) any observation or surveillance that is not reasonably expected by the data principal.

The Bill does not however address the manner in which a data principal is to identify that harm has been caused, and the question of where the burden of proof will rest in such a situation. One of the difficulties in enforcement of data protection laws, is the proving of harm. Whereas some harm, for instance in the form of bodily injury may be easier to prove, others may pose significant burdens. In the age of big data, it may become impossible for a data principal to be aware of discriminatory activities, for instance discriminatory pricing in advertisements shown on social media platforms. While discriminatory treatment in itself is a harm, such treatment could also lead to other harms such as financial loss. However, unless there are reports

[87] The Personal Data Protection Bill, s.3(21) (2018).

showing that such practices exist, a data principal may not even be aware of the potential for such harm, leave alone any actual harm they suffer.

In order to address these situations, it is important to ensure that adequate systems are built in, using existing provisions under the Bill and other mechanisms. We have already discussed the need for notifying individuals of breaches of their personal data above. Such notification would not only allow the data principal to protect themselves better and take action to prevent further breach, but also seek compensation where appropriate. In addition, we recommend that a suitable mechanism is built in to the law by way of which, if a penalty is levied, and it is likely that harm has occurred (irrespective of a breach, as defined for the purpose of breach notifications), data principals are be informed of such likelihood. Processes to assist data principals to learn about and then access compensation should also be put in place.

We also recommend in this context, that the law should enable and advocate the adoption of new means of engagement between the data principal, data fiduciary and the DPA in order to allow for better enforcement[88].

11.2. Overriding effect of the data protection law

Section 110 of the Bill provides that unless expressly provided by the law, the provisions of the data protection law will have an overriding effect where there is inconsistency between the Bill and other laws / legal instruments.

We note here, that a comprehensive data protection law is the minimum requirement for protection of personal data in India. However, the law should enable the adoption of higher standards for protection of personal data, particularly in relation to sensitive sector specific personal data, such as financial information / health information. We recommend that such language is built in accordingly.

[88] For instance, data due process mechanisms suggested by academics such as Kate Crawford, Jason Schultz, and Danielle Citron – *See* Kate Crawford & Jason Schultz, *Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms*, 55 B.C.L. Rev. 93 (2014); Danielle K. Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249, 1256 (2008).

CENTRE FOR COMMUNICATION GOVERNANCE AT NATIONAL LAW UNIVERSITY, DELHI

COMMENTS TO WHITE PAPER OF THE COMMITTEE OF EXPERTS ON A DATA PROTECTION FRAMEWORK FOR INDIA[1]

1. Table of Contents

[1]With contributions from Smitha Krishna Prasad, Chinmayi Arun, Aditya Singh Chawla, Geetha Hariharan, Ira Dhasmana, and Aakanksha Kaul.

2. Executive Summary

The Centre for Communication Governance (Centre) is an academic research centre within the National Law University, Delhi and is dedicated to working on information law and policy in India. It seeks to embed human rights and good governance within communication policy and protect digital rights in India through rigorous academic research and capacity building.

The protection of the right to privacy, and particularly informational privacy is an integral aspect information law and policy. We welcome the efforts of the Ministry of Electronics and Information Technology (MEITY), Government of India and the Committee of Experts set up by MEITY, in this direction.

We have provided our responses to the White Paper (defined below) that the Committee has published below. In preparing these comments, we have drawn upon

existing principles of Indian law, including the Supreme Court's judgment in *Puttaswamy v. Union of India*, and India's experience with data protection and other laws where relevant, as well as international law, and experiences of other jurisdictions where relevant.

In this section of the document, we summarise our responses to the Committee's White Paper.

2.1. Key Principles

It is important to have a law that is based on strong principles that work towards protecting the rights of individuals. The law must be clear and allow for unambiguous enforcement by authorities, and it must empower citizens. Any exceptions to the rights-based protections should be narrowly crafted, and for specific, defined purposes. Privacy by design and privacy by default should be incorporated in any principles adopted by the Committee.

We suggest that the Committee discusses these principles in a detailed report as well as the statement of objects and reasons in order to enable interpretation of the law.

2.2. Part II: Scope and Exemptions

For territorial scope, a balanced approach would help avoid overly broad and uncertain claims of (extra territorial) jurisdiction, while also ensuring that the rights of individuals in India are protected.

We recommend against data localisation. The data protection rules must however be applied strictly to the flow of personal information from India to other countries without restriction of the flow of data.

The data protection law should protect the rights, and the data / information of natural persons. It should protect a wide range of data that identifies or is capable of being used to identify individuals. Special categories of 'sensitive' data should receive additional protection.

We recommend strong safeguards for the information/ data of natural persons. Both natural and juristic persons, whether public or private entities, should be required to follow the data protection rules in their collection and use of data.

The law must define 'processing' or use of data in a wide and inclusive manner. The law should account for both automated and manual processing of data.

Distinctions may be made to account for the nature of processing by different natural / juristic persons i.e. data controllers and data processors. These distinctions should be made for the purpose of ensuring ease of access to rights and remedies by the data subject. The obligations of the different types of persons in this respect, i.e. the data controllers and data processors should not be limited because of such distinctions.

In order to ensure adequate protection is provided to individuals, the data protection law should apply retrospectively to data already in the possession of controllers and processors.

Any exceptions should be limited to reasonable, and narrowly defined parameters that are defined / outlined under law, to the extent possible. In particular, exceptions on the grounds of national security / (criminal) law enforcement should be compliant with international human rights law, carefully crafted, and provide for adequate procedural safeguards.

Exceptions for both targeted or mass surveillance should be limited to specific purposes, and not be crafted in a manner that would render the fundamental right to privacy (or other basic human rights) meaningless. The minimum safeguards that need to be adopted (on the basis of international human rights principles) are as follows: (i) any exceptions should be prescribed by a clear, precise and accessible law, (ii) the law should indicate who is authorised to conduct data surveillance and in what circumstances, (iii) the exception should be for the purpose of a legitimate aim, and also be shown to have some chance at achieving such aim, and (iv) the actions to be undertaken under the scope of such an exception should be necessary and proportionate to such aim, and must be the least intrusive manner in which such aim can be achieved. The law should also ensure that individuals whose data is used for these purposes have the right to know of such use, and access to remedies.

Adequate procedural checks and balances should also be built in, to ensure accountability and transparency in the implementation of the data protection law and its exceptions.

2.3. Part III: Grounds of Processing, Obligation on Entities and Individual Rights

This part covers internationally accepted data protection principles. It includes notice, consent, purpose specification, storage limitation and individual rights to access, review and correct data, and object to processing of data.

These principles must be incorporated in the Indian law. However additional safeguards will be necessary to account for new technology and uses of data.

Consent of the data subject should continue to be a pre-requisite for data collection and processing. The manner in which notice is provided and consent obtained for the collection and processing of personal data must ensure individuals are providing informed and meaningful consent.

However, the law should take note of the issues that have been highlighted in the context of collection and use of big data, and other situations where consent is not typically informed and / or meaningful. Consent should be unbundled, and separated in the context of collection of data that is used for different purposes, as well as data that is not necessary for the service in question.

The law should provide substantive safeguards to ensure that the contractual nature of consent is not misused to work around the implementation of data protection principles. These safeguards can include purpose and storage limitation requirements, and individual access rights, in order to ensure that data controllers cannot contract out of certain minimum obligations and responsibilities. Higher levels of protection should be provided for in relation to sensitive personal information.

Additional safeguards should also be put in place in relation to consent and other requirements applicable to collection and processing of children’s data.

Individual access rights, including those mentioned in the White Paper, should be emphasised, and data subjects should be empowered to exercise as much control over the processing of their data as possible.

2.4. Part IV: Regulation and Enforcement

We disagree with the White Paper's focus on 'co-regulation'. Despite its significant advantages especially in terms of industry involvement, co-regulation is only successful under certain circumstances. It poses risks like regulatory capture and domination of incumbent industry players with greater resources such that new entrants with less capacity to engage with the regulator find themselves disadvantaged.

Ideally, the data protection framework must function through an open consultative process. The enforcement mechanism for the framework must offer consumers and users at least as much access as industry has, accounting for the disparity in resources. A central and independent data protection authority must be created, and provided with adequate resources and powers to administer the data protection law. Principles of 'responsive regulation' can be used to build a system under which the regulatory mechanism takes into account the differing motivations of different actors and builds this into its responses.

The system should provide accountability mechanisms that are again responsive, and relevant to the nature of the business / operations of the data controller / processor in question. We discuss in detail in our submission. One important requirement in this regard is the implementation of measures to ensure that notifications are made by controllers to the authorities and affected individuals, of any breach in data security, in a timely manner. The notification must be detailed, and include information about the potential consequences of the breach, and suggest possible measures that data subjects may take to insulate themselves against such consequences. In order to incentivise data controllers to disclose information about breaches, penalties must be imposed for failure to do so, in cases where the disclosure was warranted.

The data protection law must provide for strict and effective enforcement measures. In addition, a strong framework for remedies to individuals who are affected by

violation of the law. This should include but not be limited to compensation. The data protection authority should be given powers to conduct initial investigations into any violation of the data protection law. Such authority and data controllers should be required to maintain records of any issues raised by data subjects, as well as the actions that were taken to address the same. The data protection authority should also be empowered to impose penalties, and order compensatory payments by the data controller to the data subject. An adequate appellate mechanism, with an independent adjudicatory authority that is equipped both in terms of technical and legal knowledge, as well as resources and infrastructure to take on such a role, should be put in place.

2.5. Procedural Concerns

In addition to our substantial comments on the contents of data protection law itself, we take this opportunity to welcome the efforts of MEITY and the Committee in working towards the enactment of a data protection law in India. However, we note that there have been some concerns about the lack of transparency in the composition and working of the Committee. We note that the Committee is indeed providing some platforms for other stakeholders to participate in the process, such as the call for comments to the White Paper, and the public consultations. However, we note that stakeholders have not been provided adequate time to prepare for these consultations.

We appreciate the efforts of the Committee, and also urge the committee to be more open and transparent about its functioning in the future. We request the Committee to consider adding members that would better enable it to build an effective data protection framework for India. We also request the Committee to continue the public consultation process after written comments to the White Paper are provided by the various interested stakeholders.

3. Introduction

Over the past few months, we have seen an increasing number of discussions on the concepts of privacy and data protection in India. In August, the Supreme Court of

India has affirmed that the right to privacy is a fundamental right under the Indian Constitution, in a detailed judgment in *Puttaswamy v. Union of India*[2]. During the hearings for this case, the Government of India informed the Court that data protection laws would be put in place in India, and set up a Committee of Experts (Committee) to identify key data protection issues in India and recommend methods of addressing them[3]. The Telecom Regulatory Authority of India (TRAI) called for comments in a consultation on "*Privacy, Security and Ownership of the Data in the Telecom Sector*"[4] (TRAI Consultation Paper).

The white paper[5] (White Paper) that these comments respond to, was published by the Committee set up by the Ministry of Electronics and Information Technology (MeitY), Government of India.

It is clear that there is an immediate need for better laws and regulations on privacy and data protection in India, across sectors. We appreciate the efforts of MEITY and the Committee in this regard. We note that there have been some concerns about the lack of transparency in the composition and working of the Committee. There have also been several calls for the Committee to consult with stakeholders, and note that to this effect the Committee has both published the White Paper, and held consultations in various cities across the country[6]. These steps are welcome, however, we note that stakeholders have not been provided adequate time to prepare for these consultations. We appreciate the efforts of the Committee, and

---

[2] *Justice K.S Puttaswamy (Retd.)* v. *Union of India,* (2017) 6 MLJ 267.

[3] Ministry of Electronics and Information Technology, Office Memorandum No. 3(6)/2017-CLES, *available at*http://meity.gov.in/writereaddata/files/MeitY_constitution_Expert_Committee_31.07.2017.pdf (Last visited on January 30, 2018).

[4] Telecom Regulator Authority of India, *Consultation Paper on Privacy, Security and Data Ownership in the Telecom Sector*, (2017) *available at* http://trai.gov.in/sites/default/files/Consultation_Paper%20_on_Privacy_Security_ownership_of_data_09082017.pdf (Last visited on January 30, 2018) ["White Paper"].

[5] Ministry of Electronics and Information Technology, *White Paper of the Committee of Experts on a Data Protection Framework for India,* (2017) *available at*http://meity.gov.in/white-paper-data-protection-framework-india-public-comments-invited (Last visited on January 30, 2018).

[6] Ministry of Electronics and Information Technology, Press Release, *available at* http://meity.gov.in/writereaddata/files/public_consultation_on_white_paper.pdf (Last visited on January 30, 2018).

also urge the committee to be more open and transparent about its functioning in the future. We request the Committee to consider adding members that would better enable it to build an effective data protection framework for India. We also request the Committee to continue the public consultation process after written comments to the White Paper are provided by the various interested stakeholders.

Our comments draw upon the constitutional right to privacy, and criticisms of the current data protection regime including those in the report of the Group of Experts, headed by (Retd.) Justice A. P. Shah to begin with. We have also discussed various laws and policies in place across jurisdictions, in order to highlight good practices, and key concerns that any new data protection regime must address.

4. Privacy as a Fundamental Right

Before we answer the specific questions set out in the White Paper, we wanted to highlight a few of the observations made by the Supreme Court in *Puttaswamy v. Union of India*[7]. We have included an excerpt from our submissions to the TRAI Consultation Paper[8] below:

> The Supreme Court has affirmed and recognised that the right to privacy is a fundamental right under Article 21 of the Constitution. It may also be drawn as a fundamental right under any of the other fundamental rights recognised under the Constitution. Accordingly, the Court has observed that although the right is not absolute, any restrictions imposed by the State on the right to privacy must be 'reasonable restrictions'. These reasonable restrictions must meet the various tests for limitations / violations of the right, applicable in relation to the relevant fundamental rights. *At the same time, the Court has also noted that there is a positive obligation for the state to create a regulatory environment that allows individuals to enjoy their right to privacy*.

[7] (2017) 6 MLJ 267.

[8]Centre for Communication Governance at National Law University Delhi, *Comments to Telecom Regulatory Authority of India's Consultation Paper on Privacy, Security and Ownership of the Data in the Telecom Sector* (November 15, 2017), available at http://trai.gov.in/sites/default/files/Nlud_15112017.pdf (Last visited on February 25, 2018).

In recognising privacy as a fundamental right, J. Chandrachud, J. Chelameswar, J. Kaul and J. Nariman have, in their various opinions have observed that informational privacy is an important aspect of such privacy in this day and age. J. Chandrachud has noted the setting up of the Committee of Experts, and recommended that the central government puts in place a robust data protection regulation in place in order to protect this right.

In the observations that lead up to his conclusions, J. Chandrachud has also noted that data protection regulation is a complex issue which needs to address many aims[9]. The first of these aims is the individual's right to be left alone. Second and more importantly, the regulation needs to ensure that the individual's identity is protected. Third, the individual's autonomy in making decisions about the use of data about them, and their right to know how this data is being used must be protected. Fourth, data protection regulation should ensure that data is not collected in a manner that is discriminatory towards anyone.

We have highlighted the observations made by the Supreme Court in our comments to the TRAI's Consultation Paper on "*Privacy, Security and Ownership of the Data in the Telecom Sector"* and in our earlier writing on the *Puttaswamy*[10] case.

We have also highlighted the fact that any data protection law that comes into force in India must work towards allowing people to exercise a fundamental right, in our

[9] (2017) 6 MLJ 267), Chandrachud J.'s opinion, paras 177-178.

[10] *See*: Chinmayi Arun, *A Judgment for the Ages,* THE HINDU (August 3, 2017) *available at* http://www.thehindu.com/opinion/lead/a-judgment-for-the-ages/article19409905.ece (Last visited on January 30, 2018); Chinmayi Arun, *Data privacy: Great idea, but there's room for the State to step in,* The New Indian Express (August 25, 2017) *available at* http://www.newindianexpress.com/opinions/2017/aug/25/data-privacy-great-idea-but-theres-room-for-the-state-to-step-in-1647907.html (Last visited on January 30, 2018); Smitha Krishna Prasad, *The Right To Privacy And How It Will Play Out In Our Lives,* HUFFINGTON POST (August 30, 2018) *available at* http://www.huffingtonpost.in/smitha-krishna-prasad/the-right-to-privacy-and-how-it-will-play-out-in-our-lives_a_23190236/ (Last visited on January 30, 2018).

interventions during the public consultation that MEITY and the Committee of Experts held in Delhi.

However, we also note with concern that several sections of the White Paper focus on the need to encourage growth of the digital economy, as well as the costs of compliance should certain principles / methods of data protection be adopted[11]. Many of the stakeholders at the public consultation have also expressed concerns about data protection laws stifling the growth of industry / increasing the costs of compliance for industry[12].

We reiterate the fact that the right to privacy is a recognised fundamental right under the Indian Constitution[13]. As discussed above, the right to protection of personal information has also been recognised as an integral part of this right. In this context, we note that the primary function of any data protection law should be to protect the data and privacy of individuals, and therefore protect the rights of such individuals themselves[14]. While we appreciate the concerns raised, we wish to note that innovation cannot override basic human rights.

5. Current data protection laws

Our assessment is that the current data protection rules are insufficient to protect the interests of individuals whose data is used by both the public and private sectors.

---

[11] White Paper, at 50, 153.

[12] Nikhil Pahwa*, Liveblog on Data Protection Consultation open house Delhi,* MEDIANAMA (January 5, 2018) *available at* https://www.medianama.com/2018/01/223-data-protection-consultation-open-house-live/ (Last visited on January 30, 2018).

[13] (2017) 6 MLJ 267.

[14] A. Saraph, *The Srikrishna Committee White Paper on Data Protection,* THE ECONOMIC TIMES (November 28, 2017) *available at* https://tech.economictimes.indiatimes.com/catalysts/the-purpose-of-data-protection-then-is-to-protect-people/2725 (Last visited on January 30, 2018); A. Gupta, *Rights in the Age of Big Data*, THE HINDU (January 13, 2018) *available at* http://www.thehindu.com/todays-paper/tp-opinion/rights-in-the-age-of-big-data/article22433037.ece (Last visited on January 30, 2018); *Data protection about protecting people,* THE FINANCIAL EXPRESS (December 16, 2017) *available at* http://www.financialexpress.com/industry/technology/at-indian-express-thinc-data-protection-about-protecting-people/976192/ (Last visited on January 30, 2018).

We agree broadly with the position in the White Paper that there is a need to "make a comprehensive law to adequately protect personal data in all its dimensions and to ensure an effective enforcement machinery for the same"[15].

The White Paper has also referred to the report of the Group of Experts, headed by (Retd.) Justice A. P. Shah, in 2012 (GOE Report)[16]. We note that this GOE report also found the various data protection rules that are currently applicable, inadequate[17]. The GOE Report has examined best practices and principles of data protection laws across the world, and recommended the incorporation of a set of 9 national privacy principles in any proposed privacy law[18]. The GOE Report has then gone on to find that the existing data protection regulations do not meet the requirements set forth in these principles[19].

The existing data protection laws, including particularly the provisions under the Information Technology Act, 2000 (IT Act) and the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 under the IT Act (IT Rules) have also been criticised by industry and civil society members alike[20].

In our comments below we address some of the issues raised in the different parts and sections of the White Paper. We have tried to provide our comments in the form of responses to the specific questions posed where possible. However, we note that in many cases restricting our responses to the questions as provided in the White

---

[15] White Paper, at17.

[16] Report of the Group of Experts on Privacy, *available at* http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf (Last visited on January 30, 2018) ["Report of the Group of Experts on Privacy"].

[17] Report of the Group of Experts on Privacy, Chapter 4.

