University of New South Wales Law Research Series

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

GRAHAM GREENLEAF

[2018] *UNSWLRS* 6

UNSW Law
UNSW Sydney NSW 2052 Australia

E: unswlrs@unsw.edu.au
W: http://www.law.unsw.edu.au/research/faculty-publications
AustLII: http://www.austlii.edu.au/au/journals/UNSWLRS/
SSRN: http://www.ssrn.com/link/UNSW-LEG.html

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

Graham Greenleaf AM FAAL, Professor of Law & Information System, UNSW Australia

31 January 2018 – Comments are welcome to <graham@austlii.edu.au>

Contents

Introduction

Structure of submission

This submission is to the *Committee of Experts on a Data Protection Framework for India* on its *White Paper*,[1] structured around the 'Provisional Views' set out by the Committee in each Chapter of the *White Paper*. In the submission, the Provisional Views are in italics, followed by my submissions on those views in each case. The White Paper makes numerous valuable references to laws outside India, including those of the US, UK, Australia and Canada. It makes few if any mentions of the numerous data privacy laws in other Asian jurisdictions, or the more than twenty years experience (in some cases) in their enforcement. Because Asian data privacy laws is one of my areas of expertise, I have referred briefly to relevant provisions in those laws in my submission, with references to where further details may be found.

Qualifications of submitter

My qualifications to make a submission on India's data protection laws are, in brief, as follows. I have been involved in data protection and privacy issues for over 40 years, as an official (NSW *Privacy Committee Act 1975*), an academic, privacy advocate, and a consultant. As an academic, I have published over 100 articles concerning privacy, and my most recent book, *Asian Data Privacy Laws: Trade and Human Rights Perspectives* (OUP, 2014; paperback 2017), is a study of privacy and data protection in all 28 countries in Asia, including India. I am the Asia-Pacific Editor for *Privacy Laws & Business International Report*, which in 2017 published my 5th Global Survey of Data Privacy Laws and DPAs, covering 120 countries. As a consultant, I have among other engagements written two 'Expert Reports' for the European Commission concerning the level of data protection in India (2009 and 2013), and so I am well aware of existing Indian law concerning data protection and privacy. I am also familiar with social and economic conditions in India, having visited India on at least eight occasions since 1978.

As a privacy advocate, I am a co-founder and member of the Board of the *Australian Privacy Foundation* since 1987, and founder of the *Asian Privacy Scholars Network*. In 2010 I was made a member of the Order of Australia (AM) for my contributions to advancing free access to legal information, and to the protection of privacy, and in 2017 was elected as a Fellow of the Australian Academy of Laws (FAAL). I am a co-founder of the free access online law service, the Australasian Legal Information Institute (AustLII).

I acknowledge the assistance I have received from colleagues from India and Australia in writing this submission, including Amba Kak, Usha Ramanathan, Sean McLaughlan and Elizabeth Coombs. However, all responsibility for views expressed remains with me.

General approach to a data protection law

PART I – CONTEXT-SETTING – 3. Comparative Approaches to Data Protection

The White Paper observes 'that there are two distinct models in the field of data protection' (an EU model, and a US model) (p. 10), and that the 'EU model appears to be the preferred mode in several countries who have adopted data protection legislations recently' (p. 12). This is a considerable understatement and a misunderstanding. Over 120 countries have now enacted data privacy laws that meet or exceed the '1st generation' standard of the 1980s OECD

[1] http://www.meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_171127_final_v2.pdf

Guidelines and Council of Europe Convention 108.[2] Of the 67 of these 120 countries *outside Europe* their average implementation of the ten '2nd Generation' 'European' principles (ie those in the EU Directive of 1995 that go beyond the OECD Guidelines), is at least 6/10 principles. That also applies to those countries outside Europe with the highest GDP, with a privacy law.[3] The reality, therefore, is that the current global standard of data privacy laws *even outside Europe*, is closer to the EU Directive than the OECD Guidelines. The US, with no general data privacy laws, is completely out of step with the rest of the world. There is one global standard – and then there is the US, increasingly isolated.

As the White Paper also observes, in the EU 'the right to privacy is a fundamental right which seeks to protect an individual's dignity' (p. 10). In the USA there is no such fundamental right in relation to privacy as a whole, and particularly not in relation to information privacy. The position in India, as a result of *Puttaswamy*,[4] is in general principle the same as the EU: privacy is a fundamental inalienable right, with the ability of governments to derogate from it requiring considerable justification. Although the details of these contours await definition in post-*Puttaswamy* cases, it would seem that Indian governments will have nothing like the leeway given to US legislatures, governments and business to override privacy interests with few constraints. The US approach of near-complete absence of regulation is not an option for India, and nor is it desirable because more unrestrained innovation will be offset by developments which disregard and damage social welfare and human rights, particularly in relation to the more vulnerable. Such damage caused by the unrestrained development of India's Aadhaar is become notorious outside India.

It seems, therefore, that a realistic approach for the Expert Committee to take toward its task is for it to assume that an India data protection law will have to meet standards approximating those of EU laws if it is to constitute the background environment within which particular legislative interferences with privacy can be justified within the *Puttaswamy* requirements. There are many other reasons why India should adopt a global 'gold standard' data privacy law, but *Puttaswamy* also adds an element of necessity.

Furthermore, India has already signalled its interest in obtaining an 'adequacy' finding for its data protection system from the EU, because it has twice applied for such a finding, but without success. A new data protection law for India, coupled with *Puttaswamy's* implications, will create a completely new opportunity to obtain a positive finding. Although such an assessment would now be made under the EU's new General Data Protection Regulation (GDPR), rather than under the 1995 Directive, the GDPR retains the concept of 'adequacy'. The November 2017 guidelines[5] from the Article 29 Working Party of EU data protection Commissioners (A29WP) indicate that the criteria applied in the assessment of adequacy under the GDPR should be in most respects similar to those applied under the Directive, with notable exceptions being tighter requirements concerning 'onward transfers' of data, and more attention paid to

---

[2] Greenleaf, G 'Global data privacy laws 2017: 120 national data privacy laws now include Indonesia and Turkey' (2017) 145 *Privacy Laws & Business International Report,* 10-13. <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2993035 The total is now at least 125, with the addition of the Cayman Islands, Niger, Mauritania, Guinea (Conarky) and Comoros.

[3] Greenleaf, G 'European data privacy standards in laws outside Europe' (2017) 149 Privacy Laws & Business International Report, 21-23

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

[5] Article 29 Data Protection Working Party *Adequacy Referential (updated*) WP 254, Adopted on 28 November 2017. 'The Working Party of EU Data Protection Authorities1 (the WP29) has previously published a Working Document on transfers of personal data to third countries (WP12). With the replacement of the Directive by the EU General Data Protection Regulation (GDPR)3, WP29 is revisiting WP12, its earlier guidance, to update it in the context of the new legislation and recent case law of the European Court of Justice (CJEU). This working document seeks to update Chapter One of WP12 relating to the central question of adequate level of data protection in a third country, a territory or one or more specified sectors within that third country or in an international organization (hereafter: "third countries or international organizations").'

government access to private sector data (in light of the *Schrems* decision[6]). Without attempting any detailed analysis here of GDPR adequacy requirements, it does seem that it would be valuable for the Committee of Experts to pay careful attention to whether its recommendations are likely to meet those criteria. For that reason, those criteria will be mentioned in this submission where appropriate.

PART V - Key Principles of a Data Protection Law

Although the set of seven general 'key principles' come at the conclusion of the White Paper, it makes sense to address them first before addressing the specific 'Provisional Views'.

> *A data protection framework in India must be based on the following seven principles:*

These principles are useful guides to the aims of legislation, but not suitable for inclusion within legislation.

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

Agreed, but it must have sufficient precision to allow unambiguous enforcement by authorities, and demands for remedies by data subjects.

> *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.*

Agreed, with the emphasis on 'differential' obligations rather than an absence of obligations, and only as far as consistent with India's fundamental inalienable right of privacy.

> *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.*

Agreed, but consent should not be the first resort in deciding how data subjects exercise their informational self-determination. Modern privacy laws rely first on privacy by design and by default (for example, GDPR, art. 25), based on public interest and privacy protection considerations, and only then allow clearly statements of preferences by data subjects to over-ride the legislation's policy preferences. Such statements of preference must be completely 'unbundled', expressed separately from any other choices or provision of information. The *White Paper* is deficient in not sufficiently recognizing the role of privacy by design and default.