[18] Report of the Group of Experts on Privacy, Chapter 3.

[19] Report of the Group of Experts on Privacy, Chapter 4.

[20] *Outsourcing: India adopts new privacy and security rules for personal information*, LEXOLOGY (August 9, 2011) *available at*https://www.lexology.com/library/detail.aspx?g=9a9b9ec0-e390-45b8-a6f1-4363e29e9af3 (Last visited on January 30, 2018); Bhairav Acharya, *Comments on the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011*, *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 visited on January 30, 2018).

Paper would result in an incomplete assessment of the issues that are being discussed. In such cases we have supplemented our responses with an introductory note to the part or section being discussed.

6. Key Principles

We note that the White Paper has proposed that India's data protection framework must be based on 7 key principles:

1. Technology agnosticism- The law must be technology agnostic. It must be flexible to take into account changing technologies and standards of compliance.

2. Holistic application- The law must apply to both private sector entities and government. Differential obligations may be carved out in the law for certain legitimate state aims.

3. Informed consent- Consent is an expression of human autonomy. For such expression to be genuine, it must be informed and meaningful. The law must ensure that consent meets the aforementioned criteria.

4. Data minimisation- Data that is processed ought to be minimal and necessary for the purposes for which such data is sought and other compatible purposes beneficial for the data subject.

5. Controller accountability- The data controller shall be held accountable for any processing of data, whether by itself or entities with whom it may have shared the data for processing.

6. Structured enforcement- Enforcement of the data protection framework must be by a high-powered statutory authority with sufficient capacity. This must coexist with appropriately decentralised enforcement mechanisms.

7. Deterrent penalties- Penalties on wrongful processing must be adequate to ensure deterrence.

We note that it is important to have a law that is based on strong principles that work towards protecting the rights of individuals. If the Committee is to adopt certain

principles as the basis of their recommendations, and the basis for any future data protection law, it is important to ensure that these principles are available to aid the interpretation of such a law. It is therefore recommended that the Committee considers incorporating these principles in some form of introductory section in the law, such as the statement of objects and reasons. It is also recommended that a clear message about the rights-based nature of the law is included in such a section.

However, we do note that the principles as listed in the White Paper are in some cases ambiguous, and in certain cases detract from globally established principles of data protection. Should the Committee consider including data protection principles in their recommendation, or any draft law, the principles as provided in the White Paper will need to be amended and updated.We have listed our comments on some of the individual principles described in the White Paper below.

***Principle 1: Technology agnosticism – The law must be technology agnostic. It must be flexible to take into account changing technologies and standards of compliance*.**

CCG Comments: We agree that the principles must be technology agnostic and flexible enough to be applicable to new technologies and means of using data that we may not anticipate today. However, it is not clear what changing 'standards of compliance' are.

The manner in which data protection rights are exercised may change with changing technology, similar to the manner in which the right to privacy itself has evolved over the past century. However, in relation to compliance, we note that it is important that the law is clear and allows for unambiguous enforcement by authorities[21], and always empowers citizens.

[21] Graham Greenleaf, *Data Protection: A Necessary Part of India's Fundamental Inalienable Right of Privacy – Submission on the White Paper of the Committee of Experts on a Data Protection Framework for India,* (2018) available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3102810 (Last visited on February 25, 2018).

Principle 2: Holistic application- The law must apply to both private sector entities and government. Differential obligations may be carved out in the law for certain legitimate state aims.

CCG Comments: We agree with this principle. We suggest that the language used for this principle may be amended slightly to emphasise on the fact that both private sector entities, and all government agencies that collect, process, and use personal information will need to comply with the law. The law itself may provide different provisions and in some cases limited exceptions, that are applicable depending upon the nature of processing concerned. It should be clarified however, that in the event of any violations of the data protection principles by the State, such violations must adhere to the spirit of the Constitution in order to be considered permitted exceptions.

Principle 3: Informed consent- Consent is an expression of human autonomy. For such expression to be genuine, it must be informed and meaningful. The law must ensure that consent meets the aforementioned criteria.

CCG Comments: We agree that consent, and particularly informed and meaningful consent is an important aspect of data protection law. However, we note that one of the most common criticisms of data protection law across jurisdictions is that there is too much reliance on consent, resulting in concerns regarding the problem of bounded rationality. Our concerns in this regard are elaborated in our comments on the chapter addressing the issue of consent, below.

It may be useful to add that the terms of consent must work within both the letter and the spirit of the data protection law.

Principle 4: Data minimization - Data that is processed ought to be minimal and necessary for the purposes for which such data is sought and other compatible purposes beneficial for the data subject.

CCG Comments: We agree that data minimization should also be an important principle of data protection law. However, we note that the term ‘other compatible purposes beneficial for the data subject’ is ambiguous, and could undermine the principle of purpose limitation which is a long-standing data protection principle.

Principle 5: Controller accountability- The data controller shall be held accountable for any processing of data, whether by itself or entities with whom it may have shared the data for processing.

CCG Comments: We agree that accountability is a key principle of data protection. However, we note that strict controller accountability is only one aspect of accountability. The data controller should be liable directly to the data subject, in relation to both exercise of the data subject's rights, and any claims for compensation. However, both data controllers and data processors should be accountable and liable for any wrongful processing or breach of the data protection law.

Principle 6: Structured enforcement- Enforcement of the data protection framework must be by a high-powered statutory authority with sufficient capacity. This must coexist with appropriately decentralised enforcement mechanisms.

CCG Comments: We agree that proper and structured enforcement of the data protection law is key to its implementation. In addition to the capacity to enforce, statutory authorities, at any level should be both empowered and required to ensure that the data protection law is enforced in an unambiguous, and consistent manner. Appropriate checks and balances should be in place to ensure such enforcement.

Principle 7: Deterrent penalties- Penalties on wrongful processing must be adequate to ensure deterrence.

CCG Comments: We note that any enforcement and remedies frameworks should empower citizens to access redressal mechanisms. We suggest that this principle also incorporates language to this effect.

In addition to the above, we recommend that all data controllers and processors should be encouraged to adopt the concepts of privacy by design and privacy by default. These concepts would make valuable addition to any data protection principles that are meant to form the basis of India's data protection law.

7. Part II: Scope and Exemptions

7.1. Chapter 1: Territorial and Personal Scope

Our responses to the questions raised in this chapter are below:

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

CCG Response: A useful definition of 'extra territorial jurisdiction' is provided by the International Law Commission (ILC) which defines it as "an attempt to regulate by means of national legislation, adjudication or enforcement the conduct of persons, property or acts beyond its borders which affect the interests of the State in the absence of such regulation under international law."[22] With the internet becoming ubiquitous, States are frequently called upon to assert jurisdiction outside their own territory. The cross-border interaction fostered by the internet entails that India's data protection law must have a certain degree of extra-territorial applicability, in order to effectively protect the rights of residents and citizens. The Courts in India have similarly upheld the power of the legislature to enact laws with extra territorial reach, when "such extra-territorial aspects or causes have, or are expected to have, some impact on, or effect in, or consequences for: (a) the territory of India, or any part of India; or (b) the interests of, welfare of, well being of, or security of inhabitants of India, and Indians."[23]

It is customary to distinguish between three different forms of jurisdiction, as reflected in the ILC's description of extra territoriality. Prescriptive (or legislative) jurisdiction relates to the power to make law in relation to a specific subject matter. Adjudicative jurisdiction deals with the power to adjudicate a particular matter. Enforcement jurisdiction relates to the power to enforce existing law. A valid exercise of prescriptive jurisdiction in the adoption of a law is a prerequisite for the valid

[22]International Law Commission (ILC), 'Report on the Work of its Fifty-Eighth' UN Doc A/61/10, Annex E, para 5.
[23]GVK Industries v. Income Tax Officer, 2011(4) SCC 36, para 76.

exercise of adjudicative or enforcement jurisdiction with respect to that law.[24] At the same time, limitations of enforcement jurisdiction may provide policy reasons to circumscribe prescriptive territorial application of law. Determining the scope of India's data protection law is primarily an evaluation of prescriptive and adjudicative jurisdiction, but as noted by the Committee of Experts, must consider issues of enforceability.

By grave warns against such regulatory overreach - "a situation in which rules are expressed so generally and non-discriminatingly that they apply prima facie to a large range of activities without having much of a realistic chance of being enforced."[25] Legislation that cannot realistically be enforced undermines the Indian legal system. **Further, an overly broad and uncertain claim of extra territorial jurisdiction can create uncertainty for business, and impede economic activity, in a time when there is movement towards ensuring interoperable frameworks to promote cross border data flow**. **In that light, India should eschew articulations of uncertain scope**. For instance, as noted by the Committee of Experts, Singapore's law does not explicitly set out its territorial scope. This creates uncertainty over whether jurisdiction may be claimed over foreign entities. The Australian and European Union (EU) approach is more appropriate, wherein jurisdiction is explicitly extended to foreign entities that satisfy certain specified criteria laid down by statute.

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

CCG Response: Please refer to our response to question 1 above.

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

[24] Dan Svantesson, *Extraterritoriality in the Context of Data Privacy Regulation*, 7(11) MASARYK UNIVERSITY JOURNAL OF LAW AND TECHNOLOGY 87, 92 (2013) *available at* https://journals.muni.cz/mujlt/article/viewFile/2628/2192 (Last visited on January 30, 2018).
[25] Lee Bygrave, Determining Applicable Law Pursuant to European Data Protection Legislation, COMPUTER LAW & SECURITY REPORT, 16(4) 252, 255 (2000).

CCG Response: As noted by the Committee of Experts, there exist various grounds for asserting jurisdiction in International law. These include the principles of subjective or objective territoriality, nationality, passive personality, protective principle, and universal principle. Data protection regimes typically invoke a combination of them in their extra territorial applicability. The Supreme Court of India in *GVK Industries* v. *Income Tax Officer,*[26] has echoed this principle, stating that the connection must be real, or expected to be real, and not illusory or fanciful.Thus, the existence of jurisdictional basis is premised on evaluating whether there exists some form of 'meaningful link' with the forum.[27]In the context of data protection, this has found a variety of articulations, as evident from the Committee's survey of various jurisdictions. The broader principle appears to be that the foreign entity addresses its activity specifically to a territory or its residents. The Australian and EU instruments are both modeled on this approach.

The EU approach appears to be more specifically tailored to address cross border interactions online. For instance, Art. 3(2) of the General Data Protection Regulation (GDPR)[28]recognizes that online services are often offered for free, and further attempts to regulate entities that monitor its residents' behaviour online.[29]Adopting an approach similar to the EU model offers additional advantages. For instance, India would have greater chances of being recognised as having an 'adequate' data protection framework by the EU, thereby improving our trade relations with the EU and other countries that adopt similar standards.[30]Further, adopting principles that

[26]GVK Industries v. Income Tax Officer, 2011(4) SCC 36, para 76.

[27] Christopher Kuner, TRANSBORDER DATA FLOWS AND DATA PRIVACY LAW, 128 (Oxford University Press, 2013).

[28]The General Data Protection Regulation has been introduced with the objective of harmonizing data privacy laws across the European Union. It will replace the current Data Protection Directive (95/46/EC), and will be directly applicable in all Member States without the need for implementing legislation. The GDPR was approved by the EU Parliament on April 14, 2016 and is set to come into force on May 25, 2018.

[29]Art. 3, General Data Protection Regulation, Regulation (EU) 2016/679 ["GDPR"].

[30]Under the GDPR, the European Commission may declare a non EU country as having an 'adequate' level of data protection. Personal data may be freely transferred to such countries. This assessment examines, among other things, the extent to which data subjects can enforce rights against entities that process their data. The territorial scope of such enforcement would be a relevant consideration.

are considered best practices across jurisdictions would also assist in increasing interoperability for businesses that operate across borders.

However, in the event that India adopts the language employed by the GDPR, it must address the interpretative pitfalls present as well. For instance, there must be certainty about when an entity would be considered as 'offering goods and services'in India. Evidently, the mere availability of an entity's website would not be sufficient, as that would amount to regulating the entirety of the internet. In this regard, the EU has typically employed standards such as whether the website is offered in an EU language, or if services are offered in an EU currency, or more clearly, if the product is marketed towards EU citizens.[31] This has been referred to as the 'purposeful targeting' test. Some factors to be considered include the use of a language or currency other than those generally used by the organization; listing of phone numbers with an international code; or using country specific top level domains.[32]Similarly, the United States Supreme Court, examines whether a foreign organization "purposefully avail[ed] itself of the privilege of conducting activities in the forum state, thus invoking the benefits and protection of its laws."[33]

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

CCG Response: We do not have any comments on this question at this time. We will submit additional comments at a later stage if necessary.

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

---

[31] Omar Tene and Christopher Wolf, *Overextended: Jurisdiction and Applicable Law under the EU General Data Protection Regulation*, FUTURE OF PRIVACY FORUM WHITE PAPER, 7 (2013) *available at* https://fpf.org/wp-content/uploads/FINAL-Future-of-Privacy-Forum-White-Paper-on-Jurisdiction-and-Applicable-Law-January-20134.pdf (Last visited on January 30, 2018).

[32]*Id.*

[33] J. McIntyre Mach., Ltd. v. Nicastro, 131 S. Ct. 2780 (2011).

CCG Response: We do not have any additional comments on this chapter at this time. We will submit additional comments at a later stage if necessary.

7.2. Chapter 2: Other Issues of Scope

Our responses to the questions raised in this chapter are below:

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

CCG Response:

Natural/Juristic Persons

Juristic persons may have a legitimate interest in certain aspects of data protection. For instance, juristic persons too would seek to ensure that decisions affecting them be taken on accurate and relevant information; or be able to challenge decisions on the basis of erroneous or irrelevant information. Thus, the protections premised on non-discrimination, and fairness could be applicable to juristic persons as well. Assessments as to creditworthiness are a commonly cited example.[34] Further, companies are mandated to provide a host of information regarding their functioning. This is to ensure scrutiny over their financial position, consumer practices, environmental impact, etc. Though the necessity for such collection is a generally accepted, principles such as purpose limitation, confidentiality, and data security may similarly be applicable.

However, as noted by the Supreme Court in *Justice K.S Puttaswamy (Retd.)* v. *Union of India,*[35] the right to privacy flows from the right to life and personal liberty, as well as in aspects of the autonomy and dignity of individuals. Juristic persons, such as companies, do not possess such aspects. Thus, the extension of such

[34] Douwe Korff, for the Commission of the European Communities *"EC Study on the Protection of the Rights and Interests of Legal Persons with Regard to the Processing of Personal Data Relating to Such Persons"* 6 (Study Contract ETD/97/B5-9500/78) *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1288583 (Last visited on February 25, 2018).
[35] (2017) 6 MLJ 267.

protections to juristic persons would be inapplicable. However, we do note that the law should be applicable to personal data of individuals that is held by such juristic persons. By contrast, the position in South Africa's Protection of Personal Information Act is a product of how privacy jurisprudence has evolved in South Africa, where protections are extended to juristic persons as well.[36] The South African Bill of Rights explicitly extends its guarantees to the extent required by the nature of the rights and the nature of that juristic person.[37]

Thus, protections under new law the should primarily extend to personal data of natural persons. The concerns noted above regarding the treatment of corporate data could be suitably addressed through sector specific legislation.

Public/Private

Public and private entities both collect and control vast quantities of personal data. Thus, both have data protection obligations. The AP Shah Report specifically notes that there is an international trend towards a set of unified norms governing both the private and public sector, and both should be brought within the purview of legislation.[38] While private sector processing of data is premised on its commercial exploitation for profit, public sector entities have obligations and functions related to governance, which require the processing of data. As a result, the nature of data that is controlled by public entities may also be particularly sensitive. If combined or aggregated, or unlawfully accessed, privacy incursions by the public sector can be especially egregious. The revelations about US government surveillance make a strong argument for the scrutiny of government handling of personal data. However, long before these revelations, it has been recognised that individuals have the right to exercise their (informational) privacy against the State. The European Convention on Human Rights provides that[39]:

[36] South African Law Reform Commission, Privacy and Data Protection, Discussion Paper 109 (October, 2005) *available at* http://www.justice.gov.za/salrc/dpapers/dp109.pdf (Last visited on January 30, 2018).
[37] *Id.*
[38] Report of the Group of Experts on Privacy, at 4.
[39] Article 8, European Convention on Human Rights.

"*1. Everyone has the right to respect for his private and family life, his home and his correspondence.*

2. There shall be no interference by a public authority except such as is in accordance with law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the protection of health or morals or for the protection of the rights and freedoms of others."

In India as well, the Supreme Court has recognized the applicability of informational privacy restrictions on public sector[40]. In this case, the Court found that even if a public officer is empowered to inspect documents and information available in a public office, such access cannot be extended to information held privately[41].

Consistency in the law also requires that the same principles be applicable to both the public and the private sector.

Special provisions can be incorporated into the law to address the differential rights and obligations of public entities. These may be in the nature of additional obligations, or even derogations from the law, given the function performed by the entities. For instance, the GDPR recognizes that there may exist an imbalance of power between public authorities and data subjects. Consent in that context might not be 'freely given.' Thus, public bodies may have to qualify other grounds for the processing of personal data.[42] On the other hand, if there are exceptions from the standard set of obligations, they must be necessary, proportional and in accordance with law.[43]

Retrospective Application

The data protection legislation, and the obligations therein, should apply retrospectively to data that already exists with controllers and processors. For instance, data subjects should indisputably have the right to access, correct, erase

[40] District Registrar & Collector, Hyderabad v. Canara Bank (2005) 1 SCC 496.
[41] *Id*.
[42] GDPR, recital 43.
[43] Report of the Group of Experts on Privacy, at 56.

etc., personal data that has been previously collected.[44] The law should thus introduce a transition period before the Act comes into force. This would allow controllers and processors sufficient time to update their notices and processes in accordance with the new regime.

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

CCG Response: The law should restrict its scope to the protection of data of natural persons. To clarify, the law will be applicable to juristic persons in relation to any collection and use of data of natural persons, by such juristic persons.

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

CCG Response: The law should be applicable to both public and private entities. Special provisions can be incorporated into the law to address the differential rights and obligations of public entities. Please refer to our response to question one in this chapter for additional comment.

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

CCG Response: Yes, the law should provide protection retrospectively. Please refer to our response to question one in this chapter for additional comments.

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

CCG Response: The data protection legislation should introduce a transition period before the Act comes into force

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

[44] Greenleaf, *supra* note 21, at 7.

CCG Response: We do not have any additional comments on this chapter.

7.3. Chapter 3: What is Personal Data

CCG Response:

We agree with points 1 and 2 in the provisional views stating that any data that relates to an individual, whether an individual is identified or identifiable directly or indirectly, and whether such data is accurate or not, should be covered within the ambit of any data protection law. The nature of data that is collected and processed is constantly changing with technology, and it is imperative that any data protection laws should be drafted in a manner that accommodates this change.

The IT Rules define 'personal information' (PI) as '*any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person*.' This definition appears to be wide, but it is also qualified to some extent by the definition of the term information as follows: "*information includes data, message, text, images, sound, voice, codes, computer programmes, software and data bases or micro film or computer generated micro fiche*".

Reading the two definitions above together shows that the 'personal information' under the IT Rules is limited to information available to a body corporate[45]. It is also limited to information available electronically, via specific technology as seen in the definition of the term 'information'. These limitations are understandable within the context of the limited scope of the IT Act and IT Rules themselves. The IT Act was enacted to provide legal recognition to transactions carried out by electronic means[46]. The IT Rules are meant to govern the use of personal and sensitive personal information within this framework[47]. It may seem that in this day, most transactions, and most use cases for personal information are in the electronic or

[45] The term 'body corporate' has been defined to mean a company and to include firms, sole proprietorships or other associations of individuals engaged in commercial or professional activities.
[46] Statement of Objects and Reasons, Information Technology Act, 2000.
[47] Section 43A, Information Technology Act, 2000.

even online space, however, if we are to enact a comprehensive data protection law, we should refrain from making such assumptions in the law itself.

The white paper proposes 7 key principles of data protection that the law needs to be based on, the first of which is that the law should be applicable in a technology agnostic manner. As we move towards a comprehensive data protection law, we must ensure that it is applicable in relation to all collection and use of personal data, irrespective not only of the nature of technology that is used to collect, process or use the data, but also whether or not technology is used at all.

The second of the 7 principles proposed by the white paper is that the law should be holistic in its application and should apply to both private and public sectors. The law that the committee proposes will apply across industries and organisations that deal with varying types of data about employees, customers, and other individuals[48]. Keeping this in mind, the use of terms such as 'body corporate' should be avoided. The white paper discusses in some detail the need for defining the term 'controller' and 'processor' later in this chapter. Our comments on these questions are below. However, in the context of defining 'personal information', we note that if these terms are defined, these terms may be used in definitions, such as that of personal information if required, without limiting the scope of the law.

The European Union's GDPR provides one example of the sort of wide definition that is necessary in this context: 'personal data' is simply defined as any information relating to an identified or identifiable natural person[49]. The definition goes on to provide that an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. We recommend the adoption of this approach.

---

[48] Smitha Krishna Prasad, *Defining 'personal info' broadly key to protecting it,* DECCAN HERALD (January 21, 2018), *available at*http://www.deccanherald.com/content/655012/defining-personal-info-broadly-key.html (Last visited on February 25, 2018).

[49] Article 4(1), GDPR.

We agree that as noted in the white paper, a wide definition of 'personal information' may cause the application of certain principles of data protection law to be redundant, or have a negative effect in some situations. The white paper refers to the proposals by scholars Paul M. Schwartz and Daniel J. Solove[50] in this regard. They note with regard to the EU approach to defining personal information that the "*expansionist approach is flawed because it treats data about identifiable and identified persons as conceptually equivalent. The difficulty is that there is a broad continuum of identifiable information that includes different kinds of anonymous or pseudonymous information*"[51].

The classic example that is provided to argue for this is that implementing the notice principle, as well as the rights of access and correction for instance in a case where information falls in the identifiable category would require identification / re-identification as the case may be. This process might then reduce the protection available to the person whose data is now identified.

We understand the concerns that are highlighted by Schwartz and Solove. The solution proposed by Schwartz and Solove is that the spectrum of personal information may be divided into three categories: information can be about an (1) identified person – where the person's identity is ascertained, (2) identifiable person – when specific identification, while possible, is not a significantly probable event, or (3) non-identifiable person – where the information carries only a remote risk of identification[52]. They then go on to describe in greater detail standards and examples for when data would fall within each of the categories, and how such data should then be dealt with.

While this approach does indeed provide for the flexibility that may be required of the law in order to make it practical and implementable, the adoption of this approach is not an issue that is pertinent in the definition of personal information. The approach suggested by Schwartz and Solove may be incorporated into the sections of the law

[50] Paul Schwartz and Daniel Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information,* (2011) *available at* https://scholarship.law.berkeley.edu/facpubs/1638/ (Last visited on February 25, 2018).
[51] *Id*.
[52] Schwartz and Solove, *supra* note 50.

that describe how personal information should be treated, in a targeted manner. For instance, the sections that detail the requirement for provision of notice to data subjects may provide for a narrowly crafted exception to this requirement in cases where the individual is not already identified. The requirement to provide notice can then become applicable if and when the individual is identified**. However, the definition of personal information should continue to be a wide definition, along the lines of the GDPR, as described above.**

Responses to questions raised in the white paper:

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

CCG Response: As described above, a wide definition of personal data or information should be adopted. The law that the committee proposes will apply across industries and organisations that deal with varying types of data about employees, customers, and other individuals[53]. Adoption of a wide definition of personal information will facilitate such comprehensive application of the law, in accordance with the key principles suggested in the white paper.

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

   Alternatives:

   a. The SPDI Rules use the term sensitive personal information or data.

   b. Adopt one term, personal data as in the EU GDPR or personal information as in Australia, Canada or South Africa.

CCG Response: As discussed above, the IT Rules and IT Act used terms such as 'data' and 'information' in the context of the scope of the IT Act. However, the distinction between these terms as provided for under the IT Act and IT Rules, would not be relevant in the context of a separate, and comprehensive data protection law. Therefore, we do not find a specific objection with use of either term. It is

[53] Prasad, *supra* note 48.

recommended however, that one term be used consistently in order to limit any risk of confusion.

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

CCG Response: As discussed above, we agree with points 1 and 2 in the provisional views stating that any data that relates to an individual, whether an individual is identified or identifiable directly or indirectly, and whether such data is accurate or not, should be covered within the ambit of any data protection law.

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

CCG Response: Focusing on the concept of 'identifiability' of an individual in defining personal information is in line with internationally accepted standards. This approach also facilitates inclusion of a broad category of information, in the definition of personal information, while avoiding the pitfalls of providing inclusive or exhaustive lists in primary law.

As discussed above, we believe that both ends of the spectrum i.e. 'identified' and 'identifiable' should be included in the definition. The application of specific rules / principles within this spectrum may be dealt with under the law separately.

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

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

CCG Response: No, anonymised and pseudonymised data should not be outside the purview of the definition of personal information itself. However, the principles of data protection may be selectively applied in the case of such data as discussed above.

We agree that anonymization and pseudonymisation should be recommended and incentivised, as these processes reduce the risk of direct identification of individuals using personal information that may then be misused. The Committee should also consider providing for restrictions on the identification/ re-identification of such data.

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

CCG Response: Yes, differentiated levels of protection may be adopted in order to ensure that the law may be implemented in a practical manner. However, as discussed above, the standards of determination need not be included in the definition of personal information itself. These standards can be provided for separately under the law to the extent possible. The regulatory authority may also be empowered to provide guidance on such standards and make decisions in this regard on a case by case basis where required

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

CCG Response: We do not have additional comments on this chapter for the present.

7.4. Chapter 4: Sensitive Personal Data

CCG Response:

The white paper rightly states that many jurisdictions treat certain categories of data as ‘sensitive’ or ‘special’. It also notes that some such types of data are qualitatively different from others. However, while noting that some of this data may be treated as sensitive, since such data can be used to discriminate against individuals, it does not

delve further into the question of why different jurisdictions treat different types of data as ‘sensitive’ or ‘special’.

In the past few years, some scholars have criticised the approach of identifying a separate category of ‘sensitive’ or ‘special’ data at all[54]. If we are to adopt such a definition, it is important to understand why the jurisdictions that do adopt similar definitions do so, and what the potential criticisms of such an approach are.

Our responses to both questions 1 and 2 in this chapter are below:

1. What are your views on sensitive personal data?

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

CCG Response: First, we look at the approach taken by two jurisdictions which are known to treat different types of data as ‘special’ or ‘sensitive’: the European Union and the United States of America (at the federal level).

The European Union’s GDPR identifies the following types of data as ‘special categories of data’: race, ethnic origin, politics, religion, trade union membership, genetics, biometrics (where used for ID purposes), health, sex life, and sexual orientation[55]. Several other jurisdictions have also incorporated many of these categories of data in their definitions of sensitive information[56].

Article 9 of the GDPR provides that processing of such data is prohibited, except in certain situations.

---

[54] Lokke Moerel, *GDPR conundrums: Processing special categories of data,* IAPP (September 12, 2016) *available at* https://iapp.org/news/a/gdpr-conundrums-processing-special-categories-of-data/ (Last visited on February 25, 2018).

[55] Article 9, GDPR.

[56] Daniel Solove, *What Is Sensitive Data? Different Definitions in Privacy Law,* LINKEDIN (July 31, 2014) *available at*https://www.linkedin.com/pulse/20140731172016-2259773-what-is-sensitive-data-different-definitions-in-privacy-law/(Last visited on February 25, 2018).

The recitals in the preamble to the GDPR provide some insights about why these specific types of data have been included as a separate, special category. Recital 51 of the GDPR states that "*Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms*".

This approach follows from the EU's approach to classification of data in the current law, i.e. the Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Directive)[57]. Under the Directive, the rationale behind regulating particular categories of data in a different way stems from the presumption that misuse of these data could have more severe consequences on the individual's fundamental rights, such as the right to privacy and non-discrimination, than misuse of other, "normal" personal data[58].

The US on the other hand has implemented a number of sector specific privacy / data protection laws, and does not have a comprehensive privacy law, sensitive information is accorded special recognition through a series of key privacy statutes that impose restrictions on explicitly identified categories of sensitive information[59]. Sector specific laws include laws which deal with financial information, credit reporting information, and health information[60]. These laws each identify certain types of data that merit special protection. However, it has been suggested that unlike the EU approach, this is not intended to prevent the collection and use of such personal information, but rather to prevent clearly unauthorized uses[61].

---

[57] European Commission, Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (1995).

[58] Article 29 Data Protection Working Party, *Advice Paper on Special Categories of Data "Sensitive data",* (2011).

[59] Helen Nissenbaum, *Privacy as Contextual Integrity,* 79 WASHINGTON LAW REVIEW 119 (2004)*available at* http://www.kentlaw.edu/faculty/rwarner/classes/internetlaw/2011/materials/nissenbaum_norms.pdf (Last visited February 25, 2018).

[60] Jane K. Winn, *Can a Duty of Information Security Become Special Protection for Sensitive Data Under US Law?* (September 9, 2008) *available at* https://ssrn.com/abstract=1265775 (Last visited on February 25, 2018).

[61] *Id.*

As discussed above, it has been argued by some that there is no need for a separate classification of 'sensitive' personal information. This argument may in some ways also resonate with the proposal made by Schwartz and Solove in relation to the definition of 'personal information', as described above. Sensitive personal information may automatically be included at the extreme end of the spectrum requiring the full strength of protection provided by the law.

However, given that data protection law in India is still at the nascent stage, we believe that it may be of value to adopt the European approach and classify certain categories of data which require additional protection separately.

Following this approach, we can begin identifying the kind of data that needs to be included in this category by looking at the fundamental rights under the Constitution of India. Article 15 provides that the State cannot discriminate against any citizen on the basis of religion, race, caste, sex, and place of birth. Article 16 deals specifically with discrimination in the context of employment by the State and includes 'residence' in addition to the above categories.

In addition to the above, international practices may be examined to identify any other kind of information that should be included in these categories.

The Universal Declaration of Human rights provides that "Everyone is entitled to all the rights and freedoms set forth in this Declaration, without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status"[62].

As described in the white paper, the GDPR itself defines special categories of data to include 'data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation'.

[62] Article 2, *Universal Declaration of Human Rights*, 217 (III) A, (Adopted on December 10, 1948).

Guidance may also be taken from the Article 29 Data Protection Working Party's Advice Paper on special categories of data[63]. This paper examines the concept of special categories of data in the Directive, and provides guidance on changes that may be incorporated in the Directive itself, or any future legal framework. The Article 29 Data Protection Working Party has considered the inclusion of additional categories of data such as biometric and genetic data, information about individuals' financial situation, data about minors, and data about individuals' geo-location.

We note here that genetics and biometrics have been included specifically in this category in the GDPR. They were not included in the corresponding definition of special categories of information under the GDPR's predecessor, the Directive[64]. In addition to the categories of information itself, this paper discusses some of the problems with the usage of broad terms within the definition of 'sensitive information'. The language proposed in the paper should be considered when the Committee is drafting the definition of the term 'sensitive information'.

For instance, if the aim is to provide additional protection to data that can be used to discriminate or limit fundamental rights, the inclusion of 'information about the financial status of individuals' may be relevant. The IT Rules on the other hand have a limited description of financial information – financial information such as bank account or credit card or debit card or other payment instrument details are considered sensitive personal data or information[65]. This definition causes ambiguity since bank account details could be read to mean the bank account number itself, or transaction details, online log in and password details, and even details about the actual money in the account at any given time. A data controller who is trying to limit their liability may choose to refer only to bank account numbers as sensitive information in their notice, consent and privacy policy documents. However, an individual whose data is being used may consider all of the above to be sensitive information.

[63] *Supra* note 58.

[64] European Commission, Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (1995).

[65] Rule 3, Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

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

CCG Response: We do not have additional comments on this chapter at present.

7.5. Chapter 5: What is Processing?

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

CCG Response: We agree with the provisional views expressed by the Committee. Existing international standards should be adopted, and the term 'processing' should be defined in a wide and inclusive manner. The GDPR defines 'processing' as follows: "*any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction*"[66]

A similar definition may be adopted in the Committee's recommendation.

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

CCG Response: While we agree broadly with the approach suggested in the provisional views, we argue that the definition of 'processing' should primarily be a wide and inclusive definition that (a) provides for as many instances of use of data as possible, and (b) allows the regulator or adjudicating body to expand on the definition to include additional actions that may not be strictly described in the definitions itself.

In addition to the above, specific actions such as collection, use, disclosure and combination of data may be broadly defined in order to facilitate greater clarity in the drafting and implementation of the data protection law.

[66] Article 4(2), GDPR.

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

CCG Response: The scope of the law should include both automated and manual processing. Not only is this in line with international standards, but allowing for both automated and manual processing of data to be covered would make the law truly technology agnostic in line with the proposed data protection principles.

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

CCG Response: We do not have additional comments on this chapter at this stage. We will follow up with additional comments if necessary.

7.6. Chapter 6: Entities to be Defined in the Law: Data Controller and Processor

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

CCG Response: The concepts of 'controller' and 'processor' have been established under data protection laws adopted by the European Union (and those countries that follow this approach), for many years now. As described in the Article 29 Data Protection Working Party's Opinion 1/2010 on the concepts of "controller" and "processor", these concepts "determine who shall be responsible for compliance with data protection rules, and how data subjects can exercise their rights in practice"[67].

The GDPR defines the terms 'controller' and 'processor' as follows[68]:

- controller: "*means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of*

[67] Article 29 Data Protection Working Party, *Opinion 1/2010 on the concepts of "controller" and "processor",* (2010). We note that this opinion was issued in relation to the Directive, in 2010. However, these statements and arguments remain relevant in the current context.
[68] Article 4, GDPR.

such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law";

- processor: "*means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller*".

The IT Act and the IT Rules do not specifically define a controller and processor. However, a look at the provisions in the IT Rules show that many of the roles and responsibilities described in the IT Rules are described along the above lines.

Bearing in mind the important role that the distinction between the two plays, especially in easing the burden on the data subject in exercising their rights, we argue that the two distinct definitions should be incorporated in India's data protection law.

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

CCG Response: As described above, the law should define both 'data controller' and 'data processor'. The definitions under the GDPR may be used as an example, and adapted to the Indian context.

In addition, we note that the GDPR also defines the role of a 'third party' i.e. "*a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data*"[69].

A similar approach can be adopted in India as well.

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

In today's world, given the fact that the same organisations often perform both roles of controller and processor, the distinction in definition and allocation of different

[69] Article 4, GDPR.

responsibilities to these two types of entities may seem redundant. However, as noted in the Article 29 Data Protection Working Party's Opinion 1/2010 on the concepts of "controller" and "processor", the distinction between the two, and the role of the controller in particular, '*goes to the heart of the Directive, its first objective being "to protect individuals with regard to the processing of personal data"*'.

The role of the controller then becomes to (i) allocate responsibility of compliance with law, and (ii) to answer to the data subject in their exercise of rights such as access, correction, objection to processing etc., as well as the right to seek remedies in the case of breach of contract or violation of law.

In these cases, the processor will have secondary liability, i.e. the processor should be liable to the controller, who in turn will be strictly liable to the data subject. Strict liability on the part of the controller is important, especially in cases where the data is transferred to a processor in a different jurisdiction. For instance, if such jurisdiction's laws do not provide the same level of data protection, it will be important for the controller to ensure that the standards under the Indian data protection law are met.

In addition to the above, it is important to ensure that where non-data subject facing responsibilities and liabilities are concerned, both controller and processor should be responsible to comply with the law. Accordingly, in situations where the regulator / authority is taking action for non-compliance with any data protection principles and provisions of the law, such action can be taken against either the controller, or the processor, or both, as may be required.

This position is in line with that in the GDPR. We recommend that the provisions of the GDPR on allocation of responsibility to controllers, processors and third parties, may be adapted accordingly in the Indian data protection law.

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

CCG Response: We do not have additional comments on this chapter at this stage. We will follow up with additional comments if necessary.

7.7. Chapter 7: Exemptions for Household Purposes, Journalistic and Literary Purposes and Research

Our response to questions 1 and 2 in this chapter of the White Paper are below:

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

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

CCG Response: We agree that exemptions may be provided for some of the above-mentioned purposes. We have provided detailed views and recommendations on the manner in which some of these exemptions can be provided, below. However, we reiterate here that any exemptions that may be permitted should be limited to reasonable and necessary measures required to achieve the purpose in question. Limitations may be either in relation to the kind of data that is used, or the individual principles / provisions of law from which the exemption is provided, or both. Further, to the extent possible, these exemptions should be governed by clear procedural guidelines, and data subjects should be allowed access to remedial measures.

Our responses to some of the individual questions in the White Paper are below.

Domestic /Household Processing

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

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

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

CCG Response (to questions 1, 2 and 3 above): We recommend that internationally accepted standards are followed in providing for exemptions from the data protection law for domestic and household use of personal information.

Concepts such as domestic, or household use may be difficult to define with certainty, however, the law can provide guidance on the purpose behind providing such an exemption, in order to aid its interpretation.

For instance, Article 2 of the GDPR states that the regulation does not apply to the processing of data 'by a natural person in the course of a purely personal or household activity'[70]. The preamble to the GDPR also explains this exemption by stating that it applies where there is no connection to any professional or commercial activity[71]. It adds that *"(p)ersonal or household activities could include correspondence and the holding of addresses, or social networking and online activity undertaken within the context of such activities*"[72].

In addition to the GDPR, all Asian countries with data protection laws include similar limitations as well, for instance, Macau excludes any processing for 'systematic communication and dissemination' from this exception[73]. Similar limitations may be provided for under Indian data protection law as well.

4. Are there any other views on this exemption?

CCG Response: We do not have additional views on this exemption.

Journalistic/Artistic/ Literary Purpose

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

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

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

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

[70] Article 2(2)(c), GDPR.
[71] Recital 18, GDPR.
[72] Recital 18, GDPR
[73]Greenleaf *supra* note 21.

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

CCG Response (to questions 1 to 5 above): We agree that certain exemptions may be provided for the processing of personal information for journalistic, artistic and literary purposes. As with the exemptions for domestic and household purposes, we recommend that internationally accepted standards are followed in providing for exemptions.

We note that there are two important concerns in this regard: (i) definition of journalist, artistic and literary purpose; and (ii) the scope of exemptions to be granted.

Below we have addressed specifically the question of how to define journalist / journalistic purposes. Similarly, definitions for artistic and literary purposes may be drawn from existing international principles.