> *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.*

Agreed that data minimization is an essential principle. However, personal data should not be collected for 'other compatible purposes', but only for 'other necessarily implied purposes'. If personal data is to be used for merely compatible purposes, the consent of the data subject (not the opinion of the data user) is the best safeguard that such uses are genuinely '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.*

Agreed, but controller vicarious liability (not just a vague notion of 'accountability') is not in itself a sufficient safeguard. Where delegated processing is to take place within India, it should be accompanied by prior notice to the data subject. Where it is proposed that delegated processing will take place outside India, all applicable rules concerning cross-border transfers must apply, as if the data was being transferred to a third party.

---

[6] Case C-362/14, *Maximillian Schrems v Data Protection Commissioner*, 6 October 2015.

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.

Agreed, an independent 'high-powered statutory authority' is essential at the national level, backed up by rights of appeal all the way to the Supreme Court. While 'appropriately decentralised enforcement mechanisms' are fully justified in a country as large and complex as India, an independent 'high-powered statutory authority' will also be fully justified in each State and Territory in India, with the national authority having powers to ensure the consistency of decision-making between State and Territory authorities (somewhat similar to the European Data Protection Board, GDPR, arts. 68-76). Indian States and Territories are very often as populous as countries in Europe, and more so than Australian States or Canadian Provinces, yet each of these polities have separate Data Protection Authorities at both levels. In India, a state-level statutory authority could possibly handle both private sector matters within that State, and public sector matters relating to the State government. The current system of Information Technology Officers at State level, as used by the Information Technology Act, would be manifestly inadequate to deal with the more complex and larger-scale demands of a real data protection Act. Indian governments need to allocate sufficient resources to fund DPAs with 'sufficient capacity' to effectively administer data protection at both national and state levels, so that high quality policy-making can maximize the benefits of both technology and human rights.

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

Agreed, but it is also necessary that provisions for compensation of data subjects when breaches occur are adequate (including being dealt with efficiently), not only to compensate data subjects but also to encourage them to take actions to enforce their rights, because this also acts as a strong deterrent against data breaches. With both enforcement actions and compensation claims, it is essential that the results are publicized, because it is this publicity which has the greatest effect in both deterring breaches, and encouraging claims.

PART II - Scope And Exemptions

Chapter 1: Territorial And Personal Scope - 1.5. Provisional Views

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

2. However, it may be necessary to make the law applicable to all kinds of processing which the State may have a legitimate interest in regulating even though such processing may not be entirely based in India or may be carried out by non-Indian entities that do not have a presence in India.

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

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

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

Similar to what the EU has realised, through the GDPR's extended jurisdictional scope, in order to provide consistent protection to Indian residents it will be necessary for India to assert jurisdiction where goods and services are offered remotely to those in India, or where there is a business with an establishment in India, but not simply because a website is accessible from India. The Provisional Views are consistent with this approach, and justifiably so.

However, no reason has been given for not extending jurisdiction to include processing which involves monitoring activities of persons in India, from outside India (contrast GDPR art. 3(2)(b)). This is a justifiable extension, as it does not involve assertion of global jurisdiction, but limits it to behaviour taking place in India.

In contrast, the suggestion of claiming jurisdiction over all processing of 'personal data of Indian citizens or residents', no matter where it occurs, is not justifiable. Overseas businesses may have no idea that the persons whose data they are processing are Indian citizens, or residents, and so have no reason to expect a need to comply with Indian law. It would also lead to excessive jurisdictional overlaps and conflicts between India and other countries. It is preferable to deal with part of this issue by restrictions on data exports, to help ensure that data on India residents does not go in the first place to countries with sub-standard data privacy laws.

Chapter 2: Other Issues of Scope - 2.4 Provisional Views

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

Agreed that the law should be restricted to natural persons only. It should not apply to deceased persons, and in almost all Asian countries does not so apply. There are few exceptions: Singapore continues to apply security and disclosure requirements (only) for ten years after a person's death,[7] and any such exceptions should be tightly limited in scope and duration. However, there may be a similar case for continuing access and correction rights to a deceased person's records, exercisable by their next-of-kin, for a brief period, unless they have made it clear they do not want this. This is a complex question requiring more investigation, and the best answer may be the one most often chosen, to limit rights to persons while they are alive.

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

Personal data processed by any public or private sector entities, and so *prima facie* data protection laws should apply to all such entities. The 'limited exemptions' which are justifiable in both the public and the private sectors should be required to satisfy the tests set out in *Puttaswamy*. The requirement of proportionality in the design of exemptions means that consideration should always be given to exempting only particular activities of organisations, and only from such of the privacy principles as is necessary. Organisations should not normally be exempt in relation to all their activities; nor should they be exempt from all principles (eg the security principle), as the White Paper recognises (p.31).

South Korean constitutional law requires limitations on rights of privacy to observe the 'principle of less restrictive alternatives', and an equivalent principle could equally be applied to determine the appropriate breadth of exemptions, consistent with *Puttaswamy*'s requirements.

Charitable institutions should not be exempt, because governments everywhere are increasingly relying upon non-governmental organisations to provide services on behalf of

[7] Greenleaf, *Asian Data Privacy Laws*, 2014, p. 481.

government, particularly in such areas as health services or social services for vulnerable people, involving large-scale utilisation of personal information of the primary individual and also of family and carers. Such citizens and their information deserve protection regardless of the business model of the service provider.

Exemptions for 'small' businesses should also be avoided, both because business size bears little relationship to the harm that can be caused to individuals, and also because they can easily result too few businesses having to observe privacy protections. In Australia, perhaps the only country which now has such an exemption, it applies to 94% of all businesses.

One area in which a partial exemption from data privacy legislation does need to be considered is as part of public interest disclosure or "whistle blowing" legislation, so as to ensure reporters of such conduct may be protected from adverse consequences under data privacy legislation should they make a 'whistle-blowing' report qualifying for protection. The Expert Committee should ensure consistency with protected reporting of prohibited conduct for the benefit of the public of India, wherever such legislation exists. Such legislation should cover both public and private sector individuals making qualifying disclosures.[8] This is also relevant to pages 76 and 77 of the White Paper on allied laws.

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

Data privacy laws must apply 'retrospectively' to data collected prior to the date of the Act, because otherwise people's lives may be damaged forever by incorrect, irrelevant or out-of-date information. There is usually a period between enactment and when an Act comes into force (say, a year) which gives businesses and agencies time to 'clean up' their records. This is enough.

Chapter 3: What is personal data? - 3.3. Provisional Views

> *1. It is data about/relating to an individual that may be the subject matter of protection under the law. Data in this context ought to include any kind of information including opinions or assessments irrespective of their accuracy.*
>
> *2. Data from which an individual is identified or identifiable/reasonably identifiable may be considered to be personal data. The identifiability can be direct or indirect.*

These two statements are the correct starting point for a definition of 'personal data', and has been internationally accepted since the 1980s. The question in 2017 is whether this standard definition needs to be extended somewhat, after 40 years, to provide protection against technologies which do not depend on identifiability.

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

Codes of practice will not be sufficient if based on the standard definition, because it is the definition itself which needs to be (cautiously) broadened. The definition needs to also include information which, although it does not make a person identifiable (either by itself or in combination with other information) does enable interactions with the person, or results in consequence affecting them significantly, on the basis of their personal characteristics. This extension could be limited by a further test that the interactions must have a potential effect on the person's interests. For example, a security system which refused entry to a person based on

[8] For example, see an Inquiry by the NSW Parliament, see recommendations 7, 8 and 9 in *Review of the Public Interest Disclosures Act 1994* undertaken by the Committee on the Ombudsman, the Law Enforcement Conduct Commission and the Crime Commission pp 9-10.

a measurement of their skin colour should be considered as processing of personal information, even without the system having any means of identifying the person.

Some of the most important technological challenges relevant to the meaning of 'personal data' result from developments of techniques supposedly resulting in 'anonymisation' or 'de-identification'. Undue faith in and reliance upon disguising information identifying a person, is used to enable such data to be placed in the public domain ('open data'), or made available to private 'big data' processing. This faith is very often misplaced, as illustrated by the Australian example of supposedly de-identified health and pharmaceutical scheme data being released , but later found to be able to identify both health practitioners and individual patients.

Data privacy legislation needs to place due accountability and requirements upon those who release personal information publicly, including releasing such information as Open Data, and to the conditions under which personal data can be regarded as available for further processing (beyond the original purpose of collection) on the basis of 'de-identification'. It is particularly important to assess if there is, or may be, an actual or perceived conflict of interest to house any entity responsible for Open Data in the same organisation as a Data Protection Authority (as discussed further re independence of DPAs (see Pt IV, Chapter 2D).

A precautionary approach is required to establish proper protocols around the release of data to ensure that privacy rights are not diminished. Liability (not just 'accountability') for releasing data that is supposedly de-identified but subsequently shown to be re-identified should be extremely strict (possibly absolute) and not discharged by claims of 'reasonable care'. Protocols must be developed and implemented to ensure data that is released does not diminish the privacy of those individuals connected with that data.

Chapter 4: Sensitive personal data - 4.3 Provisional Views

Higher protections for categories of sensitive data are clearly now a required part of international-standard data privacy laws. The whole purpose of 'sensitive data' categories in data privacy laws world-wide is that data in such categories obtain *additional* protections, whereas all data categorised as (normal) 'personal data' obtains all the standard privacy protections. The only law which does not follow this approach is India's current 'Rules' under the IT Act, where half of the Rules apply only to 'sensitive' data, so that normal personal data obtains no protection at all in relation to disclosure, data exports and possibly collection.[9] The crucial point here is that all normal privacy protections must apply to all personal data, and the categories of 'sensitive data' (whatever they are) should obtain exceptional extra protections. 'Sensitive' data must not be mis-used as an excuse or ruse for reducing normal privacy protections for all personal data, as it is mis-used in the Rules under the IT Act.

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

The proposed categories fall short of those included in GDPR art. 9 by omitting the following: (i) trade union membership; (ii) biometric data; (iii) 'sex life' (in addition to sexual orientation); (iv) political and philosophical beliefs; (v) criminal convictions and offences and related security matters (GDPR art. 10). India needs to give consideration to all of these omitted categories.

Additional protections specific to India and the needs of the people of India. In the Indian context, the proposed addition of 'caste information' is valuable. In India, 'third gender' identity information (concerning persons neither male nor female) should receive explicit protection as

[9] Greenleaf *Asian Data Privacy Laws* (OUP, 2014), pp. 415-16. These Rules apply only to 'sensitive' data: 5(1)-5(4), 6 and 7.

'sensitive personal information', with protections concerning how information of this type ought to be recorded. Indian constitutional law on this issue makes this imperative.

Most data privacy laws in Asia (japan, Korea, Macau, Malaysia, the Philippines and Taiwan) provide additional protections for categories of sensitive information, although the categories vary considerably. The Philippines adds age, marital status and education.

The EU includes biometric data only 'for the purpose of uniquely identifying a natural person'. However, as argued in relation to Chapter 3, there are good reasons to include in the definition of 'personal information' any collection of data which has the potential to affect a person's interests, and for any such collection of biometric data to be regarded as collection of sensitive data.

Another category of personal information which needs to be given special treatment, but with protection at least as strong as for sensitive information, is the national identification number (Aadhaar in the Indian context) and (as the GDPR puts it) 'any other identifier of general application'. The GDPR allows Member States to make special protective rules for the processing of such numbers (GDPR, art. 87). India needs to do likewise for the Aadhaar and other general identifiers.

> 3. *Though qualitatively different from the information in the previous category, financial information may also be included as sensitive personal data. Financial information has been categorised as sensitive information in India since the formulation of SPDI Rules.*

While there can be no objections to other laws giving special protections to certain types of personal financial information (eg bank records, or tax returns), blanket inclusion of such data as sensitive data has no support in international agreements such as the GDPR or the OECD Guidelines, and is not found in any Asian data privacy laws.

Such a blanket exception would appear to provide special treatment for the wealthy, and is likely to be used as a shield for corrupt activities.

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

The recording of a person's trade union membership, or of his or her political view and affiliations, are highly likely to be used for purposes of unjustifiable discrimination, so there are very good reasons why the EU treats them as sensitive information. Information on union membership can and has been used to breach various rights of individuals including rights to privacy, freedom of association and freedom of speech.

Chapter 5: What is Processing? - 5.3 Provisional Views

> *1. The data protection law may not attempt to exhaustively list all operations that constitute processing.*
>
> *2. The definition of processing may be broadly worded to include existing operations while leaving room to incorporate new operations by way of interpretation.*
>
> *3. The definition may list the three main operations of processing i.e. collection, use and disclosure of data. It may be worded such that it covers the operations/activities incidental to these operations.*
>
> *4. The law should cover both automated and manual processing*

Agreed that an open-ended definition of processing that allows judicial recognition of new forms of processing is desirable.

Chapter 6: Entities to be defined in the law: Data Controller and Processor - 6.3 Provisional Views

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

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

The distinction between controllers, processors and third parties remains sound.

Chapter 7: Exemptions for Household purposes, journalistic and literary purposes and research - 7.3 Provisional Views

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

The GDPR's exemption is limited first to processing by natural persons, and second to '*purely* personal or household activity' (art. 2(2)(c)) 'with no connection to a professional or commercial activity' (rec. 18), and those limits should be observed. All Asian jurisdictions include such limitations in their laws.[10] Macau excludes from this exception any processing for 'systematic communication and dissemination', and such a distinction needs to be made been social media communications purely with family or a circle of friends, and those intended to communicate with the world at large.

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

In adopting such a strong exceptions India will be acting consistently not only with the EU, but with the data privacy laws of almost all Asian countries, particularly those that have strong constitutional protections for freedom of speech,[11] as is also found in India.

While such exemptions may need to apply to collection, use, disclosure and retention principles it is nevertheless consistent with such exemptions to require media organisations to adhere to a data privacy law's other principles, such as security and data breach notification principles. The laws of Hong Kong and Malaysia are examples of attempts to place reasonable limits on such journalistic exceptions.[12]

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

Agreed that all of these safeguards are desirable. However, exemptions for the purposes stated should be only to those principles from which exemptions are necessary.

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

This approach is preferable to giving blanket exceptions to any processing by named police and security agencies.

---

[10] Greenleaf, *Asian Data Privacy Laws*, 2014, p. 480.
[11] Greenleaf, *Asian Data Privacy Laws*, 2014, p. 481.
[12] Greenleaf, *Asian Data Privacy Laws*, 2014, p. 481.

> *5. The exemptions must be defined in a manner to ensure that processing of data under the exemptions is done only for the stated purpose. Further, it must be demonstrable that the data was necessary for the stated purpose.*
>
> *6. In order to ensure that the exemptions are reasonable and not granted arbitrarily, an effective review mechanism must be devised.*

These are two very good general safeguards against misuse in specific cases of any exceptions.

Chapter 8: Cross-Border Flow of Data - 8.3 Provisional Views

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

Agreed that the most internationally robust and consistent approach for India to take is one similar to the EU's 'adequacy' approach, in order to best 'ensure a smooth two-way flow of information'. Some version of this approach has been adopted, not only by all EU member states but also by all other European countries (via Council of Europe data protection Convention 108), and also by about 75% of the 66 non-European countries with data privacy laws. Fourteen[13] of the 20 highest GDP countries (in these 66) have some form of export restrictions based at least in part on the extent of protection provided in the recipient country.[14] 'Adequacy' has become the global standard.

Agreed also that India's DPA should have the ability to determine which countries meet such adequacy criteria under Indian law. However, such a decision should be subject to objective tests which can, if necessary, be tested in the courts, as is the case in the EU.[15]

If India intends to seek an EU adequacy assessment, it will need to ensure that its data export rules prevent 'onward transfers' of data imported from EU countries to recipients who cannot guarantee adequate protection according to EU standards (GDPR art. 45(2(a): 'including rules for onward transfer').

> *However, an adequacy framework would require a proactive data protection authority that needs to actively monitor the developments of law and practice around the world.*

Efficient and effective Data Protection Authorities (DPAs) find it necessary to actively monitor the developments of law and practice around the world. The problems of deciding which other countries have 'adequate' laws is often not so much a question of knowledge as one of political sensitivity.

In any event, there are ways of reducing such a problem, because an Indian DPA could also decide to trust the decisions concerning adequacy (or a similar concept) that are made by one or more other international data protection authorities as also constituting 'adequacy' for Indian purposes, provided it is satisfied that the international authority applies standards that are sufficiently rigorous according to Indian law. The obvious candidate for such reliance is the European Union, whose investigation of countries' laws under the Directive is known to be

---

[13] Argentina, Australia, Colombia, India, Israel, Japan, Korea, Malaysia, Peru, Mexico, New Zealand, Singapore, Taiwan, South Africa.