With regard to the definition of 'journalists', we propose that the UNESCO's definition of journalism may be adopted. UNESCO has been undertaking efforts towards the protection of journalists, both in and outside of conflict areas for many years now[74], and has developed a nuanced understanding of journalism in these efforts. UNESCO considers individuals undertaking all types of journalism, including general journalism, photojournalism, investigative journalism, crime reporting, environmental journalism, to be journalists[75]. Further, these individuals are considered to be journalists irrespective of the nature of their contracts / affiliations[76]. These definitions are drawn from the UN High Commissioner for Human Rights' report, stating that "*all individuals are entitled to the full protection of their human rights, whether the State recognizes them as 'journalist' or not; whether they are professional reporters or*

[74]*See:* UNESCO, *Safety of Journalists, available at* https://en.unesco.org/themes/safety-journalists (Last visited on February 25, 2018).
[75] UNESCO, *Applying UNESCO's Journalists' Safety Indicators,* (February 11, 2015) *available at* http://unesdoc.unesco.org/images/0026/002608/260894E.pdf (Last visited February 25, 2018).
[76]*Id.*

'citizen journalists'; whether or not they have a degree in journalism;whether they report online or offline"[77]; and the UN Human Rights Committee's general comment stating that journalism is "*a function shared by a wide range of actors, including professional fulltime reporters and analysts, as well as bloggers and others who engage in forms of self-publication in print, on the Internet or elsewhere*"[78].

The second concern described above is the scope of exemptions to be granted. In this regard we note that many jurisdictions have often provided for wide exemptions to most principles and provisions of the data protection law, except perhaps that of maintaining technical security standards[79]. We recommend that in addition to retaining security obligations, the law also clarifies that these exemptions are only available for the purpose of information that is required to be reported, written about, or referred to in some manner in the journalistic, artistic or literary work. This would ensure that should the individuals undertaking such works be affiliated with commercial / for profit organisations, the exemption doesn't enable these organisations to undertake data processing that would otherwise be governed by the law, using such an exemption. We also recommend that principles such as storage limitation, and data minimization, which do not unduly restrict the actions of the individuals undertaking such works may continue to be applicable.

Given the wide nature of the purposes for which the exemption is granted, it may be difficult to identify which individual principles and provisions should apply in the primary law itself (apart from those mentioned above). We recommend that the regulatory authority is required to undertake this exercise (in consultation with sector specific authorities, where required), on a periodic basis.

6. Are there any other views on this exemption?

CCG Response: We do not have any additional comments on this exemption.

---

[77] UNHRC, *Summary of the Human Rights Council panel discussion on the safety of journalists*, A/HRC/27/35 (2014). See para 9.

[78] UNHRC, *General Comment No. 34*, CCPR/C/GC/34 (2011); OHCHR, *Safety of Journalists and Media Workers,* (2014).

[79] White Paper, Chapter 7.

Research/Historical/Statistical Purpose

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

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

CCG Response (to questions 1 and 2 above): We agree that certain exemptions may be provided for the processing of personal information for research purposes. As with the other exemptions, we recommend that internationally accepted standards are followed in providing for exemptions.

We recommend that in order to ensure that the exemption is used for bonafide purposes only, it is limited to research that is undertaken for non-commercial purposes, by educational institutions, scientific and research institutions. Further, as with the exemption for journalistic, artistic and literary purposes, the principles and provisions of the law that require maintenance of data security, storage limitation and data minimization should continue to apply.

In addition to the above, there may be certain situations in which even for research informed consent, or at least notice to the data subjects is required. This is particularly relevant in medical research that involves actual trials and testing on individuals. In order to account for such circumstances, the regulatory authority may be required to work with sector specific regulators, in order to ensure that adequate policies are in place to enable research and protect individuals at the same time. Where existing law or regulations already provide for higher standards of protection, the same should be adopted.

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

CCG Response: We recommend that this exemption is provided for the purposes of non-commercial / non-profit research.

4. Are there any other views on this exemption?

CCG Response: We do not have any additional comments on this exemption.

Investigation and Detection of Crime, National Security

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

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

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

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

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

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

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

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

CCG Response (to questions 1 to 8 above): The exemption from certain aspects of data protection law for investigation and detection of crimes and national security is ordinarily acceptable. However, it is important to examine the actual implications of such an exemption in India, given the current state of its system for investigation of crime national security. It is evident that there is already extensive scope for abuse and misuse. This could be exacerbated if a broad exception is created within the data protection framework. We would therefore recommend that any such exception is subject to safeguards within the data protection that subject all access, use and

retention of data by law enforcement agencies to the internationally accepted safeguards.

Since privacy is a fundamental right, the State must ensure that any actions that may limit or violate such a right fall within the existing Constitutional parameters for its restriction.

Currently, we have limited regulation of State sponsored surveillance efforts in India. Our communication interception jurisprudence has focused on targeted surveillance for years[80], and the Supreme Court has recognized that telephone tapping / interception would violate Article 21 of the Constitution unless it was permitted by procedure established by law[81]. However, the safeguards prescribed by the Court are opaque and rely solely on members of the executive to review surveillance requests, leaving little for third party scrutiny, or challenge by affected parties (who may never find out that they were placed under surveillance)[82].

The procedural safeguards within the data protection legislation should be crafted from this point of view. They will need to account for big data, and address both targeted and mass surveillance efforts by the State among other things. The current safeguards are out of date and do not comply with international human rights norms.

As per the Supreme Court's order in *Vishaka v. State of Rajasthan*, in the absence of specific case law or legislation dealing with such issues, the contents of International Conventions and norms are significant for the purpose of interpretation of the rights guaranteed under the Constitution[83].

First, we refer to the Universal Declaration of Human Rights (UDHR) adopted by the United Nations General Assembly in 1948, and the International Convention on Civil

[80] Chinmayi Arun, *Paper-Thin Safeguards and Mass Surveillance in India,* NATIONAL LAW SCHOOL OF INDIA REVIEW 26 (2014): 105 available at https://ssrn.com/abstract=2615958 (Last visited February 25, 2018).
[81] *People's Union for Civil Liberties (PUCL) v. Union of India*, (1997) 1 SCC 301 AIR 1997 SC 568; see also Chinmayi Arun, *Paper-Thin Safeguards and Mass Surveillance in India,* NATIONAL LAW SCHOOL OF INDIA REVIEW 26 (2014): 105 available at https://ssrn.com/abstract=2615958 (Last visited January 30, 2018).
[82] *Supra* Note 80.
[83] Vishaka v. State of Rajasthan, AIR 1997 SC 3011.

and Political Rights (ICCPR), to which India is a state party[84]. Article 12 of the UDHR and Article 17 of the ICCPR both state as follows:

> *"1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.*
>
> *2. Everyone has the right to the protection of the law against such interference or attacks."*

The ICCPR notably does not contain a limitations clause to Article 17, which recognises the right to privacy. However, the permissible limitations to this right are elaborated in the Human Rights Committee's general comments, and can also be drawn from the Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights[85]. Interference with an individual's right to privacy is only permissible under international human rights law if it is neither arbitrary nor unlawful[86]. The Human Rights Committee's General Comment 16 explains that "*the term "unlawful" means that no interference can take place except in cases envisaged by the law. Interference authorized by States can only take place on the basis of law, which itself must comply with the provisions, aims and objectives of the Covenant*"[87].

In her report on 'The right to privacy in the digital age'[88] (OHCHR Report), the (then) United Nations High Commissioner for Human Rights has noted that "the very existence of a mass surveillance programme thus creates an interference with privacy. The onus would be on the State to demonstrate that such interference is neither arbitrary nor unlawful."[89] The report also notes that the collection and

---

[84] UN General Assembly, *International Covenant on Civil and Political Rights*, 999 UNTS 171 (Adopted on December 16, 1966).

[85] UNHRC, *Report of the Office of the United Nations High Commissioner for Human Rights, The right to privacy in the digital age*, A/HRC/27/37 (2014) *available at* http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf (Last visited on January 30, 2018).

[86] *Id.*

[87] UNHRC, *General Comment No. 16*, HRI/GEN/1/Rev.9 (Vol. I) (1988).

[88] *Supra* note 85.

[89] *Supra* note 85.

retention of communications data amounts to an interference with privacy whether or not those data are subsequently consulted or used[90]. The report discusses the permissible limitations to the right to privacy under Article 17, explaining that:

"*To begin with, any limitation to privacy rights reflected in article 17 must be provided for by law, and the law must be sufficiently accessible, clear and precise so that an individual may look to the law and ascertain who is authorized to conduct data surveillance and under what circumstances. The limitation must be necessary for reaching a legitimate aim, as well as in proportion to the aim and the least intrusive option available. Moreover, the limitation placed on the right (an interference with privacy, for example, for the purposes of protecting national security or the right to life of others) must be shown to have some chance of achieving that goal. The onus is on the authorities seeking to limit the right to show that the limitation is connected to a legitimate aim. Furthermore, any limitation to the right to privacy must not render the essence of the right meaningless and must be consistent with other human rights, including the prohibition of discrimination. Where the limitation does not meet these criteria, the limitation would be unlawful and/or the interference with the right to privacy would be arbitrary*".

The OHCHR Report discussed above notes that even where laws are in place that act as limitations or exceptions to the right to privacy, they must be further supported by effective procedural safeguards, and adequately resourced and effective institutional arrangements to support these safeguards[91]. The OHCHR Report also considers independent civilian oversight agencies, as well as the involvement of all branches of government in the oversight of surveillance programmes essential[92].

In this context, it may also be helpful to take note of J. Kaul's reference, in *Puttaswamy v. Union of India*[93], to the restrictions allowed under EU's GDPR as an example of the restrictions that may be considered reasonable in India.

[90] *Supra* note 85.
[91] *Supra* note 85.
[92] *Supra* note 85.
[93] (2017) 6 MLJ 267.

Under the GDPR, states may restrict obligations of data protection to safeguard national security, public security and the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security[94]. However, such a restriction must respect the essence of the fundamental rights and freedoms, must be a necessary and proportionate measure in a democratic society. In particular it must contain provisions regarding[95]:

(i) the purposes of the processing or categories of processing;

(ii) the categories of personal data;

(iii) the scope of the restrictions introduced;

(iv) the safeguards to prevent abuse or unlawful access or transfer;

(v) the specification of the controller or categories of controllers;

(vi) the storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing;

(vii) the risks to the rights and freedoms of data subjects; and

(viii) the right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction.

In the context of limited safeguards on both targeted and mass surveillance, concerns have been raised regarding various projects run by the Indian government, including the Central Monitoring System, Network Traffic Analysis / NETRA, National Intelligence Grid, New Media Wing and the Aadhaar project[96].

[94]Article 23, GDPR.

[95] Article 23(2), GDPR.

[96]*Supra*note 80; Chinmayi Arun*, Privacy is a fundamental right*, THE HINDU, March 18, 2016, available at http://www.thehindu.com/opinion/lead/lead-article-on-aadhaar-bill-by-chinmayi-arun-privacy-is-a-fundamental-right/article8366413.ece; Devirupa Mitra, *India Gears Up to Defend Internet Rights Regime as it Operationalises Mass Surveillance Project*,

The Snowden revelations have shown that even though on paper many checks and balances are in place, including judicial review of intended data collection schemes, the effectiveness of the way the safeguards have been implemented remains doubtful[97]. We need to move towards recognizing privacy as a societal interest, and focus on oversight and accountability mechanisms, bearing in mind the impact of unrestrained surveillance on the health of our democracy[98].

The third committee of the UN General Assembly in its resolution on 'The Right to Privacy in the Digital Age', adopted in 2016, has called for States to undertake the following actions among others[99]:

(a) develop or maintain and implement adequate legislation, with effective sanctions and remedies, that protects individuals against violations and abuses of the right to privacy, namely through the unlawful and arbitrary collection, processing, retention or use of personal data by individuals, governments, business enterprises and private organizations;

(b) further develop or maintain, in this regard, preventive measures and remedies for violations and abuses regarding the right to privacy in the digital age that may affect all individuals, including where there are particular effects for women, as well as children and those vulnerable and marginalized; and

(c) refrain from requiring business enterprises to take steps that interfere with the right to privacy in an arbitrary or unlawful way

India's data protection law, and any law, policy or executive order (specific to national security or not) that calls for or regulates surveillance in any form, should necessarily incorporate these measures. Any restriction of data protection rights must comply with the UN norms as well as the threshold to protect rights detailed in the GDPR. These safeguards and oversight mechanisms must be properly encoded

---

THE WIRE, May 3, 2017, available at https://thewire.in/107292/india-mass-surveillance-project-cms/; and https://privacyinternational.org/node/1002.

[97] Working Party 29, *Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes*, 819/14/EN WP 215 (April 10, 2014).

[98] *Supra* note 80.

[99] General Assembly Resolution A/RES/71/199.

in law, rules, or regulations, in order to ensure that they are applied consistently across different cases. In addition to independent third-party oversight of this system, controllers and processors should be required to be transparent about requests received from law enforcement / government agencies for protected information. If it is not in the public interest to provide granular information, other details such as number of requests made, legal basis for the requests made etc., can be provided.

9. Are there any other views on these exemptions?

CCG Response: We do not have any additional comments on this section at this stage.

7.8. Chapter 8: Cross Border Flow of Data

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

CCG Response: Regulation of cross border flows is necessary to ensure that controllers do not circumvent national legislation simply by transferring personal data to other countries. After the Snowden revelations, concerns about foreign government access to data have also been exacerbated[100]. Further, as evidenced from the EU's experience, regulating cross border transfers may result in growing pressure for other jurisdictions to formulate strong and equivalent data protection laws[101].

Kuner distinguishes between geographically-based, and organizationally-based approaches to regulating cross border data flow[102]. The GDPR typifies the former. Thus, transfers are regulated based on whether the territory to which the data flows is considered 'adequate', 'comparable', 'equivalent' etc. In contrast, the Asia Pacific Economic Cooperation Framework (APEC), a set of voluntary privacy principles,

[100] Tatevik Sargsyan, *Data Localization and the Role of Infrastructure for Surveillance, Privacy, and Security*, INTERNATIONAL JOURNAL OF COMMUNICATION 10, 2221, 2221 (2016) *available at* http://ijoc.org/index.php/ijoc/article/viewFile/3854/1648 (Last visited on January 30, 2018).
[101] Christoper Kuner, TRANSBORDER DATA FLOWS AND DATA PRIVACY LAW, 66 (Oxford University Press, 2013).
[102] *Id.,* at 64.

follows the organizational approach[103]. This ensures that the original collector of personal data remains accountable for compliance with the original privacy framework that applied when and where the data was collected. This is regardless of the data being subsequently transferred to other organizations or countries.

There is no conflict as such between the two approaches, and jurisdictions may implement a combination of both. For instance, the GDPR also recognizes binding corporate rules, and standard contractual clauses[104].

An integrated framework would also limit the disadvantages of adopting a framework reliant purely on the bureaucracy riddled process of an adequacy assessment. Kuner has noted that there may be considerable procedural delays in the process[105]. The determination requires a comprehensive study of the country's legal system. Often, the regulator may lack the expertise to conduct such a study, and must turn to contractors. This may cause further delay. Political factors may also come into play[106]. As such he recommends that a framework which restricts cross border flows must be accompanied by the minimisation of bureaucratic restrictions (such as requiring regulatory filings or approvals for individual data transfers); encouragement of organizationally-based data transfer mechanisms (such as binding corporate rules); and prioritisation of enforcement to focus on those data flows that carry the greatest risks for individuals[107].

Greenleaf further suggests that the Indian regulator could place reliance on adequacy assessments by other regulators and international data protection

---

[103] Principle 9, APEC Privacy Framework (2005), *available at* http://www.apec.org/Groups/Committee-on-Trade-and Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx (Last visited on January 30, 2018).

[104] Article 46, GDPR.

[105] Christopher Kuner, *Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future*, OECD DIGITAL ECONOMY PAPERS, No. 187, 29 (2011) *available at* http://www.kuner.com/my-publications-and-writing/untitled/kuner-oecd-tbdf-paper.pdf (Last visited on January 30, 2018).

[106] *Seefor instance*: John Oates, *Ireland to block EU-Israel data hoover,* THE REGISTRAR, (July 12, 2010) *available at* https://www.theregister.co.uk/2010/07/12/ireland_israel_passport/ (Last visited on January 30, 2018).

[107] Kuner *supra* note 101, at 27.

authorities, whose standards are considered sufficiently rigorous[108]. A harmonized approach could thus significantly reduce the burden on the regulator. The European Union would be a primary contender for such an alignment, entailing that there would already be 43 jurisdictions where data may flow freely[109].

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

CCG Response: Cross border transfers should occur only when an adequate and equivalent level of protection can be assured over personal data. The data protection law should incorporate an integrated framework which factors in both geographical based and organization based assessments.

The data controller should be required to obtain consent for cross border transfer of data specifically, and additional penalties should be imposed for breach of this obligation (i.e. in addition to other penalties that may be applicable, and remedies available to the data subject)

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

CCG Response: No, we do not believe that such a restriction is necessary.

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

CCG Response: We note that although the White Paper describes the concepts of binding corporate rules and model contractual clauses, there is no reference to the same in either the provisional views or the questions posed in the White Paper. We believe that the use of these rules and clauses aids compliance. We recommend that the data protection law puts in place a detailed and strong framework for the adoption of both, and provide for pre-approved drafts of such rules and contractual clauses. The regulator may be empowered to revise these documents as required

[108] Greenleaf, *supra* note 21, at 11.
[109] Greenleaf, *supra* note 21, at 11.

from time to time. However, the framework for adoption of binding corporate rules and model contractual clauses should clarify that the provisions of the draft law must be treated as minimum standards to be improved upon by both controllers and processors, as well as the regulator.

7.9. Chapter 9: Data Localisation

1. What are your views on data localisation?

CCG Response: Data localization requires entities that collect data to retain it within a state's jurisdictional limits. For this reason, these measures have also been alternatively termed, data residency, or data nationalism[110]. It appears to be self-evident that measures such as localization are not scalable globally. It is highly unlikely that the necessary infrastructure could be established in all developing or small countries. The associated costs of building or renting infrastructure in each jurisdiction would be prohibitive to much of online enterprise. The industry perspective provided by the Committee of Experts appears to strongly discourage the mandatory localization of data on grounds of economic efficiency. Even so, as Kuner suggests, assessing policy purely on such a metric presupposes the primacy of efficiency among other competing values[111]. Further, "clothing industrial policy in the language of legality can corrode public trust in the status of fundamental values as standing apart from partisan interests."[112] Thus, our analysis places emphasis on how the values of privacy and security may be impacted by data localization.

The White Paper notes two broad arguments for the localization of data. First, it may protect citizens from unlawful foreign surveillance. Second, it may support investigations by domestic law enforcement.

---

[110] Anupam Chander and Uyên Lê*, Data Nationalism*, 64 EMORY LAW JOURNAL 677 (2015) *available at* http://law.emory.edu/elj/_documents/volumes/64/3/articles/chander-le.pdf (Last visited on January 30, 2018).

[111] Christopher Kuner, *Data Nationalism and its* Discontents, 64 EMORY LAW JOURNAL 2095 (2015) *available at* http://law.emory.edu/elj/_documents/volumes/64/online/kuner.pdf (Last visited on January 30, 2018).

[112] *Id.* at 2089.

Foreign Surveillance

The Committee of Experts notes that the push for localization has come from concerns of surveillance by foreign governments. These fears were exacerbated in light of the Snowden revelations[113]. However, it has been argued that localization may be an ineffective remedy. First, localization laws such as Russia's, that merely mandate the storage of local copies of data, only increase the risk of unlawful surveillance by domestic authorities, while maintaining the same degree of exposure abroad[114]. Second, reports suggest that foreign governments routinely employ surveillance tactics overseas, along with the use of malware[115]. This implies that physical access to data storage or processing is not technically necessary, and relocating the data would not serve the purpose of protecting it.