[14] G Greenleaf, " 'European' Data Privacy Standards Implemented in Laws Outside Europe" (2017) 149 Privacy Laws & Business International Report 21-23 < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3096314> .

[15] Case C-362/14, *Maximillian Schrems v Data Protection Commissioner*, 6 October 2015.

rigorous, and will be even more so under the GDPR, but these are not agreements to which India can be a party.

However, the other potential candidate is the Council of Europe's data protection Convention 108 (CoE 108), particularly once its 'modernisation' process is complete. Modernised CoE 108 will require a standard that I have described as 'GDPR Lite' in that it includes the key requirements of the GDPR, but not all its requirements.[16] The 51 parties to CoE 108 include not only all EU states, but also all other European members of the Council of Europe, and a growing list of non-European countries that have acceded to it (4 at present, 5 more invited to accede). I have estimated that CoE 108 has a potential membership of 80 countries out of the 120 countries with data privacy laws.[17] The examination of the effectiveness of the laws of countries acceding to the modernised Convention 108 will be more demanding, and continuous, creating a good basis for reliance.

If India enacts a data privacy law similar to these Provisional Views, then there should be little difficult in India also acceding to Convention 108, obtaining many benefits by doing so,[18] and influencing its future development and its administration (through its Consultative Committee and otherwise). Accession to Convention 108 is also regarded by the EU as a strong element supporting an EU adequacy determination (GDPR, art. 45(2)(c), and r. 105). For an Indian law, or its DPA, to recognise the 'adequacy' of the laws of parties to such a Convention would simply be for it to endorse the quality of an agreement to which it is a party.

Chapter 9 : Data Localisation - 9.5 Provisional Views

> *From these practices it emerges that certain countries have embraced data localisation in some form or manner. However, most countries, do not have a data localisation mandate. India will have to carefully balance the enforcement benefits of data localisation with the costs involved pursuant to such requirement.*

This is a sensible, moderate approach to data localisation, avoiding hysterical rejection of any examples of localisation requirements, but also avoiding unnecessary requirements that copies of every piece of unimportant personal data be kept within India. Strong data export restrictions (as discussed in Chapter 8) can ensure that personal data of Indians does not go to countries, or companies, that do not provide it with adequate protection.

Data localisation is an appropriate response in some situations, and is being required in many countries. India will need to be on guard against free trade agreements (FTAs), such as the Trans-Pacific Partnership (past and proposed versions), which make it prohibitively difficult, and potentially punitive, for countries to adopt data localisation.

> *Different types of data will have to be treated differently, given their significance for enforcement and industry. It appears that a one-size-fits-all model may not be the most appropriate. Thus while data localisation may be considered in certain sensitive sectors, it may not be advisable to prescribe it across the board.*

Agreed that it may be best to leave data localisation requirements to sectoral laws dealing with such categories of personal information, rather than trying to including a generic answer within a data privacy law.

---

[16] G. Greenleaf, Graham, 'Renewing Convention 108: The CoE's 'GDPR Lite' Initiatives' (2016) 142 *Privacy Laws & Business International Report*, 14-17 <https://ssrn.com/abstract=2892947>

[17] G. Greenleaf, 'Data Protection Convention 108 Accession Eligibility: 80 Parties Now Possible' (2017) 148 *Privacy Laws & Business International Report*, 12-16 <https://ssrn.com/abstract=3062415>; There are now at least 125 countries with data privacy laws: see footnote 2.

[18] G. Greenleaf, 'Balancing Globalisation's Benefits and Commitments: Accession to Data Protection Convention 108 by Countries Outside Europe' UNSW Law Research Paper No. 52. (June 23, 2016) <https://ssrn.com/abstract=2801054>

PART III - Grounds of Processing, Obligation on Entities and Individual Rights

Chapter 1: Consent - 1.4 Provisional Views

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

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

In addition to the factors mentioned here, it is very important to require that consents be 'unbundled', or required to be separated from other information with which they should not be combined, including:

(i) separation of consents for each item requiring consent, not one overall consent (GDPR, art. 7(2)); and
(ii) separation of consents from the collection of any other information not necessary for the performance of the contract (GDPR, art. 7(4)).

Korean law has the most strict consent requirements of Asian laws, and achieves both (i) and (ii) above.[19] Other Asian data privacy laws require consent before processing, while some only require notice.[20] Indian lawmakers should consider the Korean provision as well as the GDPR.

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

It is common in data privacy laws for more specific forms of consent to be required for collection of sensitive information. In some instances consent to limited use may also be implied from the circumstances of collection.

Big Data, data analytics, open data, and developments in technology do require current law and/or thinking on consent to be cautiously and rigorously re-thought, but this does not mean that the importance of consent should be lessened or abandoned. The primary reason for re-consideration of 'consent' arises from the fact that so much information about individuals and their activities can be produced by the 'internet of things', derived data, or produced by artifical intelligence. This data can be created, collected and used for purposes to which the individual has little, if any, connection to either the process, the outcome, or knowledge that this is happening. The role of consent can be retained through a number of steps: (i) collection of personal data should not in itself mean it can be used as personal data; (ii) consent (or notice of intended use) can be given ex-post collection, if the data is to be so used; (iii) the law should specifically recognise very limited situations where such use is allowed although consent/notice is impossible.

Individuals are often presented with bundled consent options with only one option, to accept, if they wish to use the consumer item or process in question. This should not be allowed, to ensure that individuals have the maximium ability to control the use of information about them. Korean law has particularly strong requirements for 'un-bundling' consents.

---

[19] Greenleaf, *Asian Data Privacy Laws* (OUP, 2014), pp. 139-144, esp. p143.
[20] Greenleaf, *Asian Data Privacy Laws* (OUP, 2014), p. 487.

Chapter 2: Child's Consent - 2.4 Provisional Views

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

2. One solution to this could be to seek parental authorisation or consent when data controllers process personal data relating to children. This may also be a solution to the conundrum that children do not have the capacity to enter into a valid contract. Many jurisdictions recognise that solely relying on parents' consent would have a chilling effect on the use of the Internet by children. Therefore, these jurisdictions have created an age-limit, below which a parent's consent is necessary, in order to protect very young children from privacy harms. Similarly, a variable age limit can be drawn (not necessarily 18- which is the generally accepted age of majority in India) below which parental consent is to be mandatory. Methods for effectively ensuring parental consent must be considered, either for certain categories of services or through certain processes that may be onerous for the child to circumvent.

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

The White Paper is correct that children's consent should be addressed specifically in the legislation. A combination of the age-based limits in (2) above with the prescription of stronger provisions relating to particular information services more likely to be harmful to children, may give the best combination. Such specific provisions could include the DPA requiring data protection impact assessments (DPIAs), and higher levels of parental consent verification.

Chapter 3: Notice - 3.4 Provisional Views

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

It is necessary for notice to be mandatory both where information is collected from the data subject (GDPR, art. 13), and where information is collected other than from the data subject (GDPR, art. 14).

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

The specificity and scope of such requirements is the key, and also how they mesh with equally specific consent requirements. The GDPR provisions above-cited give the most up-to-date and thorough indication of the categories of information that should be provided. This is particularly so in relation to where information will or may be transferred overseas.

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

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

These steps can be worthwhile, but only if the requirements in the law are sufficiently specific and demanding, so as to ensure that any guidance by a DPA will not be ignored because there are no consequences.

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

Data use policies, by themselves, do not indicate trustworthiness, because they do not measure compliance, or other factors such as the inherent intrusiveness of the data collected. 'Data trust' cannot be measured automatically, cannot be self assessed without fraud, cannot be trusted to private intermediaries (who have a conflict of interest between collecting fees and giving low scores), and are not realistic to impose as a task on a DPA. Such suggestions should be deferred for future

> *6. Similarly, having a _consent dashboard' could help individuals easily view which organisations have been provided with consent to process personal information and how that information has been used.*

The degree of coordination required from data controllers, device providers and others to make such a technological solution feasible are likely to make it an unpromising place to start, and one with potentially discriminatory effect between different classes of data subjects.

Chapter 4: Other Grounds of Processing - 4.4 Provisional Views

> *1. Consent continues to play a very important role in data processing activities. It may not be possible to seek consent of the individual, prior to collection and use of her information in all circumstances, particularly when information is used for various purposes for which they might not have been originally intended. There may be a need to have certain legally recognised grounds to permit processing of personal data in these circumstances.*
>
> *2. Grounds such as performance of contract; and necessity for compliance with law appear to be intuitively necessary, and have been adopted, as is, by jurisdictions.*
>
> *3. Other grounds such as the public interest ground finds mention within the EU GDPR; however lack of specificity as to what it comprises, has led to countries such as the UK to modify it to fit the particular administrative, judicial and legislative requirements of each country. For instance, other grounds of processing could include collection of information in the event that it has been ordered by a court of law; where a public authority needs to collect data necessary to the exercise of the functions of the legislature, such as the drafting of new laws. Adaptations suitable for India will have to be explored.*
>
> *4. There may also be a need of a ground which permits the collection of information in situations of emergency where it may not be possible to seek consent from the affected individual.*

Yes, there are numerous other grounds which make processing justifiable, which will need to be customised to Indian conditions. However, a high level of justification is needed for grounds of processing which go beyond matters analogous to those set out in GDPR art. 6(1)(a), given the consideration that has been given to these grounds on an EU-wide basis.

> *4. The —legitimate interest‖ ground under the EU GDPR appears to be subjective and difficult to enforce. It places a heavy burden on the data controller who must carry out the balancing test weighing its interests against that of the rights of the individual. Despite this, there may be a need to have a residuary ground under which processing activities could take place, as it is not possible for the law to foresee and provide for all situations, which may warrant the processing of information without seeking consent of the individual. This residuary ground would be intended for the benefot of the individual.*

The legitimate interest ground, though it may in some cases require specific adjudication by a DPA and eventually be the courts, will in due course generate a body of decisions which will guide controllers, data subjects and the DPA as to when it may legitimately be relied upon.

> *As an alternative, the data protection authority could designate certain activities as lawful, and provide guidelines for the use of these grounds and the data controller would be permitted to collect information under these grounds.*

In the interim, the DPA could be empowered to issue non-binding guidelines, rather than regulations, until DPA or court decisions clarified the meaning of the legitimate interest ground. Decisions interpreting the ground, not delegated legislation independent of it, are preferable.

Chapter 5: Purpose Specification and Use Limitation - 5.4 Provisional Views

These Provisional Views are not specific enough to be useful, and some are dangerously vague. However, the White Paper's text (pp. 105-9) does give a convincing explanation of the rationale of the purpose specification and use limitation principles, and how they are implemented in the GDPR. This text should guide the formulation of legislation, not the Provisional Views below.

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

'Ensur[ing] that individuals retain control over the manner in which their personal data is collected, used and disclosed', or 'informational self determination' is indeed the underlying objective or end. If this is kept in mind, then the means by which this is achieved make sense.

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

'Minimisation' is the key term in how this objective is achieved. As the White Paper says (pp. 105-6, quoting B. Marr), the 'underlying logic of the use limitation and purpose specification principles is that of data minimisation, or the practice of limiting the collection of personal information to that which is necessary to accomplish a specified purpose.' This has been the core principle of data privacy laws since at least 1980, it has not changed, and it requires thorough implementation.

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 on use. This approach is equivalent to also abandoning not only notice but the very idea of a purpose of 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.

> *3. In light of recent developments in data flow practices and new technologies, data may be multi-functional and being required to specify each use in an exact manner within a privacy notice may prove to be burdensome. Using layered privacy notices, which provide hyperlinks to more information on data use practices, which can be accessed as required, could mitigate this situation. Further, incompatible purposes, irrespective of how beneficial they may be to the user may not be permitted for further processing.*

As the White Paper (p. 106) makes clear, technological developments have not made the principle of purpose specification irrelevant: in fact they have made it even more necessary for the purposes of services to be determined in advance, and if further uses beyond what was originally envisaged are desired, then further consent should be obtained.

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

Although a 'reasonable expectations' test can be used as means of determining what are compatible / incompatible proposed additional uses of data, it is important these do not include 'expectations' that are formed because of what data controllers say they intend to do with data, irrespective of whether data subjects wish such uses to be made. 'Reasonable expectations',

must continue to be subject to what uses are compatible with the original specified purpose of collection of the data.

Chapter 6: Processing of Sensitive Personal Data - 6.4 Provisional Views

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

While this now seems self-evident, the 1980 OECD Guidelines did not recognise any categories of sensitive information requiring special protection, and so many 'first generation' data privacy laws did not give special protections to categories of sensitive data. However, almost all data privacy laws now include special protections for categories of sensitive data, including the majority of data privacy laws in Asia[21] (now including Japan, since its 2015 amendments).

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

The existing categories of sensitive data in the so-called SPDI Rules should be ignored because the make little sense: they are only given the 'normal' level of data protection, whereas 'non-sensitive' data is given lesser protection,[22] so they are not 'sensitive data' provisions at all. The categories of sensitive information needing extra protection in India are discussed more usefully in Pt II Ch 4.

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

'Heightened' protection is the whole point of categorising 'sensitive data', but the White Paper fails to nominate what special protections must be given. 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)).

Indian legislation need to consider the imposition of at least these special protections, if the designation of 'sensitive information' is to have any meaning.

Chapter 7: Storage Limitation and Data Quality - 7.4 Provisional views

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

Requiring limits on the period for which personal data is retained, although not included in the '1st generation' OECD Guidelines, has since become a clearly accepted part of almost all national

[21] Greenleaf, *Asian Data Privacy Laws* (OUP, 2014), pp. 493.
[22] Greenleaf, *Asian Data Privacy Laws* (OUP, 2014), pp. 415-16.

data privacy laws, including all laws in Asia[23] (now including Japan) except in Vietnam and China.

The distinction must be made between (i) automatic deletion or de-identification, and (ii) deletion on request. Both are now recognised as normal rights of data subjects (with conditions). India's law should include both types of storage limitation.

(i) Automatic deletion or de-identification of personal data is required by the GDPR once it is no longer necessary for the data controller to keep it in a form permitting identification, for the purpose for which it is being processed (usually the original purpose for which it was collected) (GDPR, art. 5(1)(e)). Data controllers therefore have an automatic (without request) obligation once the purpose of the processing is complete, but also have the option whether to delete or de-identify the data. Such automatic obligations are required in all Asian data privacy laws (now including Japan), except Vietnam and China.[24] India should adopt what is now a global practice.

(ii) Erasure of personal data on request by the data subject should also occur on the basis of a set of grounds to be specified in the legislation, which would include such matters as where data has been processed unlawfully (GDPR, art. 17(1)(d)); where the data subject withdraws consent to processing that they have previously given (and the controller does not have overriding grounds to retain the data) (GDPR, art. 17(1)(a) and (b)); and where the data is found to be inaccurate and cannot be rectified (GDPR, art. 5(1)(d)). In some cases decisions concerning the balance of interests between the data subject and the data controller will need to be made by the DPA or some other adjudicator, but this is normal result of the provision of rights which cannot be precisely defined for all circumstances, and not a reason for avoiding provision of such rights. Rights to erase personal data on request, or to block its use, are found in most data privacy laws in Asia (South Korea, Macau, Malaysia, Philippines and Hong Kong).[25]

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

All Asian jurisdictions with data privacy laws, except India and China, include the minimum data quality requirement that personal data must be relevant, accurate, complete and up-to-date, relative to its purpose of use.[26] The GDPR includes as part of its 'accuracy' principle 'where necessary, kept up-to-date' (art. 5(1)(d)). These data quality obligations are never regarded as absolute obligations, but are always relative to the purpose of use of the data.

Chapter 8: Individual Participation Rights-1 - 8.4 Provisional Views

> *1. The right to seek confirmation, access and rectify personal data allow an individual control over data once such data has been collected by another entity. These rights may be suitably incorporated. However these rights are harder to enforce in the context of personal information that has been derived from the habits and observed behaviour of the individual and other such inferred insights. This information is nevertheless personal and an individual should be made aware of the fact that the data controller has this sort of information.*
>
> *2. Given that responding to individual participation rights can be costly for organisations, and comes with its set of technical challenges, a reasonable fee may be imposed on individuals when exercising these rights. This will also discourage frivolous and vexatious requests. The fees may be determined via sector specific subsidiary legislation or regulations. An illustration of this is the CIC Act under which the charge for accessing a copy of a person's credit information report by a specified user is laid down by the RBI via regulations.*

[23] Greenleaf, *Asian Data Privacy Laws* (OUP, 2014), pp. 492.
[24] Greenleaf, *Asian Data Privacy Laws* (OUP, 2014), pp. 492.
[25] Greenleaf, *Asian Data Privacy Laws* (OUP, 2014), pp. 492.
[26] Greenleaf, *Asian Data Privacy Laws* (OUP, 2014), pp. 485.