Law Enforcement Access

The Committee notes that the storage of data locally could aid domestic investigations, and provide a larger pool of data to law enforcement agencies. It is admitted that law enforcement agencies need sufficient access to evidence both for securing convictions, as well as the protection of the wrongly accused. However, mandating localization purely to ensure access to data for law enforcement appears to be an overbroad measure. It may be more appropriate to avail other alternatives, such as incorporating investigative jurisdiction which shifts focus away from the location of the data to the nationality and location of the target[116]. This could empower domestic authorities to compel companies within its jurisdiction to disclose data stored abroad, when a substantial link is present. Indeed, Microsoft's stand in *Microsoft Corporation* v. *United States of America,*[117] has been that the Stored Communication's Act doesn't currently allow such disclosures, but the company

[113] Sargsyan, *supra* note 100 at 2221.

[114] Neha Mishra, *Data Localization laws in a Digital World*, THE PUBLIC SPHERE 137, 143 (2016) *available at* http://publicspherejournal.com/wp-content/uploads/2016/02/06.data_protection.pdf (Last visited on January 30, 2018).

[115] *Id.*

[116] Dan Svantesson, *Law Enforcement Cross-border Access to Data (Preliminary Report),available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2874238 (Last visited on January 30, 2018).

[117] Microsoft Corporation v. United States of America, No. 14-2985 (2d Cir. 2016).

supports ongoing measures by Congress to suitably amend the law[118]. Thus, the proposed International Communications Act[119] illustrates such an approach. The underlying principle is that search and seizure powers are traditionally domestic, but what has changed is the global infrastructure of the internet, which allows service providers to frustrate the administration of justice. Thus, providers in the United States can be ordered to assist with the production of foreign-stored data belonging to US persons but not the foreign-stored data of foreigners.

Cross border access to data is rife with jurisdictional conflicts. For instance, the European Commission, in its amicusbrief, in Microsoft has argued that compelling a transfer of data from Ireland to the United States, would also be subject to the applicable rules for cross border data flows from the EU[120]. In that light, the U.N. Special Rapporteur on the Right to Privacy has proposed that "negotiation and legislation are the most appropriate means of developing mechanisms by which a state may efficiently obtain access to cloud data."[121] It is argued that new processes must be operationalized, given the failure of the MLAT process. An example, previously endorsed by the Rapporteur,[122] could be an international framework that allows for the grant of an 'international data access warrant.'[123]

---

[118] United States of America v. Microsoft Corporation, Case No. 17-2, Brief in Opposition, *available at* http://www.scotusblog.com/wp-content/uploads/2017/09/17-2-BIO.pdf (Last visited on January 30, 2018).

[119] United States International Communications Privacy Bill, 2017 *available at* https://www.congress.gov/115/bills/s1671/BILLS-115s1671is.pdf (Last visited on January 30, 2018).

[120] United States of America v. Microsoft Corporation, Case No. 17-2, Brief of the European Commission on Behalf of the European Union as *Amicus Curae* in Support of Neither Party, *available at* https://www.supremecourt.gov/DocketPDF/17/17-2/23655/20171213123137791_17-2%20ac%20European%20Commission%20for%20filing.pdf (Last visited on January 30, 2018).

[121] United States of America v. Microsoft Corporation, Case No. 17-2, *available at* https://www.supremecourt.gov/DocketPDF/17/17-2/24918/20171222120327043_35632%20pdf%20Krishnamurthy.pdf (Last visited on January 30, 2018).

[122] UNHRC, *Report of the Special Rapporteur on the right to privacy, Joseph A. Cannataci,* 18 A/HRC/34/60 (2017).

[123] United States of America v. Microsoft Corporation, Case No. 17-2, *available at* https://www.supremecourt.gov/DocketPDF/17/17-

Individual Rights

In addition to the above, localization may adversely affect the rights of data subjects. It has been suggested that localization may make data more vulnerable to security attacks as well as natural disasters.[124] Typically, data is partitioned and stored over multiple physical locations, in a process known as sharding. Mandating localization would preclude such practices.[125] Localization also creates a 'jackpot' problem, with vast quantities of data centralized within a jurisdiction as a compelling target for unauthorized access.[126]

Kuner further suggests that data localization may be contrary to the values enshrined in the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, which protect the freedom to seek, receive and impart information of all kinds, regardless of frontiers[127].

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

CCG Response: As argued above, data localisation is an overbroad measure for the objective of preventing foreign surveillance, and ensuring law enforcement access to data. It can also detrimentally impact the rights of data subjects. We do not recommend a data localisation requirement for the storage of personal data within the jurisdiction of India. Please refer to our response to question 1 above for additional information.

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

CCG Response: As described above, we do not recommend a data localisation requirement for the storage of personal data within the jurisdiction of India.

2/24918/20171222120327043_35632%20pdf%20Krishnamurthy.pdf (Last visited on January 30, 2018).

[124] Mishra, *supra* note 114 at 143.

[125]Mishra, *supra* note 114 at 143.

[126] Chander and Le, *supra* note 110, at 717.

[127] Kuner, *supra* note 101, at 2096.

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

CCG Response: As described above, we do not recommend a data localisation requirement for the storage of personal data within the jurisdiction of India.

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

CCG Response: We do not have additional comments on this chapter at this stage.

7.10. Chapter 10: Allied Laws

CCG Response: We have not examined each of the laws referred to in this chapter in detail due to the paucity of time. We recommend that once the data protection law is in effect, the provisions of this law should govern the use of personal data or sensitive personal data under any other law in India, in so far as the data protection law acts as a minimum standard. Where sector specific laws provide for standards that provide increased protection to data subjects, above the standards prescribed in the data protection law, such standards may be enforced.

8. Part III: Grounds of Processing, Obligation on Entities and Individual Rights

8.1. Chapter 1: Consent

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

Alternatives:

a. Consent will be the primary ground for processing.

b. Consent will be treated at par with other grounds for processing.

c. Consent may not be a ground for processing.

CCG Response: The concepts of choice and consent have been integral to data protection principles and laws across jurisdictions for many decades now[128]. However, changes in technology and business, leading to the collection and use of large amounts of personal information, have called into question the manner in which the consent principle is currently being applied.

Consent is often obtained in the form of standard form contracts where there is a power imbalance / information asymmetry in favour of the data controller who is obtaining the consent. The language used in consent documents is not typically user friendly, and even where a data subject does understand the terms of consent, they do not often have the ability to negotiate these terms. Data controllers leverage these imbalances, and typically insist on consent as a pre-requisite for provision of the service / product in question. As a result, data subjects are left with no option but to accept terms of consent that are most often onerous.

The above, among other reasons, have resulted in consent often being considered meaningless in the age of big data. This becomes more problematic given that in many jurisdictions, consent is considered the foremost of the data protection principles. Other traditional data protection principles such as purpose limitation are subject to / governed by the terms of consent[129].

In order to combat this, there have been calls to re-visit the data protection principles as they are understood today, particularly in the context of the consent principle. Harm / risk based approaches – which propose regulating the use of data only in the context of a harm, or risk of harm – have been suggested as viable alternatives[130]. Daniel Solove has suggested that the problems with consent can be addressed by

[128]Fred H. Cate, *The Failure of Fair Information Practice Principles,* CONSUMER PROTECTION IN THE AGE OF THE INFORMATION ECONOMY (2006) *available at* https://ssrn.com/abstract=1156972 (Last visited on February 25, 2018).

[129]*Id.;* Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARVARD LAW REVIEW 1880 (2013) *available at* https://pdfs.semanticscholar.org/809c/bef85855e4c5333af40740fe532ac4b496d2.pdf (Last visited on February 25, 2018).

[130]Cate, *supra* note 128; Rahul Matthan, *Beyond Consent – A New Paradigm for Data Protection*, Takshashila Discussion Document, 2017-03, *available at* http://takshashila.org.in/wp-content/uploads/2017/07/TDD-Beyond-Consent-Data-Protection-RM-2017-03.pdf (Last visited on February 25, 2018).

adopting the following measures (i) Rethinking consent and employing nudges i.e. architecting choices towards changing behavioural patterns, without actually forbidding or restricting actions under law, (ii) developing partial privacy self-management, where individuals have the option to manage their consent terms, but not necessarily in relation to all data processing, (iii) moving the focus of privacy law towards regulating use of data at the time when new purposes / uses of data are brought in, and (iv) ensuring that the data protection laws have more substantive rules on collection, use and disclosure of data[131].

Some suggest that since consent is no longer meaningful, there is no place for it in the data protection framework at all.

However, it is important to remember that the Indian data protection law is being drafted in the context of the recognition of the right to privacy, including informational privacy, as a fundamental right under the Indian Constitution. The data protection law must ensure that the right to informational privacy as a whole is preserved. This would include (a) allowing an individual to exercise autonomy over the use of their personal information, and (b) ensuring that the right to privacy is preserved, and that any violation of this right is checked, in addition to ensuring that any harms that arise out of the use of personal data are remedied[132].

In this context, consent is important to ensure that an individual's autonomy over their informational privacy is maintained. Therefore, we recommend adoption of an approach that works towards addressing and correcting the problems with consent, rather than doing away with it altogether.

Greenleaf has suggested that consent should mandatorily be 'unbundled' i.e. consent should be separated from information with which the consent terms should not be combined[133]. He notes that the GDPR adopts two provisions in this regard: (i)

---

[131]Solove, *supra* note 129.

[132]Smitha Krishna Prasad, *Back to the Basics: Framing a New Data Protection Law for India* (January 30, 2018*) available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3113536 (Last visited on February 25, 2018).

[133]Greenleaf, supra note 21.

separation of consents for each item requiring consent, not one overall consent[134]; and (ii) separation of consents from the collection of any other information not necessary for the performance of the contract[135]. He also recommends the adoption of the South Korean approach, where both forms of unbundling mentioned above are mandatory. We recommend that the Committee adopts this approach.

Some of the problems with consent can also be addressed by way of regulating consent, and ensuring that consent is no longer the focal point for implementation of the other data protection principles. Traditional provisions on consent typically prescribe the contents a notice / privacy policy / consent agreement should contain – these include the type of information being collected, purpose of collection / processing of information, third parties that the information may be transferred or disclosed to, among others[136]. However, in order to ensure that consent is no longer the focal point that is relied on for implementation of other principles, we also need to look at the substance of the law. A look at existing Indian laws that govern contracts, shows that there are several examples of provisions of law that govern the terms of contracts, for instance under the Indian Contract Act, 1872, or the Sale of Goods Act, 1930. Adopting some of Solove's suggestions, more substance can be brought into the law, by adding guidance on acceptable or unacceptable terms of such contracts of consent[137].

Some examples of potential restrictions that could be introduced in relation to the consent agreement are listed below[138]:

(i) Restrictions on limitation of liability by data controllers and processors

(ii) Broad provisions on acceptable and unacceptable terms in the context of purpose limitation – for instance, generic clauses such as permission for use of personal information for any current or future business purpose of the controller, may be considered invalid.

---

[134] Article 7(2), GDPR.
[135] Article 7(4), GDPR.
[136] *See for instance*: Rule 4, Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.
[137] Prasad, *supra* 132.
[138] *Id*.

(iii) Provisions may be included to regulate situations where controllers deny service in the absence of consent for collection and use of data that is not actually required for provision of the products / services that are the subject of the contract. This is particularly relevant where sensitive categories of information are collected and used.

(iv) Provisions addressing situations where data is processed or transferred / disclosed to third parties for the purpose of making (automated) decisions that affect provision of essential services (financial services, healthcare facilities) to individuals, on the basis of broad provisions that do not adequately inform the data subject.

(v) Sector or subject specific restrictions on terms of contract, particularly in situations where there in an obvious case of power imbalance between the parties, and / or information asymmetry – for instance in the context of collection of information from students or employees of an organisation.

The above allow individuals the flexibility of exercising their right to consent, while also providing them the assurance that some basic provisions of law that protect them will be applicable, even if they do not fully understand or know what they are consenting to.

In addition to the above, sector specific methods of ensuring meaningful consent may also be adopted. For instance, in the field of bioethics research, it has been suggested that "a power of attorney model that essentially allows the patient to outsource his or her ability to consent to more capable professionals might be more respectful, efficient, and more empowering to the patient"[139].

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?

CCG Response: Please refer to our response to question 1 in this chapter.

[139]Danielle Hornstein et al., *More nuanced informed consent is not necessarily better informed consent*, 15(9) THE AMERICAN JOURNAL OF BIOETHICS 51 (2015).

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

CCG Response: Please refer to our response to question 1 in this chapter.

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

CCG Response: Please refer to our response to question 1 in this chapter.

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

CCG Response: Please refer to our recommendations in our response to question 1 in this chapter. As mentioned earlier in our comments, while the effect of compliance on business is a valid concern, it cannot be used to override basic rights that form an integral part of the right to privacy.

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

CCG Response: We do not have additional comments on this chapter at this stage. We will follow up with additional comments if necessary.

8.2. Chapter 2: Child's Consent

1. What are your views regarding the protection of a child's personal data?

CCG Response: In the previous chapter, we have discussed the fact that it is becoming increasingly difficult if not impossible for individuals – adults – to provide informed and meaningful consent to the collection and processing of their personal information. At the same time we see that the collection and processing of personal information, by all manner of organisations is increasing daily, and is not limited to adults only. In this context, protecting the rights to children and reconsidering when children are capable of consenting and when they are not, is very important.

We recommend that the processing of children's data, and their capability to consent to such processing is considered in two separate buckets –

(a) *Collection and use of personal information for essential services and / or in the public interest*, for instance collection of basic identifying information of children by schools, collection and processing of data for provision of healthcare services, or even medical research in the public interest – in this context, collection and processing of personal information, or even sensitive information should be permitted, with informed and meaningful parental consent. Processing of sensitive personal information should be limited to circumstances where it is absolutely necessary, such as for the purpose of medical / healthcare services.

(b) *Collection and use of personal information for commercial services*, for instance use of information provided to social media websites, use of information for targeted marketing etc.: A stricter standard for collection and processing of personal information may be provided for in these situations – for instance, a requirement for explicit consent may be implemented. Data required to provide the commercial service may be collected, but not processed or retained beyond such immediate use. Collection and processing of sensitive personal information should not be permitted.

However, as mentioned in the White Paper, children are increasingly online, and are active users of many services that are not typically targeted at children. In order to address this, the solutions suggested in provisional view 2 above, may be adopted. Verifiable consent mechanisms (to verify that parental consent has been obtained) such as those recommended under US law may be considered[140].

In addition to the above, irrespective of the nature of consent provided, children should be provided with a specific time frame (for instance 5 years), after reaching the age of majority, to withdraw any consent provided before such age, and have

[140]Children's Online Privacy Protection Rule, 2000, *available at* https://www.ecfr.gov/cgi-bin/text-idx?SID=4939e77c77a1a1a08c1cbf905fc4b409&node=16%3A1.0.1.3.36&rgn=div5#se16.1.312_15 (Last visited on January 30, 2018); *See also:* Federal Trade Commission*, Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business,* available at https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance#step4 (Last visited on January 30, 2018).

any data that remains with the controller or processor deleted. In order to fully enforce these solutions, we recommend that the data protection law should require data controllers and processors to architect their systems in a manner that allows for such additional protections to be provided to children.

8.3. Chapter 3: Notice

The principles of notice, choice and consent typically go together, and as such we believe that the questions regarding the substance of notices to be provided by data controllers to data subjects have largely been addressed in the chapter on consent.

With regard to the form of notice, we agree with point 3 in the provisional views above. The data protection authority should work with the controllers to make notice documents more accessible for data subjects. Several relevant suggestions have been made during the public consultations held by the Committee and MEITY in this regard. These include ensuring that notices are accessible in regional languages where required, and creating a system similar to that of the Open Source Initiative, which provides standardised copyright licenses[141].

It is recommended that the Committee considers recommending the adoption of such methods. However, as a note of caution, it should also be clarified that these standard form, or easily accessible notices, should not be misused and turned into a tool for generating mass ‘consent’ for commercial entities. While adoption of forms of notice that are easy for data subjects to read and understand is a necessary element of ensuring individual autonomy, it should not preclude the applicability of other requirements and restrictions in relation to consent, under law.

8.4. Chapter 4: Other Grounds of Processing

Processing of personal data is considered lawful once a controller has procured consent. However, it has been acknowledged that pure consentbased processing has been ineffective in safeguarding the rights and interests of data subjects. It has been further acknowledged that procuring consent may not be possible, or might defeat the purpose of processing under certain circumstances.

[141]Pahwa, *supra* note 12.

Given the above, the Committee has proposed and sought comments on inclusion of grounds of processing, other than consent, which may make processing, lawful. In this regard, we would recommend a GDPR-style provision. At a macro level, our recommendation finds basis in the over-arching rights, risks, and harms based approach adopted by the Council of the EU in implementing the Directive and in drafting the GDPR. At a micro level, we find that Article 6 of the GDPR (Lawfulness of Processing) strikes a balance between the rights and interests of data subjects, and the interests of controllers.

1. Other Grounds of Processing

At the outset, we recommend that key principles, particularly the Data Minimisation Principle proposed by the Committee under Part V of the Consultation Paper be considered while framing provisions in relation to other grounds of processing.

1.1 Performance of Contract

Processing may be deemed lawful when it is necessary for:

- the performance of a contract to which the data subject is party; or
- in order to take steps at the request of the data subject prior to entering into a contract.[142]

The above covers two scenarios. Firstly, where personal data is processed to perform a contract with the data subject. For instance, further to an employment agreement with the data subject, the controller would necessarily require bank account details to pay salary. Secondly, where processing is necessary prior to entering into a contract with the data subject. For instance, where the data subject solicits a car insurance quote from an insurer - the make, year of manufacture of the car, etc., would necessarily be required to prepare a quote. Article 29 Working Party helpfully clarifies here that pre-contractual processing is lawful when undertaken at

[142]Recital 44; Article 6(1)(b), GDPR.

the request of the data subject, rather than at the initiative of the controller or any third party.

It is noteworthy that this provision covers situations where processing is genuinely necessary for the performance of a contract as opposed to being unilaterally imposed by the data controller.

In interpreting this provision,

- the substance and fundamental objective of the contract must be identified and assessed; and
- there should be a clear nexus between assessment of necessity and compliance with the Purpose Limitation Principle.

1.2 Compliance with Legal Obligation

This provision would provide legal basis to processing which is necessary for compliance with a legal obligation to which the controller is subject[143], for instance, statute mandated obligation on an employer to report its employees' salary related data to local tax authorities.

The obligation must be imposed by law (and not for instance arise under a contract) and should be mandatory (compliance should not be discretionary). Accordingly, voluntary unilateral engagements and public-private partnerships processing data beyond what is required by law are thus not covered. For instance, if - without a clear and specific legal obligation to do so – an Internet service provider decides to monitor its users in an effort to combat illegal downloading, this provision will not be an appropriate legal ground for this purpose.

Scope: obligation under Indian laws

Processing should be permitted if it is necessary for compliance with a legal obligation under the laws of India. Therefore, an obligation to process personal data arising under US law would not provide lawful basis for processing personal data.

[143]Recital 45; Article 6(1)(c) and 6(3), GDPR.

Article 29 Working Party guides that such law must fulfill all relevant conditions to make the obligation valid and binding, and must also comply with data protection law, including the requirement of necessity, proportionality and purpose limitation.

1.3 Protection of Vital Interests

This provision would provide a legal ground in situations where processing is necessary in order to protect the vital interests of the data subject or of another person (e.g., children of the data subject).[144] It is recommended that this provision be interpreted restrictively and its application should be on a case by case basis.

In its White Paper, the Committee has expressed that the scope of the grounds on which valid processing may take place would need to be well defined and may need to be bespoke. Drawing from the clarifications issued by Article 29 Working Party, vital interest appears to limit the application of this ground to questions of life and death, or at the very least, threats that pose a risk of injury or other damage to the health of the data subject or that of another person.

1.4 Performance of task carried out in Public Interest or in the exercise of Official Duty

This provision would provide a legal ground in situations where processing is necessary for the performance of a task carried out in the public interest of India or in the exercise of official authority granted by the Government of India vested in the controller or in a third party to whom the personal data is disclosed.[145]

To stand up to rigors of data protection law, processing must be necessary for the performance of a task carried out in public interest. Alternatively, either the controller or the third party to whom the controller discloses the personal data must be vested with an official authority and the data processing must be necessary to exercise the authority.

[144]Recital 46; Article 6(1)(d), GDPR.
[145]Recital 45; Article 6(1)(e), GDPR.

Official Authority / Public Task

Official authority or public task should typically emerge from an Indian statute or other applicable legal regulations.

Strict Interpretation

Given its broad scope and far reaching impact on the privacy of data subjects, this provision pleads for a strict interpretation and a clear identification, on a case by case basis, of the public interest at stake and the official authority justifying the processing. These questions, and the 'task carried out in public interest' would normally be subject to the provisions of the Constitution.

1.5 Legitimate Interest of Controller

This provision would provide a legal ground in situations where processing is necessary for the purposes of the legitimate interest of the controller or a third party except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

It is noteworthy that processing carried out by public authorities in performance of their tasks are excluded from the scope of this provision.

Balancing Test

At its core, this provision aims to provide guidance on applying a balancing test to determine whether this provision may be relied upon as legal ground for processing. More specifically, this provision guides on how to balance the legitimate interest of the controller or a third party against the interests or fundamental rights and freedoms of the data subject.

Broadly, essential elements of legitimate interest should be:

- Lawful (i.e., in accordance with applicable Indian law);
- Clearly articulated to allow the balancing test to be carried out against the interests and fundamental rights of the data subject;

- Represent a real and present interest (should not be speculative).

In the event that the interest of the controller or third party does not fall within the contours of legitimacy, the balancing test will not come into play as the initial threshold for the use of this provision will not have been reached.

Guidance may be taken from the Opinion[146] of Article 29 Working Party which endeavours to provide controllers with flexibilities for situations where processing does not cause undue impact on data subjects, while at the same provide legal certainty and guarantees to data subjects that this provision will not be misused. The Opinion further proposes the method of carrying out the balancing test and further guidances may be derived from the published results of Public Consultation on Opinion on Legitimate Interests of the Data Controller[147].

Briefly, the key factors that should be considered while applying the balancing test include:

- the nature and source of the legitimate interest;
- the impact on the data subjects;
- the balance of power between the data subject and the data controller;
- additional safeguards to prevent undue impact on the data subjects, including:
    - data minimisation;
    - accountability, transparency, the right to object and beyond.

2. Data Subjects' Right to Object

In cases where the controller relies on public interest (discussed at 2.4 above) or legitimate interest (discussed at 2.5 above) as lawful basis of processing, and given

[146]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* (2014) *available at* http://www.dataprotection.ro/servlet/ViewDocument?id=1086 (Last visited on January 30, 2018).

[147]Article 29 Data Protection Working Party, *Overview of results of public consultation on Opinion on legitimate interests of the data controller (Opinion 06/2014),* (2014).

that these grounds are not absolute, it is recommended that data subjects' be given the right to object to processing of their personal data.[148]

Guidance may be taken from the GDPR which obligates a controller to cease processing unless the controller:

- is able to demonstrate compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject; or
- requires the personal data in order to establish, exercise or defend legal rights.

Controller to bear the Burden of Proof

The Directive permitted an organisation to continue processing personal data unless the data subject could demonstrate that an objection to processing was justified. However, the GDPR reverses the burden and requires the organisation to demonstrate that it either has compelling grounds for continuing the processing, or that the processing is necessary in connection with its legal rights. If it cannot demonstrate that the relevant processing activity falls within one of these two grounds, it must cease that processing activity. This burden of proof is likely going to compel organisations currently relying on their own legitimate interests as a lawful basis for processing personal data to re-evaluate their interests.

8.5. Chapter 5: Purpose Specification and Use Limitation

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

CCG Response: The purpose and use limitation principles are integral components of data protection laws across jurisdictions, and have been for several years now. We have provided below an excerpt from Graham Greenleaf's submissions to the

[148]Recitals 50, 59, 69-70, 73; Article 21, GDPR.

Committee, explaining why these principles are important and continue to be relevant[149]:

"*It is essential for privacy protections that collection limitations are maintained, and that collection should be limited to what is necessary for the notified purpose of collection. 'Big data' proponents are attempting to argue that there should be no limits on collection, only some limits use. This approach is equivalent to also abandoning not only notice but the very idea of a purpose limitation collection, and with it any individual control over use of personal data based on knowledge or consent. While new technologies may mean that some personal data will inevitably be collected in situations where individual notice and consent are not possible, these can be dealt with by (i) recognising they are the exception, not the rule; (ii) limiting how such data can be used as personal data which has individual effects, even if it can be used for other purposes; and (iii) developing methods of notice, consent and exceptions for where use as personal data affecting individuals is desired or desirable*".

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

CCG Response: In this context we refer back to our submissions in the chapter on 'consent', and note that there is a need to ensure that these principles stand independently, and are not solely relevant in the context of consent. To this effect, we suggest that the purpose and use limitation provisions in the data protection law must be drafted with substance, as suggested in our submissions on consent, and specifically the examples provided there.

With regard to the questions that have been raised on the determination of whether subsequent uses are compatible with the initially declared purposes, we note and recommend as follows:

(a) if the recommendations we have made in relation to the chapter on consent are adopted, and purpose limitation is drafted as a substantive provision, then controllers and processors will be obliged under law to limit consent and use

[149]Greenleaf, *supra* note 21.

of data to specific, targeted purposes (as opposed to broad purpose limitation clauses)

(b) Should the personal data be required for a new ‘use’, not contemplated under the initial purpose, consent of the data subject should be obtained for the same

(c) Where the controller is doubtful about whether a particular use falls within the scope of the initial purpose, or requires fresh consent, a mechanism should be provided whereby the data protection authority can provide formal guidance. Records of such guidance should be maintained for transparency.

(d) In addition, regular privacy audits and impact assessments should be used in order to keep check on the purpose for which personal information is used and processed.

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?

CCG Response: We refer back to our response to Question 2 and note that adoption of the recommendations there would provide for adequate guidance in this regard.

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

Alternatives:

a. The sectoral regulators may not be given any role and standards may be determined by the data protection authority.

b. Additional/ higher standards may be prescribed by sectoral regulators over and above baseline standards prescribed by such authority.

c. No baseline standards will be prescribed by the authority; the determination of standards is to be left to sectoral regulators.

CCG Response: We recommend that where necessary, additional provisions may be made by way of rules and regulations, or otherwise to address sector specific concerns. However, the provisions of the data protection law should form the baseline that will need to be complied with at a minimum.

8.6. Chapter 6: Processing of Sensitive Personal Data

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

CCG Response: We note that the issue of defining the concept of 'sensitive personal information' has already been addressed in Part I, Chapter 4. Our recommendations on the categories of data that may be included under this definition have been provided accordingly.

With regard to the additional safeguards to be protected to these categories of data, we note that the EU's GDPR has the most comprehensive approach among the jurisdictions examined. It is also among the jurisdictions that provide the highest levels of protection in this regard.

As suggested by Greenleaf, "the GDPR provides the following special protections for sensitive data ('special categories'), among others:

(i) Processing (including collection of data) is entirely prohibited unless an exception applies (art. 9(2));

(ii) Additional limits are placed on using such data for automated decision -making (art. 22(4).

(iii) Overseas controllers who process such data on a large scale have additional obligations (art. 27(2).

(iv) Exemption to the obligation to keep records of processing may not apply (art. 30(5)).

(v) Their processing increases the need for data protection impact assessments (art. 35(3)(b)).

(vi) Their processing may result in the need for a data protection officer (art. 37(1)(c)).”[150]

We recommend that the provisions adopted by the GDPR in the context of processing of sensitive personal information is adopted in the Indian data protection law as well.

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?

CCG Response: We note that the issue of defining the concept of ‘sensitive personal information’ has already been addressed in Part I, Chapter 4.

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.

CCG Response: Please refer to our response to Question 1. As suggested in this response, we recommend the adoption of provisions similar to those in the GDPR.

[150]Greenleaf, *supra* note 21.

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?

CCG Response: We recommend that where necessary, additional provisions may be made by way of rules and regulations, or otherwise to address sector specific concerns. However, the provisions of the data protection law should form the baseline that will need to be complied with at a minimum.

8.7. Chapter 7: Storage Limitation and Data Quality

We note that as with the principles of purpose and use limitation, the principles of storage limitation and data quality are integral and long-standing principles of data protection law.

Data Quality:

We note that the requirements regarding maintenance of data quality in most jurisdictions are relative to the purpose for which the data is being used[151]. In this context, we do not believe that this is an onerous obligation as suggested in the White Paper. It is however, an important obligation given that in many situations, data controllers and processors may be making decisions that affect the data subject, on the basis of personal information that they assume is accurate.

We also note that while the individual data subject does and should have the right to access and correct their personal information where required, the **obligation** to ensure that data quality is maintained will remain with the data controller.

Storage Limitation:

We note that a look at the data protection laws adopted by international jurisdictions (many of which are referenced in the White Paper), show that the standard

[151]Greenleaf, *supra* note 21.

provisions for storage limitation provide that personal data should be "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed"[152]. We recommend that this internationally accepted standard is adopted in India, and see no reason for the introduction of the concept of 'reasonably necessary' in this context, as suggested in the White Paper.

8.8. Chapter 8: Individual Participation Rights – I: Right to Confirmation, Right to Access, and Right to Rectification

We recommend that the rights discussed in this chapter should be available to data subjects, in the manner that allows them to exercise autonomy over their personal information best. We recommend adoption of provisions along the lines of those in the GDPR, in this regard. These rights should be available in relation to all personal information that identifies an individual[153], and exceptions to these rights should be limited.

As noted in the White Paper, awareness of these rights may be low, even in jurisdictions such as the EU. However, these are important rights that allow individuals to understand the manner in which their personal data is being used, and identify whether or not they are comfortable with such use. In this context, efforts should be made to educate individuals about, and encourage them to exercise their rights - it may not be very helpful to impose a fee on individuals who do wish. We note here that the right to access, review and correct their information is also currently available to individuals under the IT Rules. The inclusion of these rights under the new data protection laws should not then create a difficult situation in terms of increased cost of compliance as suggested in the White Paper[154].

[152]Article 5(1)(e), GDPR.

[153] We note that in Part II, Chapter 3 on definition of personal information, it has been recommended that these rights may not be provided to the extent that the information does not identify the individual at the time.

[154]White Paper, at 24.

8.9. Chapter 9: Individual Participation Rights – II: 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

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

CCG Response: The rights described in this chapter are important rights that allow individuals to fully exercise their right to informational privacy in the context of the way technology operates and functions today. We recommend that these rights are incorporated in the Indian data protection law.

The right to restrict processing, object to processing and processing for the purpose of direct marketing are both contemporary, relevant rights that are being incorporated in data protection laws in many jurisdictions today[155]. On the right to object to processing, the sole concern expressed in the White Paper is that it is applicable in contexts that are not currently recognised as grounds of processing in India. It is not clear however, why this should prevent us from incorporating this right if it is otherwise considered relevant. Our recommendations in the chapter on other grounds of processing specify that the grounds adopted in the GDPR may be adapted and incorporated in the Indian context. Accordingly, we recommend that the right to object to processing is also granted to individuals.

With regard to the right to object to processing for the purpose of direct marketing, we agree with the views expressed in the White Paper, that there is a need for a framework which provides for direct and unsolicited marketing across sectors / means of communication.

The right to data portability and the right not to be subject to a decision solely based on automated decision making are also both important rights, the denial of which could adversely impact individuals. In the first case, where controllers are not

[155] *See* Greenleaf, Graham, *'European' Data Privacy Standards Implemented in Laws Outside Europe,* 149 PRIVACY LAWS & BUSINESS INTERNATIONAL REPORT 21-23 (September 3, 2017) *available at* https://ssrn.com/abstract=3096314 (Last visited on February 25, 2018).

operating in a privacy friendly manner, individuals should be permitted to port to other controllers. We have elaborated more on the right to data portability in our response to question 2. The right not to be subject to a decision solely based on automated decision making is equally important, considering the potential issues that individuals could face as a result of inaccurate decision making – ranging from receiving promotional material for services you are not interested in, to unjustified discrimination on the basis of social factors[156].

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?

CCG Response: Please see our response as it relates to the right to data portability below. Our comments on the right to restrict processing are included in our response to Question 1.

In the course of using online services, individuals typically provide an assortment of personal data to service providers. The right to data portability allows a user to receive their data back in a format that is conducive to reuse with another service. For instance, Apple Music users could switch to a rival service without having to lose playlists, play counts, or history; or Amazon users could port purchasing history to a service that provides better recommendations. Crucially, users could also port to services with more privacy friendly policies, thereby enabling an environment where services must also compete on such metrics.

Data Portability is premised on the principle of informational self-determination, which forms the substance of the European Data Protection framework. This concept was famously articulated in what is known as the Census decision of the German Federal Constitutional Court in 1983. The Court ruled it to be a necessary condition for the free development of one's personality, and also an essential element of a democratic society. In this regard, the right to data portability operates to restore the data subject's autonomy over her personal data.

[156]Article 29 Data Protection Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679* (2017) *available at* http://ec.europa.eu/newsroom/document.cfm?doc_id=47742 (Last visited on February 25, 2018).

While there may be some costs associated with the operationalization of the right to data portability, there is a strong case for incorporating it into India's data protection regime. First, data is a non-rival, unlimited resource, and has great economic potential if maintained in interoperable and machine-readable formats. Data portability gives greater choice and control to the consumers with respect to their data held by other entities. It also creates a level playing field for newly established service providers that wish to take on incumbents, but are unable to do so because of the significant barriers posed by lock-in and network effects[157]. Data portability thus has the potential to enhance competition between service providers, since new providers will find it easier to attract new users once they can take their data with them[158].

The current Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, already recognize rights such as the right to access and the right to erasure of personal data. Data portability is in a sense, an evolution from these rights, with greater interoperability requirements.

Finally, as stated earlier, the adoption of the right to data portability by the EU GDPR is itself a compelling case for incorporating it in India. This would further bring India's regime in parity with the EU regime, so that India can meet the adequacy requirements imposed by the GDPR.

Under the GDPR, the right to data portability is subject to certain conditions. It applies only to personal data that the data subject 'provided' to the controller; the processing must be pursuant to consent or a contract, therefore, data processed in public interest, or in the exercise of official authority is excluded; the processing must

[157]Article 29 Data Protection Working Party, *Guidelines on the right to data portability,* 5 (2016) *available at* http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_en_40852.pdf (Last visited on February 25, 2018).

[158]Inge Graef et al., *Putting the Right to Data Portability into a Competition Law Perspective*, THE JOURNAL OF THE HIGHER SCHOOL OF ECONOMICS, ANNUAL REVIEW 53 (2013) *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2416537 (Last visited on February 25, 2018).

be through automated means; the right must not adversely affect the rights and freedoms of others.

The above scheme is premised on the articulation provided by the GDPR, and would have to be suitably amended for the Indian statute. However, the condition that the right to data 'provided' by the subject is a crucial limitation. This entails that the right covers data explicitly provided, such as age, or address, etc., through online forms; as well as data generated and collected by controllers on account of the usage of the service. However, data derived or inferred by the controller would not be within the scope of this right[159]. The scope of the term 'provided by' is currently subject to dispute, and will require suitable clarifications[160].

8.10. Chapter 10: Individual Participation Rights – III: Right to be Forgotten

CCG Response: We agree with the provisional views in this chapter of the White Paper. The ability for individuals to determine for themselves when, how, and to what extent information about them is communicated to others is an integral part of the right to privacy. Recognizing the right to be forgotten would be a step in that direction. However, it is important that this right should not be used to compromise transparency and free flow of information in our democracy. The right must therefore come with exceptions for public figures, archiving in public interest and other major public interest goals as are listed in the GDPR.

As a first step to recognizing this right, we need to understand what it constitutes. A basic definition or principle to start with can be that "if an individual no longer wants his personal data to be processed or stored by a data controller, and if there is no legitimate reason for keeping it, the data should be removed from their system."[161]

---

[159]*Supra* note 157, at 8.

[160]David Meyer, *European Commission, experts uneasy over WP29 data portability interpretation,* IAPP (April 25, 2017) *available at*https://iapp.org/news/a/european-commission-experts-uneasy-over-wp29-data-portability-interpretation-1/ (Last visited on February 25, 2018).

[161]Viviane Reding, Vice President, Eur. Comm'n, The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age 5 (Jan. 22, 2012).

We recommend that the data protection law should draw upon this principle, in determining the scope of the right in India.

The right should be exercisable in respect of personal data that is both provided by the individual and to information about an individual that is provided by a third party. It must also deal with the right to de-linking / de-indexing, as seen in the European Court of Justice's decision in *Google v. Spain*[162], and in addition to the right to erasure of the information from the controller's possession.

The limitations and restrictions on the right itself can vary, depending on the context in which the information was provided.

We recommend that the Committee looks into the different mechanisms in place across jurisdictions, not just in the context of the right to be forgotten, but also take down of content online for various reasons.

9. Part IV: Regulation and Enforcement

9.1. Chapter 1: Enforcement Models

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

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

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

CCG Response (to Questions 1, 2 and 3):

The concepts and issues raised in each chapter under this part of the White Paper are important. However, we believe that it is best to look at the concepts of regulation and enforcement holistically to begin with at least. Below we have provided our comments on the nature of monitoring and enforcement models that

[162] Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González (C-131/12).

may be incorporated under India's data protection law, and the roles and responsibilities of some of the actors in this field.

It is always useful to start with examining the purpose and object of regulation. The creation of a data protection framework in India is arguably directed mainly at protecting the human right to privacy. This goal should be kept in mind as we examine the regulatory frameworks to best implement the Indian data protection rules. Before we discuss the enforcement models set out in the questions, we wish to note that our responses to the White Paper already contemplate other regulatory strategies such as information disclosure and creation of rights and liabilities[163].We would urge the data protection committee to use the full spectrum of regulatory strategies to enforce different elements of the data protection framework as may be appropriate.

The White Paper examines the concepts of 'self-regulation', 'co-regulation' and 'command and control regulation' and suggests that 'co-regulation' may be adopted. However, co-regulation, despite its significant advantages especially in terms of industry involvement, is only successful under certain circumstances[164]. It poses risks like regulatory capture and domination of incumbent industry players with greater resources such that new entrants with less capacity to engage with the regulator find themselves disadvantaged.

We would therefore urge the committee to keep an open mind and not to create the risk of capture of a newly formed regulator or regulatory framework at the start. It is possible instead to build an open consultative process, in which consumers and users have at least as much access to the enforcement mechanism as industry does. Over time, it may be possible to contemplate a multi-stakeholder regulator rather than a co-regulator so that all interests, not just industry priorities, are accounted for as the regulator makes its decisions.

However, in the interests of effective enforcement, it is possible to follow an enforcement model which is nimble and able to gradually ensure that the data

[163] Refer to responses above in relation to Part III of the White Paper, specifically, Chapter 1, 8 and 9.
[164]Greenleaf *supra* note 21.

protection principles are actually enforced. From this point of view, it is useful to consider the principles of 'responsive regulation',[165]. This is a system in which the regulatory mechanism takes into account the differing motivations of regulated actors and builds this into its responses. For example, some subjects of regulation may not follow rules for lack of information on how they might comply. Others might be persistent, creative even, in the violation of rules demonstrating that it is not lack of information but the intention not to comply that drives them. It takes different kinds of responses to make these differently motivated actors comply and ideally a regulatory system should build these responses into its functioning.