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

These Provisional Views are uncontroversial, but a number of cautions need to be observed.

The very wide disparity of financial resources in India means that great care needs to be taken with setting of any fees before a person can exercise constitutionally protected human rights to view and rectify their own personal information. At least some categories of indigent persons should have automatic waiver of any fees.

Refusal of access to personal information should be avoided in almost all cases, because it is usually possible to arrange for a third party trusted by both data subject and data controller (including the DPA) to access a record on behalf of the data subject in situations where direct access is not appropriate. This should be required. The same should apply to the rectification of records which cannot be accessed directly by the data subject.

Chapter 9: Individual Participation Rights-2 - 9.4 Provisional Views

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

It is important that Indian law implement this right. Data portability is of increasing importance with social networks, and with any other online systems where individuals have invested a considerable amount of time in curating information produced by themselves (UGC, user-generated content), whether that be blog posts, videos, photos or academic articles. The definition of 'personal information' needs to be clear that all information generated by a person is included, so that the right of data portability can apply.

The GDPR extends the right only to where data is provided by consent or pursuant to a contract, but not where it results from carrying out public duties (GDPR, art. 20 and r. 68), limits which make the right workable. The data controller must also inform the data subject of the right of portability (GDPR, art. 13(2)(b)). The Philippines data privacy law already implements data portability, based on an early version of what is now in the GDPR.

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

This is not a very convincing objection. Factors such as public interest, and the balance of legitimate interests, will always require sophisticated decision-making by DPAs and courts, and those in India are just as capable of making such decisions as those elsewhere.

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

As suggested in this Provisional View, this right is now essential. The right to object to decisions based solely on automated processing (including profiling) where this significantly affects a person, although it has existed in the EU Directive since 1995, is now reiterated in the GDPR (art. 22). Since decisions about individuals are increasingly made on the basis of algorithmic decision-making, and using AI-based techniques, this right is of greatly increased importance. Although in the past it has been the 'European' principle implemented least in Asian data

privacy laws (only implemented in part in Macau and in the Philippines),[27] this is unlikely to be the case in future.

The GDPR allows exceptions based on the data subject's explicit consent, processing necessary for contracts, and where legislation provides safeguards for data subjects (art. 22(2)), but with a right to human intervention in all cases (art. 22(3)). Where sensitive categories of personal data are involved, necessity for contracts is not sufficient for exceptions, and higher standards of legislative protections are required (art. 22(4)). In India, where important categories of sensitive information could very easily be made invisible within automated decision-making, it is particularly important that these rights are give a very strong embodiment.

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

The key question in relation to direct marketing is whether the data subject's right should be 'opt-in' (ie no marketing without prior consent) or only 'opt-out' (ie marketing permitted provided an op-out facility is provided). Although opt-out was previously the standard approach (since the 1995 EU Directive), Hong Kong and South Korea have already enacted the tougher opt-in requirements, with severe financial penalties for breaches.[28] The GDPR adheres to the opt-out ('right to object') approach (art. 21). Among Asian countries, only Singapore and the Philippines do not have direct marketing restrictions (although Singapore has a rigorous 'do not call' law). India should consider following the more rigorous opt-in standard set by Hong Kong and South Korea.

Chapter 10: Individual Participation Rights 3- Right to be forgotten - 10.4 Provisional Views

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

In addition, Indonesia's legislature enacted a right to be forgotten in December 2016, as an amendment to its electronic transactions law.[29] It is likely that such a right will become a common component in the post-GDPR '3rd generation' of data privacy laws. As *Puttaswamy* indicates, the Supreme Court may interpret India's constitutional right of privacy to include such a right.

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

Agreed, because the sufficiency of such guidelines can, if necessary, be tested by the Courts against the constitutional right of privacy.

---

[27] Greenleaf, *Asian Data Privacy Laws* (OUP, 2014), p. 494.
[28] Greenleaf, *Asian Data Privacy Laws* (OUP, 2014), p. 493.
[29] G. Greenleaf, 'Indonesia' section in *2014-2017 Update to Asian Data Privacy Laws - Trade and Human Rights Perspectives* UNSW Law Research Paper No. 47, 2017 (July 12, 2017) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3000766>.

PART IV - Regulation And Enforcement

Chapter 1: Enforcement Models - 1.3 Provisional Views

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

Despite its theoretical attractions (including to the AP Shah Committee), co-regulation models have had little successful take-up anywhere in the world. They are of no significance in Asian data privacy laws.[30] Co-regulatory schemes have been tried and discontinued under Australia's *Privacy Act 1988*, which attempted to make them a major aspect of its regulatory approach.[31]

The *White Paper* conspicuously fails to cite a single example of a successful co-regulatory scheme (pp. 144-146; pp. 157-159). The *White Paper* also sets up false dichotomies in attempting to find virtues in co-regulation. 'Flexibility' through industry-specific codes has no inherent relationship to co-regulation, and can be more easily achieved via a DPA's power to issue (and revoke) delegated legislation following industry consultations (see 2A below re industry codes). 'Command and control' regulatory mechanisms (ie a DPA making rules) is not inherently more technologically laggard, nor slow-moving, than some industry-based committee. It just has fewer vested interests.

There is a risk everywhere that 'data security' and other industry bodies would like to get their hands on regulation-making powers concerning privacy. Calls for co-regulation are too often a disguised call for self-regulation, which have a proven history of failure.[32] Despite the White Paper's half-hearted attempt to endorse co-regulation, the rest of Part IV proceeds to then avoid it, indicating that it is a sop to a minority of committee members.

The GDPR includes a very highly-regulated approach to when and how Member States may introduce elements of co-regulation (GDPR arts. 40-41). If India does include any co-regulatory mechanisms – which it need not do in order to obtain an adequacy determination from the EU – then it should ensure that it also includes controls at least as strict as those of the EU. In particular, there needs to be provision for (i) data subject to appeal to the DPA or the courts against any decisions by a co-regulatory body; and for (ii) data subjects to commence actions to have the DPA shout down co-regulatory schemes that are ineffective or insufficient in their remedies. The relevant industry should also bear all the costs of the co-regulatory scheme.

'Command and control vs co-regulation' is not the best, or even a particularly valuable lens through which to view models of privacy regulation. A much more useful model, for privacy regulation, is that of 'responsive regulation', based on well-accepted regulatory theory and consistent with both international privacy agreements and leading privacy scholarship.[33] That model has been applied to a comparison of the regulatory effectiveness of data privacy laws in

---

[30] Greenleaf *Asian Data Privacy Laws*, 2014, p. 524.

[31] G. Greenleaf, Privacy in Australia (March 6, 2008). Chapter in Rule J and Greenleaf G (Eds) *Global Privacy Protection: The First Generation*, Edward Elgar, Cheltenham, 2008 < https://ssrn.com/abstract=3072270 >

[32] R. Gellman R., and P. Dixon 'Failures of Privacy Self-Regulation in the United States'. In: Wright D., De Hert P. (eds) *Enforcing Privacy* (2016) vol 25 *Law, Governance and Technology Series*, Springer; see also R. Gellman R., and P. Dixon 'Many Failures: A Brief History of Privacy Self - Regulation in the United States' World Privacy Forum, 2011 <http://www.worldprivacyforum.org/wp-content/uploads/2011/10/WPFselfregulationhistory.pdf>.

[33] Greenleaf, *Asian Data Privacy Laws* (OUP, 2014), pp. 62-75 (Ch 3.4 'Standards for enforcement mechanisms, and "responsive regulation" ').

Asian countries,[34] resulting in the conclusion that (as of mid-2014) South Korea, Macau and Hong Kong had the most effective methods of regulation (though using quite different tools).[35]

Chapter 2: Accountability and Enforcement Tools - 2.4 Provisional Views

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

This approach, which is desirable, is similar to the GDPR's approach to accountability, requiring that the controller 'shall be responsible for, and be able to demonstrate, compliance with' the other Principles relating to processing of personal data (GDPR art. 5(2)). 'Accountability', used in this sense, is no substitute for any liability that otherwise falls on data controllers, and in fact adds another head of liability.

A. Codes Of Practice - 2.9 Provisional Views

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

While their importance may be over-rated (see Chapter 1 above), provisions for codes of practice such as are in the GDPR are no objectionable (GDPR arts. 40-41).

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

Agreed, and such consultation is standard practice globally. However, it has nothing to do with co-regulation, because the industry bodies neither make the codes nor enforce them.

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

As discussed in Chapter 1 above, it should also cover rights of appeal against code body decisions, provisions for discontinuance, the costs of operating codes, and the other matters covered by the GDPR.

B. Personal Data Breach Notification - 2.12 Provisional Views

Data breach notification is now a standard part of the 3rd generation of data privacy standards, having been included in the GDPR, in the 2013 revised OECD Guidelines, and in various data privacy laws in other Asian countries. Australia's notification requirements, to both individuals and to DPAs, will come into force in early 2018.[36]

1. The law may require that individuals be notified of data breaches where there is a liklelihood that they will suffer privacy harms as a result of data breaches.

The GDPR puts the onus on data controllers to notify individuals affected where the breach 'is likely to result in a high risk' (art. 34). South Korea, the Philippines and Taiwan require notifications to individuals.

2. The law may also require that the data protection authority or any authority be notified immediately on detention of data breaches.

---

[34] Greenleaf, *Asian Data Privacy Laws* (OUP, 2014), pp. 507-527 (Ch 18 'Assessing Data Privacy Enforcement in Asia – Alternative and Evidence').

[35] Greenleaf, *Asian Data Privacy Laws* (OUP, 2014), pp. 525-27.

[36] Information on the Australian scheme is at <https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme and https://www.legislation.gov.au/Details/C2017A00012>

The GDPR puts the onus of notification to DPAs on data controllers 'unless the personal data breach is unlikely to result in a risk' (art. 33). Immediate notification is desirable. The Philippines and South Korea require notifications to the DPA.

> *3. Fixing too short a time period for individual notifications may be too onerous on smaller organisations and entities. This may prove to be counter productive as well as an organisation may not have the necessary information about the breach and its likely consequences.*

If there is immediate notification to the DPA, then the DPA should be able to override the controller's assessment of the likelihood of risk and order the controller to notify individuals (as required by GDPR, art. 58(2)(e)).

The most important aspect of data breach notification provisions is that failure to comply with them must be made a separate breach of the legislation, resulting in administrative penalties and possibly compensation claims (as in the GDPR, and in Australia's new provisions).

C. Categorisation Of Data Controllers - 2.16 Provisional Views

> *1. The effective enforcement of a data protection law may require some form of differentiated obligations so that certain entities covered under the framework whose processing activities create higher degrees of risk or may cause significant harm can be more readily engaged with and guided in ensuring compliance with relevant obligations.*

In order to require data protection impact assessments (DPIAs) by businesses involved in higher risk forms of processing, there is no need to require all businesses to register. There is only a need for a DPA to publish the risk criteria requiring DPIAs, and to put the compliance onus on businesses (with advice from the DPA). That is all the GDPR requires (art. 35).

Australia's so-called 'small business' exemption exempts more than 95% of all Australian business from the operation of the *Privacy Act 1988* (unless they undertake a few higher risk activities), as noted in the *White Paper* (p. 167). It is a poor example to raise or emulate because it removes almost all privacy protections, with the result that it is one of the main reasons why the EU has twice declined Australia's applications for an adequacy finding. India should avoid following this example.

D. Data Protection Authority - 2.20 Provisional Views

> *1. Based on the above, it follows that a separate and independent data protection authority may be set up in India for enforcement of a data protection legal framework.*

One or more independent supervisory authorities (DPAs) are an essential requirement of the GDPR (art. 51), and an essential requirement for a third country like India to be assessed as having an adequate system of protection. The requirements of independence are now more explicitly set out in the GDPR (art. 52), are quite strict, and have already resulted in a number of enforcement actions before the CJEU by the Commission under the Directive. These independence criteria must be taken seriously by India if an adequacy finding is to be achieved. South Korea has already had to modify it adequacy application because its original nominee as DPA did not have sufficient independence or powers.

DPAs should not be established within a body carrying out both data protection and RTI functions. (such as an 'Information Commissioner'). Far from being efficient, such as structure creates an inherent conflict of interest between two often contradictory objectives. A DPA needs to be 'free standing' and to be seen to be so by the citizenry, if it is to be genuinely independent. Similarly, 'open government' and particularly 'open data' responsibilities are not fully compatible with a commissioner or commission responsible for data protection.

> *2. There are three broad categories of functions, powers and duties which may be performed by a data protection authority: monitoring, enforcement and investigation; standard-setting; and awareness generation.*
>
> *3. Specifically, the above functions may include:*
>
> *(i) Monitoring, enforcement and investigation – This may include the power to (a) ensure compliance and enforcement with the provisions of a data protection law; (b) conduct inspection, investigations and collect documents as may be required; (c) adjudicate disputes arising between individuals and data controllers; (d) monitor cross-border transfer of data; (e) monitor security breaches; (f) issue directions to all relevant entities; (g) impose civil penalties for non-compliance; and (h) issue regulations in order to facilitate the enforcement of data protection principles and other ancillary matters relating to data protection.*[805]

While this list is of some use, it only refers to a fragment of the necessary responsibilities and corresponding powers of a DPA. These are most comprehensively set out in the GDPR arts. 57 ('tasks'), 58 ('powers' – investigative, corrective, authorisation and advisory), and 59 (annual report). While additional useful tasks and powers may be found in non-EU national laws (and in the suggestion following concerning reporting of investigation results), the GDPR gives the most comprehensive starting point.

> *(ii) Awareness generation – This may include: (a) the ability to conduct research and promote public awareness of data protection; and (b) the power to educate public and private entities.*

A very important aspect of 'awareness generation' is for a DPA to ensure transparency in relation to its adjudication of disputes, and its awarding of penalties and compensation. This is a vital part of responsive regulation, helping to ensure that all parties/stakeholder, including data subject and their representatives, and data controllers and other regulated parties, and their representatives, all know the principles that the DPA is actually applying when deciding breaches, and the 'tariff' (penalties/compensation) for breaches of the Act. Such transparency can encourage both compliance and the exercise of rights by data subjects. It also means that the DPA cannot hide weak or non-existent enforcement behind obscurity, and thus helps make the DPA accountable. These accountability principles need to apply not only to adjudicated decisions, but also (at least to the extent of statistics), mediated settlements.

Databases of complaint determinations by DPAs are now a standard practice of DPAs, at least in common law countries, as demonstrated by the 25 Case Law databases aggregated in the free access *International Privacy Law Library*.[37] India's legislation should require such transparent reporting by its DPA, consistent with the superb publishing practices of India's RTI tribunal.

> *(iii) Standard setting – This may include the power to: (a) issue codes of conduct/practice; (b) lay down standards for security safeguards; (c) lay down standards for data protection impact assessment; and (d) lay down standards for registration for data controllers as may be required and maintain a database in this regard. Some of these standards relate to data protection issues, e.g., standards for data protection impact assessments; others such as standards for security safeguards are not per se related to data protection. The role of the central government in relation to setting of standards for the latter and such analogous categories and organisational measures should be ensured.*

While the central government does have a role in these matters, care must be taken that this does not infringe the necessary independence of the DPA (as to which, see all six items in GDPR art. 52). In general, it would be better if delegated legislation under the Act was left to the DPA, not to MeitY, so as to reduce political interference. However, it is highly desirable that delegated legislation made by the DPA should be subject to parliamentary disallowance, through the existing mechanisms of Congress committees, so as to maintain democratic oversight over such standard-making.

---

[37] *International Privacy Law Library*, WorldLII < http://www.worldlii.org/int/special/privacy/>.

Chapter 3: Adjudication Process - 3.4 Provisional Views

> *1. Given that under a data protection legal regime, government bodies and public authorities may be considered as data controllers, an adjudicating officer appointed under the IT Act, who is an officer of the government, may not be the appropriate body to adjudicate disputes which involve violation of data protection obligations by such government bodies and public authorities. Therefore, it may be appropriate for a separate, independent body, such as, a data protection authority to adjudicate on disputes arising between an individual and a data controller due to breach of any data protection obligation.*

This is correct – an AO under the IT Act does not have the necessary independence to investigate government. Furthermore, the existing AO-based complaint system under the IT Act has been a complete failure, with an average of only 13 decisions being made per year across the whole of India from 2000-2014, very few available, and none on privacy.[38] This system cannot have any role in a credible Indian data protection system, particularly if EU adequacy is a consideration. For both reasons, 'a separate, independent body, such as, a data protection authority' is needed, as is provided in more than 90% of the 125 countries which now have data privacy laws.[39]

> *2. It follows that an individual whose data protection rights have been violated may, at the outset, first approach the data controller or a specific grievance redressal officer of the data controller identified in this regard.*

Such a requirement is only reasonable in relation to data controllers who have an easily identifiable Data Protection Officer (DPO) or grievance redressal officer. Otherwise, data subjects should have the option to approach the DPA directly.