Ayres and Braithwaite suggest that there is a need for a range of sanctions to be available to the regulator, in order to enable the regulator to regulate in a responsive manner – they suggest that compliance is most likely when an agency displays an explicit enforcement pyramid[166]. The pyramid begins with softer tools that require the least amount of regulatory intervention at the bottom, and moves up towards the highest level of regulation, for instance from self-regulation to command regulation with non-discretionary punishments[167].

It may be beneficial to build in such a range of regulatory tools that allows for enforcement of the data protection law. Some such tools should be applicable ex-ante – for instance provision of informal guidance, private warnings etc[168]. These suggestions can be built upon to provide a full range of ex-ante and ex-post tools for enforcement. As an example, this could mean that if the ex-ante tools suggested above are at the bottom of the pyramid, the top of the pyramid will provide for imposition of non-discretionary fines and penalties, with the highest penalties being imposed where all ex-ante tools have been tried and have failed.

---

[165] Ayres, I., & Braithwaite, J., *Responsive regulation: Transcending the deregulation debate* (1992).
[166] *Id*, pg 36.
[167] *Supra* note 165, pg. 49.
[168] Malavika Raghavan, *Before The Horse Bolts*, THINK PRAGATI, (January 11, 2018) *available at* https://www.thinkpragati.com/brainstorm/3180/before-the-horse-bolts/ (Last visited February 25, 2018).

4. Are there any alternative views to this?

CCG Response: We do not have additional comments on this chapter at this stage. We will follow up with additional comments if necessary.

9.2. Chapter 2: Accountability and Enforcement Tools

Accountability

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

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

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

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

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

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

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

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

CCG Response (to questions in this chapter):

We agree that accountability is an important principle that should be incorporated in the data protection law. The accountability framework recommended in the provisional views seem to be similar to that in the GDPR, providing for data controllers to be responsible for, and be able to demonstrate compliance with the other principles[169]. We recommend the adoption of this approach.

As discussed in our comments to the chapter on consent, we note that there has been an increasing reliance on consent to ensure compliance with data protection laws and principles (beyond consent). Our comments also discuss the reasons this is problematic. Adoption of accountability frameworks might work towards reducing this reliance. We have suggested certain limited solutions in this regard.

We also recommend looking into other accountability frameworks, in addition to the GDPR standards mentioned above. The framework used may need to vary depending on the technology being used to process the data. For example, Crawford and Schultz's suggest the use of digital due process requirement in the context of big data and algorithmic processing[170].

ENFORCEMENT TOOLS

Codes of Practice:

1. What are your views on this?

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

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

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

[169]Greenleaf *supra* note 21.

[170] Kate Crawford and Jason Schultz, *Big data and due process: Toward a framework to redress predictive privacy harms*, *BCL REV.* 55 (2014) 93.

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

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

7. Are there any alternative views?

CCG Response (to questions in this chapter):

We note that implementation of codes of conduct may be a good practice to encourage data controllers and processors to adopt privacy friendly measures. However, in many situations these organisations have little incentive to put in place and implement self-regulatory or co-regulatory codes of conduct, as described in the White Paper. Rule 8 of the IT Rules is one such example – Rule 8(3) provides that "Any industry association or an entity formed by such an association, whose members are self-regulating by following other than IS/ISO/IEC codes of best practices for data protection as per sub-rule(1), shall get its codes of best practices duly approved and notified by the Central Government for effective implementation". However, in 7 years, we are yet to see any such codes of best practices.

While such codes, when implemented, may be useful, we recommend that that codes of practice or conduct should not be relied upon for implementation of the law. They may be used to offer poorly resourced companies and new market entrants some guidance on how they may comply, thereby reducing the cost of compliance. However, the data regulation framework must make the safeguards discussed elsewhere in our submission mandatory.

PERSONAL DATA BREACH NOTIFICATION

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

CCG Response: To assume the unimpeachable security of data is to overlook the ever-present potential of breach in storage security. As innumerable stories of data leaks evidence,[171] data is never fully secure, and one must necessarily put in safeguards. Additionally, there must also be processes in place in the event data

[171] See Manworren, Letwat & Daily, *Why you should care about the Target data breach*, 59 BUSINESS HORIZONS 257 (2016).

security is breached. One of the questions that arises, in the event of such a breach, is whom to inform. Ought the data protection authority be informed, and when? Ought the individuals, whose data is breached, be informed, and under what circumstances? Ought the public be informed, and when?

In data protection, these questions are answered through the use of data breach notification statutes. These laws stipulate the actions that a data controller and/or processor must take in the event of a breach in personal data security; specifically, whom to notify, under what circumstances, and within what time. The underlying idea is that a security breach must be notified, and cannot be kept secret by the data controller and/or processor, and must inform at three levels: the data protection authority, individuals and the public, where needed.

Why notify at all? A personal data breach is a breach of privacy, and as such, has a direct impact on the lives of individuals. A notification of the breach informs individuals of their breach of privacy, which may permit them, *inter alia*, to take steps to protect themselves against the violation. At the institutional level, it enables both the controller entity and the data protection authority to take steps, wherever possible, to minimize the harms arising out of the breach in security.

2. How should a personal data breach be defined?

CCG Response: A personal data breach notification law protects individuals against a data breach. A personal data breach refers, broadly, to a breach in security of personal data or personal information. Conceptually, it is a breach of confidentiality, integrity, authenticity or availability of data. The scope of its protection depends on the definition of ‘personal data’ or ‘personal information’, while its range depends on the definition of ‘breach’.

For optimal protection, it is important that the definition of ‘personal data’ remain as broad as possible. Definitions from across several jurisdictions assist us in exploring such a definition. Canada’s concise definition states that “*personal information means information about an identifiable individual*”. Other jurisdictions expand this definition further, with South Korea’s Protection of Personal Information Act, 2011 (PIPA) stating:

> "Personal information" shall mean the information pertaining to any living person that makes it possible to identify such individual by his/her name and resident registration number, image, etc. (including the information which, if not by itself, makes it possible to identify any specific individual if combined with other information).

South Korea's definition is broader, expanding on the nature of information that makes it possible to identify an individual. The expansion makes it easier to identify personal information. The GDPR is similar, in that it sets out a clear understanding of the content of personal information or data. Under the GDPR, 'personal data' means

> any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

As can be seen, the GDPR has a rightly expanded scope of protection. Taking its cue from the perspective of privacy, the GDPR does not require that the information be about an individual who may be effortlessly identified from the information accessed. It does not require that a ready identification be available. In addition, the GDPR makes an express provision for information that may only possibly identify an individual. In doing so, the GDPR recognizes that a multiplicity of information may be needed or used to identify an individual. The convergence of several points of data/information may be what identifies an individual, but it is meaningless to protect only the converged information. In the absence of protection of each separate component of data, the individual remains vulnerable to identification. It is this possibility that the GDPR (and in their own more limited way, South Korea and Canada) precludes by adding the term 'identifiable' in its definition.

South Africa has, perhaps, one of the most expanded definition of ‘personal information’ possible. Not only does it expand its definition to ‘juristic persons’, it elaborates on the content of ‘personal information’. It an inclusive definition, it considers the following data as falling within the scope of ‘personal information’:

(a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, conscience, religion, belief, culture, language and birth of the person;

(b) information relating to the education, or the medical, financial, criminal or employment history of the person;

(c) any identifying number, symbol, email address, physical address, telephone number, location information, online identifier, or other particular assignment to the person;

(d) the biometric information of the person;

(e) the personal opinions, views or personal preferences of the person;

(f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature, or further correspondence that would reveal the contents of the original correspondence;

(g) the views or opinions of another individual about the person;

(h) the name of the person if it appears with other personal information relating to the person or if the

> disclosure of the name itself would reveal information about the person;

The South African definition clarifies the content of 'personal information' or 'personal data'. Such clarity (along with the necessity of an inclusive definition) is helpful. It permits data controllers and/or processors to understand the scope of information to be protected, and also about the scope of security to be granted to such information. As such, it is our submission that in order for a 'personal data breach' to be usefully defined, the scope of 'personal data' or 'personal information' must be as broad, inclusive and clearly defined as possible.

In it is this context that a breach becomes relevant. In order to provide for the maximum protection to personal data or information, the breach definition must be defined as a breach of confidentiality, integrity, authenticity and availability of data[172]. That is, any foray into the protected personal data that is predicated on unauthorized access must be the focus of the breach definition. Any such access that results in access, destruction, loss, alteration, disclosure or acquisition of personal data within the control of the data controller or processor must be included within the breach definition.

California's data breach notification statute is clear and concise, defining a breach of the security system as an "unauthorized acquisition" of data that "compromises the security, confidentiality, or integrity of personal information."[173] However, such a concise definition has its flaws. It leaves it to the controller and/or processor's decision as to what breach jeopardises the confidentiality, integrity or security of personal data. Instead, it is more instructive to list out a series of instances where a breach of security has occurred. The EU GDPR is a good example. It defines a personal data breach as

---

[172] Sasha Romanosky, Rahul Telang & Alessandro Acquisti, *Do Data Breach Disclosure Laws Reduce Identity Theft?*, 30(2) J. POL. ANAL. MANAGEMENT 256 (2011), available at at http://ssrn.com/abstract=1268926 (Last visited February 25, 2018).

[173] Dana Lesemann, *Once More Unto the Breach: An Analysis of Legal, Technological and Policy Issues Involving Data Breach Notification Statutes*, AKRON INTELLECTUAL PROP. J. 203, 214 (2010).

> a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

As is clear, the GDPR lists out the *consequences* of a breach in security as a method of definition, and as such, makes it eminently clear in what circumstances a breach may occur. Any act that has an unintended consequence on the protected personal data qualifies as a breach in security. Canada's PIPEDA has a similar, if less expanded, definition:

> breach of security safeguards means the loss of, unauthorized access to or unauthorized disclosure of personal information resulting from a breach of an organization's security safeguards that are referred to in clause 4.7 of Schedule 1 or from a failure to establish those safeguards.[174]

South Korea, on the other hand, does not define a personal data breach, and merely requires notification in the event "personal information is leaked".[175] This method must be avoided, as it limits the definition of a personal data breach to merely unauthorized disclosure of personal data, and excludes from definition the myriad other ways in which security may be breached. The Pennsylvanian statute, similarly, limits the definition of a personal data breach to "unauthorized access and acquisition".[176]

Finally, many states create an exemption from notification for encryption or other security safeguards put in place to secure personal data. The Californian statute, for instance, requires notification only in the case of "unauthorised acquisition of unencrypted and computerised personal information".[177] Similarly, the Colorado law

[174] Section 2(1), PIPEDA.
[175] Article 34(1), PIPA.
[176] 73 PA. STAT. ANN. § 2302.
[177] Mark Burdon, Bill Lane, Paul von Nessen, *If it's Encrypted its Secure! The Viability of US State-Based Encryption Exemptions*, COMPUTER LAW & SECURITY REVIEW 26.2 (2010):

requires notification only where the information is “not encrypted, redacted, or secured by any other method rendering the name or the element unreadable or unusable”.[178] Even the GDPR creates an exemption. It states that communication to a data subject shall not be needed where:

> the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption.[179]

However, as Burdon, Low and Reid argue, the “simple technical act of encryption does not always provide effective information protection”.[180] They take the example of the Linden Labs data breach, where unencrypted information such as names, addresses were accessed, along with some encrypted information such as credit card details. As they rightly argue, it is not enough to encrypt some pieces of personal information, but encryption must be “viewed as a continuing process of information security assessment that goes beyond the simple act of encrypting certain pieces of personal information”.[181]

More importantly, as this response discussed earlier, the definition of ‘personal data’ places within it information including names, addresses, race, gender, sex, sexual orientation, etc. It is not necessary that these are encrypted in all databases, and it may even be argued that such information is not private as it is publicly available in multiple documents. However, this is a fallacy, and it is submitted that one must place the definition of personal data, i.e., “any information about an identified or identifiable individual”, at the highest consideration.

115-129, available at http://linkinghub.elsevier.com/retrieve/pii/S0267364910000208 (Last visited on February 25, 2018).

[178] COLO. REV. STAT. § 6-1-716.

[179] Article 34(3)(a), GDPR.

[180] *Supra* note 177.

[181] *Id*.

Two options are available. First, an approach such as the Minnesota law may be accepted. The law states that notification is required where "data is not secured by encryption or another method of technology that makes electronic data unreadable or unusable, or was secured *and the encryption key, password, or other means necessary for reading or using the data was also acquired*".[182]

As the law clarifies, notification is necessary where, even though encrypted or otherwise protected, the unauthorized access to the data can or has also bypassed those safeguards. This is a via media. The progressive approach would be to require notification irrespective of encryption or other safeguards, and to make this clear in the law. Such a law protects against the vulnerabilities of even encryption, and is therefore, better suited to protecting the interests of data subjects[183].

3. What are the circumstances in which data breaches must be informed to individuals?

CCG Response: While data breaches may be numerous, it may be argued that not all of them need be reported. As such, it is important to have a threshold for the reporting of data breaches. Such reporting, which must be done by the data controller to the data protection authority, to individuals or to the public, depends on several criteria. Some of these criteria include the size of the data controller entity and the databases it maintains, the timeframe required to detect breaches, the magnitude of the breach and the number of data subjects affected, etc[184].

THE STRICT LIABILITY APPROACH

Two conceptual bases may apply to data breach reporting, and both may be beneficially applied in this instance. The 'strict liability approach' requires that reporting occur at the instance of the data breach, irrespective of the presence or

[182] MINN. STAT. § 325E.61 (2006).
[183] Mark Burdon, *Contextualizing the Tensions and Weaknesses of Information Privacy and Data Breach Notification Laws*, 27(1) SANTA CLARA HIGH TECH. L.J. 63 (2011).
[184] *Id*.

absence of potential harms arising from the breach[185]. That is, if a breach occurs, and the data controller and/or processor comes to such knowledge, it must be reported. This simple standard is applied in the Californian statute, which requires notification if there is an "unauthorized acquisition" of data, compromising the "the security, confidentiality, or integrity of personal information".[186] The North Dakota statute is similar, which requires notification whether or not the breach results in compromise of personal information. Lesemann notes that thirteen American states follow the strict liability model[187].

While the strict liability model requires the extent of reporting that may lie heavily on data controllers, it has its advantages. First, all security breaches go reported, which allows the controller and/or processor entity to investigate the breach and to ensure that no harm may arise as a result of it[188]. Second, it allows the controller entity to keep track of all breaches, and to upgrade its security safeguards where necessary.

It is submitted that the strict liability model should be applied in the Indian law. The strict liability model may be used to require the reporting of data breaches by data processors to data controllers. When it comes to the knowledge of the data processor that there has been a breach in data security, it must, without fail and without delay, report the same to the data controller. There need be no other determination made by the processor; it merely has the responsibility to report. The EU GDPR adopts this approach, when it states: "The processor shall notify the controller without undue delay after becoming aware of a personal data breach"[189].

---

[185] Dana Lesemann, *Once More Unto the Breach: An Analysis of Legal, Technological and Policy Issues Involving Data Breach Notification Statutes*, AKRON INTELLECTUAL PROP. J. 203, 213 (2010).

[186] CAL. CIV. CODE § 1798.82(d).

[187] *Supra* note 185.

[188] Mark Burdon, Dana Lane & Paul von Nessen, *The mandatory notification of data breaches: Issues arising for Australian and EU legal developments*, 26 COMP. L. SEC. REV. 115 (2010).

[189] Article 33(2), GDPR.

THE RISK ASSESSMENT MODEL

While the strict liability model has the advantage of not leaving anything to the subjective determination of data controllers and/or processors, another, more nuanced model is also available. The 'risk assessment' model incorporates a materiality element in the determination of a breach that requires reporting. That is, where potential harm to the data subject can be ascertained, whether in the form of violation of rights and freedoms, such as privacy, or more tangible physical harms, then reporting is mandatory.

Several states take this approach. The EU GDPR requires mandatory notification "unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons".[190] Similarly, Canada's PIPEDA requires reporting "if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to the individual".[191] Several American states require that data controllers conduct "reasonable investigation" to examine whether there has been misuse of personal information[192].

The flaw in the risk assessment model is that it leaves the determination of risk of personal harm to the data controller. Canada's PIPEDA precludes this possibility by providing an inclusive list of harms:

> For the purpose of this section, significant harm includes bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property.[193]

This is a helpful provision, as it guides the controllers' determination of what constitutes harm, while arriving at "risk to the rights and freedoms of natural persons". It is thus submitted that the risk assessment model may be adopted in the

[190] Article 33(1), GDPR.
[191] Section 10.1(3), PIPEDA.
[192] *Supra* note 183.
[193] Section 10.1(3), PIPEDA.

case of mandatory reporting to the data protection authority and data subjects, along with a guide to determining what constitutes 'risk of harm'. Where there exists such risk of harm, notification to the data subject is mandatory.

It is submitted that India may adopt the Canadian approach of defining, inclusively, what constitutes 'harm'. In order that such determinations are not left to the sole discretion and judgment of the data controllers, it is submitted that an oversight mechanism be established. The data controller must provide a written assessment to the data protection authority of its determination of 'harm' to the data subjects, arising out of the data breach. The authority may then come to an independent conclusion as to whether, in such instances, there exists a risk of harm to data subjects.

One issue that must be carefully noted is that the data controller need not wait for the data protection authority's independent determination of 'risk of harm' in order to notify data subjects of the breach. Such a determination by the authority may occur *post-facto*.

Finally, in cases where the magnitude of the leak is high, the controller should, in addition to, communicating individually to every data subject, issue a public communication containing details regarding the nature of the breach, the estimated number of data subjects affected, the measures taken to reestablish data security, etc.

4. When should personal data breach be notified to the authority and to the affected individuals?

CCG Response (to Questions 3 and 4): Once a breach has been detected, when ought the controller and/or processor report the same? A timeframe for notification is not easy to establish, but lessons may be drawn from other jurisdictions. The EU GDPR, for instance, differentiates between notification to the authority and to data subjects, and between data processors and data controllers.

Data processors, when they gain knowledge of the breach, are required to notify data controllers "without undue delay".[194] Data controllers, when have knowledge of the breach, are required to notify the supervisory authority within 72 hours. The risk assessment element in the law thus requires data controllers to determine the risk of harm within 72 hours. While this is a short time, it minimizes the risk of expanding harm to data subjects. Other jurisdictions, such as Canada and South Korea, incorporate the terms "as soon as feasible"[195] and "without delay".[196] Other American states require notification within the "most expedient time possible," "without unreasonable delay," or "as soon as possible."[197]

A question may arise as to when knowledge of the breach is gained, as this is when the time period starts operating. Lesemann argues that the breach detection is the point of knowledge, and not when the investigation of the breach is complete[198]. It is submitted that such a definition, which clarifies the meaning of 'knowledge', along with a timeframe for notification, is apt.

It is submitted that India would benefit from following the EU GDPR's model of notification timeframe. From the point of breach detection (the starting point of actual knowledge), the controller may have 72 hours to report the breach to the data protection authority. This intimates that a preliminary assessment of 'risk of harm' must occur within 72 hours. Following further determination of 'risk of harm', the controller must then notify the data subjects "*without delay*". The use of the term "unreasonable delay" or "undue delay" create the possibility of subjective assessment, and should be avoided. Ideally a time frame must be provided within which such notification is mandatory.

[194] Article 33(2), GDPR.
[195] Section 10.1, PIPEDA.
[196] Article 34(1), PIPA.
[197] *Supra* note 185.
[198] *Id*., at 235.

5. What details should a breach notification addressed to an individual contain?

CCG Response: A breach notification to a data subject must enable her to take steps to protect herself from the potential consequences of the breach. The Canadian Act sets this out expressly, where it states:

> sufficient information to allow the individual to understand the significance to them of the breach and to take steps, if any are possible, to reduce the risk of harm that could result from it or to mitigate that harm.

As such, a breach notification must contain details concerning the nature of the data breach (including the identities and other relevant details of those who committed the security breach), the potential consequences of the breach, the estimated number of data subjects affected (or the magnitude of the breach), steps taken by controller entity to minimize the harms arising out of the breach, steps that the data subject may take in order to protect herself from harm, and importantly, must provide a contact at the controller organization, whom the data subject may correspond with to allay concerns or find out further information.

The EU GDPR requires that the breach notification contain the following information[199]:

> (a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
>
> (b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;

[199] Article 33(3), GDPR.

(c) describe the likely consequences of the personal data breach;

(d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

The South Korean law is similar, differing only in that the notification must also explain how and when the leak occurred[200]. It is submitted that the EU GDPR provides a comprehensive list of information necessary to include in a breach notification to a data subject. A public communication, where considered necessary, must also have such information.

6. Are there any alternative views in relation to the above, others than the ones discussed above?

CCG Response:

Other Issues

Record maintenance is crucial when considering data breaches; they allow stakeholders to assess the security performance of the data controllers. As such, it is submitted that India's data protection law mandate the keeping of records. Such a record must include a list of all notifications provided to the data protection authority and data subjects, along with details of the breach), the written assessments of 'risk of harm', and also note whether data subjects were informed or not.

It is submitted that the law also mandate transparency with regard to such records. As they refer to past security breaches, they will pose no threat, and will not compromise data controllers in any manner whatsoever.

[200] Article 34, PIPA.

Summary and Conclusion

A data breach notification law is crucial to assist data controllers and individuals in instituting measures to protect themselves against a breach in security. Notifying the data protection authority and individuals of breaches in data security enables them to anticipate the consequences of the breach. The effectiveness of such a law depends, inter alia, on its scope and range, on the conditions and timeline under which a notification must be made. Further, in order to assist individuals effectively, a data breach notification law must provide relevant and helpful information addressing the breach.

In order to so assist data controllers, the authority and individuals, the data protection law must provide the broadest definition to 'personal data'. Lessons may be drawn from the EU GDPR, which subsumes within its definition both information that is about an individual already identified, and information that may, by itself or when placed in conjunction with other information, be used to identify an individual. The South African Protection of Personal Information Act is also instructive, in that it provides an inclusive list of information that forms part of 'personal data', and thus enables a clearer understanding of the term.

A breach definition, consequently, must also be broad enough to address breaches in the confidentiality, integrity, authenticity and availability of data. That is, if personal data has been leaked (either publicly or to a limited non-authorised entity), there has been a breach of security of personal data. If the source of personal data, previously known, is currently unconfirmable or wrong, similarly, a breach in security may be inferred. Moreover, if the contents have been tampered with, or if data that was available to either the processor or the controller (or the individual, as the case may be) becomes, then a breach in security may be inferred. Importantly, the use of encryption or other protective measures should not be excluded from a personal data breach definition. Such protective measures are not infallible, and data remains vulnerable so long as there is a breach.

Once defined, it is important to understand in what circumstances a data breach must be notified to the data protection authority, to individuals or to the public. A data processor must, under all circumstances, be responsible for immediately notifying

the data controller of any breach in security of data under its processing. A data controller must also be responsible for notifying all breaches of personal data to the data protection authority. In this case, a ‘strict liability approach’ should be followed. However, when it comes to notifying individuals, a ‘risk assessment’ model may be utilized. That is, if there is a likelihood of harm (in the form of violation of privacy or other human rights, or of more tangible harm) to individuals from the breach in security, then individuals must be notified. Companies must be incentivized to err on the side of more rather than less disclosure and notification. This means that the law must contains penalties for failure to notify individuals and/ or the public in cases where such notification was warranted.

Now that the circumstances of notification have been determined, there remains the question of when such notification ought to occur. Different jurisdictions provide different answers to this question. The EU GDPR differentiates the notifications on the basis of the notified entity: the data controller must notify the data protection authority within 72 hours of knowledge of the breach, while individuals or data subjects must be notified “without undue delay”. Other jurisdictions, such as Canada, stipulate that notification must occur “as soon as feasible”, or “without delay”, as South Korea provides. Several factors affect the timeframe of notification: the size of the data controller entity, the time it takes to detect the breach, and the magnitude of the breach. While it is not always possible, in these circumstances, to immediately detect a breach in security, it is submitted that the starting point may be once knowledge of the breach has been acquired. Once the data controller entity has knowledge of the breach, it must notify the authority within 72 hours, and the individuals within a stipulated period of time, such as 15 days. Further, if the magnitude of the breach is such that it involves a large number of data subjects, then a public communication must be made necessary.

Finally, the contents of the notification are crucial. They must be sufficiently detailed so as to acquaint the data subject with the potential consequences of the breach, and suggest possible measures that data subjects may take to insulate themselves against such consequences. Further, the notification must describe the nature of the breach, the estimated number of individuals affected, and list out the measures take by the data controller and/or processor to minimize the harms arising out of the

breach. It must also provide the data subject with a contact within the organization of the data controller to whom they may turn to clarify concerns relating to the breach. The EU GDPR and South Korea's Protection of Personal Information Act, 2011 are instructive in this regard.

CATEGORISATION OF DATA CONTROLLERS

1. What are your views on the manner in which data controllers may be categorised?

2. Should a general classification of data controllers be made for the purposes of certain additional obligations facilitating compliance while mitigating risk?

3. Should data controllers be classified on the basis of the harm that they are likely to cause individuals through their data processing activities?

4. What are the factors on the basis of which such data controllers may be categorised?

5. What range of additional obligations can be considered for such data controllers?

CCG Response (to questions in this chapter): We agree that data controllers should be required to register, and recommend that they are then categorised based on the nature of their operations. For instance where sensitive personal information is processed, data controllers should be required to meet higher standards of accountability.

In addition, a system for publication of risk criteria similar to that provided for under the GDPR may be adopted. Any controller who meets the relevant criteria can then be required to undertake impact assessments.

6. Are there any alternative views other than the ones mentioned above?

CCG *Response*: We do not have any additional comments on this chapter at this stage.

DATA PROTECTION IMPACT ASSESSMENT

1. What are your views on data controllers requiring DPIAs?

2. What are the circumstances when DPIAs should be made mandatory?

3. Who should conduct the DPIA? In which circumstances should a DPIA be done (i) internally by the data controller; (ii) by an external professional qualified to do so; and (iii) by a data protection authority?

4. What are the circumstances in which a DPIA report should be made public?

5. Are there any alternative views on this?

CCG Response: We recommend incorporation of requirements for data protection impact assessments. We do not currently have comments on the specific manner in which these requirements may be imposed. However, we do note that any such measures should be transparent, and put in place after adequate public and stakeholder consultations.

DATA PROTECTION AUDIT

1. What are your views on incorporating a requirement to conduct data protection audits, within a data protection law?

2. Is there a need to make data protection audits mandatory for certain types of data controllers?

3. What aspects may be evaluated in case of such data audits?

4. Should data audits be undertaken internally by the data controller, by a third party (external person/agency), or by a data protection authority?

5. Should independent external auditors be registered / empanelled with a data protection authority to maintain oversight of their independence?

6. What should be the qualifications of such external persons/agencies carrying out data audits?

7. Are there any alternative views on this?

CCG Response: We recommend incorporation of requirements for data protection audits. We do not currently have comments on the specific manner in which these requirements may be imposed. However, we do note that any such measures should be transparent, and put in place after adequate public and stakeholder consultations.

DATA PROTECTION AUTHORITIES

1. What are your views on the above?

2. Is a separate, independent data protection authority required to ensure compliance with data protection laws in India?

3. Is there a possibility of conferring the function and power of enforcement of a data protection law on an existing body such as the Central Information Commission set up under the RTI Act?

4. What should be the composition of a data protection authority, especially given the fact that a data protection law may also extend to public authorities/government? What should be the qualifications of such members?

5. What is the estimated capacity of members and officials of a data protection authority in order to fulfil its functions? What is the methodology of such estimation?

6. How should the members of the authority be appointed? If a selection committee is constituted, who should its members be?

7. Considering that a single, centralised data protection authority may soon be over-burdened by the sheer quantum of requests/ complaints it may receive, should additional state level data protection authorities be set up? What would their jurisdiction be? What should be the constitution of such state level authorities?

8. How can the independence of the members of a data protection authority be ensured?

9. Can the data protection authority retain a proportion of the income from penalties/fines?

10. What should be the functions, duties and powers of a data protection authority?

11. With respect to standard-setting, who will set such standards? Will it be the data protection authority, in consultation with other entities, or should different sets of standards be set by different entities? Specifically, in this regard, what will be the interrelationship between the data protection authority and the government, if any?

12. Are there any alternative views other than the ones mentioned above?

CCG Response (to questions in this section of the chapter):

We have reproduced an excerpt from our submissions to the TRAI Consultation Paper below[201]:

> There has been a significant increase in data driven business, and associated concerns in relation to protection of personal information since the GOE Report was published. With any new data protection regulation, the establishment of regulators (or separate departments / offices within existing regulatory bodies) for implementation of the regulation will become imperative. These regulators will need to monitor data processors and controllers to ensure compliance with the new data protection regulation (and possibly any other law that deals with data protection / privacy in any form). Increasingly, data protection authorities also have administrative and quasi-judicial functions and are being allowed to decide on complaints of non-compliance and impose penalties and fines[202].
>
> The OECD's revised privacy guidelines[203] (OECD Guidelines) also provide for establishment of privacy enforcement authorities. The OECD Guidelines provide that these privacy enforcement authorities are

[201] *Supra* note 7.

[202] *Id*, 2nd and 3rd generation European Standards described in section 4.1.

[203] The OECD Privacy Framework, available at http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf (last visited on February 25, 2018).

(i) Required to have the governance, resources and technical expertise necessary to exercise their powers effectively and to make decisions on an objective, impartial and consistent basis;

(ii) to be to be free from instructions, bias or conflicts of interest when enforcing laws protecting privacy.

The OECD Guidelines also suggest that these privacy enforcement authorities engage in cross-border co-operation with similar authorities in other jurisdictions to ensure global interoperability of data protection regulations[204].

The EU's GDPR also provides for establishment of 'supervisory authorities', i.e. public authorities that oversee the implementation of the GDPR in each member state. The GDPR contains extensive provisions on the establishment, competence, tasks and powers of the supervisory authorities[205]. In certain situations, data processors and controllers are required to appoint data protection officers who, among other things, cooperate with the supervisory authority.

It may be relevant to note that the existence of a supervisory authority with enforcement powers, is one of the elements that is considered in order for a non-EU member state to obtain an adequacy decision in its favour[206]. In this context, it would be useful for the TRAI and / or MEITY to consider the provisions governing the establishment and role of supervisory authorities under the GDPR while drafting the new data protection laws in India.

To add to the above, we refer to the suggestions made in Professor Graham Greenleaf's submissions to the Committee. He notes that the GDPR and other jurisdictions that adopt this approach contain strict requirements in terms of the

[204] *Id*.
[205] Chapter VI, GDPR.
[206] Article 45, GDPR.

independence of the data protection authority[207], and recommends that India consider this approach as well.

9.3. Chapter 3: Adjudication Process

1. What are your views on the above?

2. Should the data protection authority have the power to hear and adjudicate complaints from individuals whose data protection rights have been violated?

3. Where the data protection authority is given the power to adjudicate complaints from individuals, what should be the qualifications and expertise of the adjudicating officer appointed by the data protection authority to hear such matters?

4. Should appeals from a decision of the adjudicating officer lie with an existing appellate forum, such as, the Appellate Tribunal (TDSAT)?

5. If not the Appellate Tribunal, then what should be the constitution of the appellate authority?

6. What are the instances where the appellate authority should be conferred with original jurisdiction? For instance, adjudication of disputes arising between two or more data controllers, or between a data controller and a group of individuals, or between two or more individuals.

7. How can digital mechanisms of adjudication and redressal (e.g. e-filing, video conferencing etc.) be incorporated in the proposed framework?

8. Should the data protection authority be given the power to grant compensation to an individual?

9. Should there be a cap (e.g. up to Rs. 5 crores) on the amount of compensation which may be granted by the data protection authority? What should be this cap?

10. Can an appeal from an order of the data protection authority granting compensation lie with the National Consumer Disputes Redressal Commission?

[207] Article 52, GDPR.

11. Should any claim for compensation lie with the district commissions and/or the state commissions set under the COPRA at any stage?

12. In cases where compensation claimed by an individual exceeds the prescribed cap, should compensation claim lie directly with the National Consumer Disputes Redressal Commission?

13. Should class action suits be permitted?

14. How can judicial capacity be assessed? Would conducting judicial impact assessments be useful in this regard?

15. Are there any alternative views other than the ones mentioned above?

CCG Response (to questions in this chapter): We agree with provisional views 1 to 4 in this chapter, and recommend that the independent data protection authority is given powers to conduct initial investigations into any violation of the data protection law. The data controllers and data protection authority should both be required to maintain records of any issues raised by data subjects, as well as the actions that were taken to address the same. These records should be available for review, if the decision at either stage is appealed. The data protection authority should be empowered to impose penalties, and order compensatory payments by the data controller to the data subject.

Adequate appellate mechanisms will also need to be put in place. We have not specifically looked into the capacity of the TDSAT to act as an appellate authority under this law. However, we note that any appellate authority must be equipped both in terms of technical and legal knowledge, as well as resources and infrastructure to take on such a role. It appears from the White Paper itself that the TDSAT and other consumer dispute resolution fora may not be appropriate from this point of view. It may be best to find to design an independent adjudicatory body, with the requisite expertise, for this purpose.

9.4. Chapter 4: Remedies

PENALTIES

1. What are your views on the above?

2. What are the different types of data protection violations for which a civil penalty may be prescribed?

3. Should the standard adopted by an adjudicating authority while determining liability of a data controller for a data protection breach be strict liability? Should strict liability of a data controller instead be stipulated only where data protection breach occurs while processing sensitive personal data?

4. In view of the above models, how should civil penalties be determined or calculated for a data protection framework?

5. Should civil penalties be linked to a certain percentage of the total worldwide turnover of the defaulting data controller (of the preceding financial year as in EU GDPR) or should it be a fixed upper limit prescribed under law?

6. Should the turnover (referred to in the above question) be the worldwide turnover (of preceding financial year) or the turnover linked to the processing activity pursuant to a data protection breach?

7. Where civil penalties are proposed to be linked to a percentage of the worldwide turnover (of the preceding financial year) of the defaulting data controller, what should be the value of such percentage? Should it be prescribed under the law or should it be determined by the adjudicating authority?

8. Should limit of civil penalty imposed vary for different categories of data controllers (where such data controllers are categorised based on the volume of personal data processed, high turnover due to data processing operations, or use of new technology for processing)?

9. Depending on the civil penalty model proposed to be adopted, what type of factors should be considered by an adjudicating body while determining the quantum of civil penalty to be imposed?

10. Should there be a provision for blocking market access of a defaulting data controller in case of non-payment of penalty? What would be the implications of such a measure?

11. Are there any alternative views on penalties other than the ones mentioned above?

CCG Response (to questions in this section of the chapter): We note that it is important that the data protection law provides for civil penalties in the case of breach of any obligations under the law by the data controllers. If / where any obligations fall directly upon data processors, penalties may be applicable for breach of these obligations by processors as well.

We recommend that guidance may be taken from the GDPR in identifying the nature and amount of penalties applicable in relation to the breach of any obligation under law.

COMPENSATION

1. What is the nature, type and extent of loss or damage suffered by an individual in relation to which she may seek compensation under a data protection legal regime?

CCG Response: We note that one of the problems with enforcement under the IT Act and the IT Rules has been that compensation is only available when there has been 'wrongful loss' or 'wrongful gain' due to negligence in compliance with the law. It is often difficult for data subjects to establish and prove such loss or gain. We note that Professor Greenleaf's comments to the White Paper refer to Korea's Network Act in this regard[208] - under this law, ICSPs may be required by court to pay statutory damages of up to KRW 3 million (around USD 3000) to each affected user for a negligent or wilful violation of a data protection requirement that causes data loss, theft, or leakage without the user having to prove actual damage.

[208]Greenleaf, *supra* note 21.

We recommend that options along these lines may be looked into, in order to ensure that the compensatory mechanisms adopted under the data protection law are accessible to data subjects.

2. What are the factors and guidelines that may be considered while calculating compensation for breach of data protection obligations?

CCG Response: As noted above, one of the difficulties in implementation of the IT Rules has been in relation to the proving the extent of loss or gain in order to obtain compensation. We should avoid limiting our options to such an approach under the new data protection law. As described above, Professor Greenleaf has suggested adoption of the Korean approach – where a fixed amount of damages / compensation is provided for. Other international experiences, as well as experiences from other Indian law may be used to guide this process.

3. What are the mitigating circumstances (in relation to the defaulting party) that may be considered while calculating compensation for breach of data protection obligations?

CCG Response: The implementation of transparency and accountability principles and demonstration of compliance with the data protection law by maintaining adequate records, may be considered when a decision is to be made in this regard. There can be an assessment of whether the defaulting party acted in good faith. However, this must only apply to circumstances in which the harm resulting is limited. In the event that large scale harm results, compensation must be offered regardless of the steps taken by the defaulting party. If necessary, data controllers may be required to subscribe to insurance in order to ensure that such compensation is available to those affected.

4. Should there be an obligation cast upon a data controller to grant compensation on its own to an individual upon detection of significant harm caused to such individual due to data protection breach by such data controller (without the individual taking recourse to the adjudicatory mechanism)? What should constitute significant harm?

CCG Response: In order to ensure that citizens do not have to engage in expensive, time-consuming litigation, data controllers must be incentivised to offer compensation. However, such compensation must be transparent and open to review by the data protection authority. It cannot therefore be subject to non disclosure agreements or promises not to take legal action for additional compensation. In addition, the data protection authority may be empowered to take suo-moto action in situations where there is knowledge of harm caused due to a breach of data protection laws.

5. Are there any alternative views other than the ones mentioned above?

CCG Response: We do not have any additional comments on this chapter at this stage.

OFFENCES

1. What are the types of acts relating to the processing of personal data which may be considered as offences for which criminal liability may be triggered?

2. What are the penalties for unauthorised sharing of personal data to be imposed on the data controller as well as on the recipient of the data?

3. What is the quantum of fines and imprisonment that may be imposed in all cases?

4. Should a higher quantum of fine and imprisonment be prescribed where the data involved is sensitive personal data?

5. Who will investigate such offences?

CCG Response (to questions 1 to 5): We recommend the use of responsive regulation as discussed in our response to questions in chapter 1, Part IV of this paper. Depending on the seriousness of the harm and the scale and quantity of defaults, the legal framework should incorporate the careful use of criminal liability of the individuals responsible.

6. Should a data protection law itself set out all relevant offences in relation to which criminal liability may be imposed on a data controller or should the extant IT Act be amended to reflect this?

CCG Response: We recommend that if a comprehensive data protection law is to be adopted, all related provisions should be included in this law itself. It is not clear why some provisions, such as those suggested in this chapter would need to be included in the IT Act.

7. Are there any alternative views other than the ones mentioned above?

CCG Response: We do not have any additional comments on this chapter at this stage.