> *3. Where the data controller fails to resolve the complaint of the individual in a satisfactory and expeditious manner, the individual may be given the right to file a complaint with the data protection authority. Moreover, where the data protection authority observes any violation by a data controller of any of the provisions of a data protection law, it may initiate action against such data controller on a suo motu basis.*

The individual's right to make a complaint should be unrestricted. It should only be terminated by a formal decision by the DPA that the controller has resolved the complaint, to the full extent of the individual's rights. Some DPAs – such as in Australia – have abused their powers to refuse to investigate because they claim the complaint is satisfactorily resolved, although the individual disagrees completely, and the individual then has no right of appeal. Data subjects should always have the right to appeal to a court/tribunal against the actions of a DPA, even when the DPA has not made a formal 'decision'.

Where the DPA takes *suo moto* / own motion action it is essential that the DPA can exercise all of the same remedial actions it can take when it receives a complaint, including administrative penalties.

> *4. The data protection authority may be conferred with the power to appoint an adjudicating officer who may have the requisite qualifications and expertise to inquire into the facts of the complaint and adjudicate accordingly.*

Agreed, but there must be an effective right of appeal to the full DPA, or to a court/tribunal.

> *5. Given that the Appellate Tribunal has already been provided with the mandate to hear appeals from adjudicating officers under the IT Act, it may be worthwhile to propose the Appellate Tribunal as an appellate forum for any decision passed by a data protection authority. This, of course, will be subject to suitable amendments to the TRAI Act along with the constitution of specialised benches having the requisite technical knowledge and expertise as required to achieve this purpose.*

---

[38] Greenleaf Asian Data Privacy Laws (OUP, 2014), pp. 425-6.

[39] G. Greenleaf 'Global Data Privacy Laws 2017: 120 National Data Privacy Laws, Including Indonesia and Turkey' (2017) 145 Privacy Laws & Business International Report, 10-13 <https://ssrn.com/abstract=2993035>; to these 120, now add Niger, Comoros, Guinea (Conarky) and Mauritania.

It appears that the 'Appellate Tribunal' which it is proposed will have this significant privacy appeals jurisdiction is the Telecom Disputes Settlement and Appeals Tribunal (TDSAT). In 2017 it replaced the Cyber-Appellate Tribunal (CyAT), paralysed since 2011, in relation to some appeals under the IT Act.[40] Given that it is to the Indian government's very great discredit that it could leave a whole jurisdiction – the only one able to rule on privacy disputes - inoperative for six years, and the *White Paper* admits (p. 185) that the resources of the TDSAT may not be sufficient for it to take on even the minor functions of the CyAT, what assurance can there be that it will have the credibility and resources to handle appeals from a full-blown data protection Act and DPA.

The Indian government will need to demonstrate that it has given sufficient resources and independence not only to its DPA, but also the body that hears appeals from the DPA. In relation to EU adequacy, the 'right to an effective judicial remedy' against a DPA's decisions (of which appeals to an effective intermediate tribunal is a part) must be considered (GDPR, art. 78).

> *6. In addition to the powers described in the previous section on 'Data Protection Authority' (Part IV, Chapter 2 of the White Paper), the data protection authority may be given the power to impose civil penalties as well as order the defaulting party to pay compensation.*

These are both very important proposals, and both civil penalties and compensation are now part of most modern data privacy laws, exemplified by the GDPR's requirements for civil penalties (art. 83), for criminal penalties (art. 84), and for compensation (art. 82).

> *7. Specifically, in case of compensation claims, the consumer fora set up under the Consumer Protection Act, 1986 (COPRA) typically act as avenues for filing such claims. However, it is relevant to note that given the vast number of data controllers operating in the Indian market and the number of potential data protection violation claims that may be brought by individuals, the consumer fora, especially at the district and state levels, may not have the requisite capacity as well as the technical knowledge and expertise to adjudicate on compensation claims arising from such violations. Moreover, if all compensation claims lie with the consumer fora, it may not incentivise individuals to file complaints with the data protection authority for enforcement and instead file claims relating to compensation with the consumer fora.*
>
> *8. Consequently, it may be proposed that matters in which compensation claims for injury or damage does not exceed a prescribed threshold, may lie with the data protection authority. Further, an appeal from an order of the data protection authority granting such compensation and matters in which compensation claims for injury or damage exceeds such threshold may lie with the National Commission Disputes Redressal Commission (National Commission). This may be undertaken pursuant to requisite amendments to the COPRA and by setting up benches with the requisite technical skills and expertise.*

While it is acknowledged that the National Consumer Disputes Redressal Commission (NCDRC) has done very good work,[41] it will not help India to develop good data protection policies, and consistent remedies, if initial investigation of some complaints is done by the DPA, and others by the NCDRC. There is no reason why the DPA itself cannot award compensation, and although only a minority of DPAs in the Asia-Pacific have this power, it does occurs under Australia's *Privacy Act 1988*, and in the Philippines Other alternatives involve the complaint being first heard in all cases by the DPA, and only after that the award of compensation being heard by a Human Rights Review Tribunal (New Zealand), a mediation body (South Korea) or by a court (Singapore; Hong Kong).[42] All civil law jurisdictions in Asia with data privacy laws (excepting

---

[40] The Cyber-Appellate Tribunal (CyAT) has been paralysed for six years, having made its last decision on June 30 2011 <http://cyatindia.gov.in/Judgement.aspx>, when its previous Chairman's term expired <http://cyatindia.gov.in/History.aspx>. All cases since then (67 of them) are listed as 'pending' <http://cyatindia.gov.in/Judgement.aspx>.The CyAT cannot hear a dispute unless the Chairman is part of the bench (IT Act 2000 (India), s. 49). No replacement Chairman has been appointed. With no CyAT decisions, there can be no appeals to the courts. This scandal has been notorious for many years and played a role in India's previous failed attempts to obtain a positive EU adequacy finding: Greenleaf, *Asian Data Privacy Laws* (OUP, 2014), p. 426.

[41] Greenleaf *Asian Data Privacy Laws* (OUP, 2014), pp. 429-30.

[42] For a summary, see Greenleaf *Asian Data Privacy Laws* (OUP, 2014), pp. 514-15.

Japan) allow individuals the alternative to go directly to the courts to seek compensation, but not in common law jurisdictions.[43]

The best result in India may be for the DPA be able to award compensation as well as other remedies, with a right of appeal to a court or tribunal.

Chapter 4: Remedies

A. Penalties - 4.3 Provisional Views

1. Based on a review of the extant Indian legal and regulatory framework as well as the international best practices set out above, the following models for calculation of civil penalties may be possible:

(i) Per day basis – A data protection law may stipulate that for a violation of a data protection obligation, a civil penalty of a specific amount may be imposed on the data controller for each day such violation continues, which may or may not be subject to an upper limit.860 An upper limit may be a fixed amount or may be linked to a variable parameter, such as, a percentage of the annual turnover of the defaulting data controller.

(ii) Discretion of adjudicating body subject to a fixed upper limit – A data protection law may stipulate that for a violation of a data protection obligation, an adjudicating authority may decide the quantum of civil penalty leviable subject always to a fixed upper limit as prescribed under applicable law. This model of penalty determination is common to the Indian context861 and appears to be so from an international perspective as well.

(iii) Discretion of adjudicating body subject to an upper limit linked to a variable parameter – A data protection law may stipulate that for a violation of a data protection obligation, an adjudicating authority may decide the quantum of civil penalty leviable subject always to an upper limit which is linked to a variable parameter. There are instances in Indian law where such a standard has been adopted.862 In the context of a data protection law, the EU GDPR adopts a similar standard and sets the upper limit of a civil penalty that may be imposed on a defaulting data controller as a percentage of the total worldwide turnover of the preceding financial year of the defaulting data controller.

Option (iii) is preferable, not only because of its consistency with the GDPR's approach (art. 83), but also because attempts to specify daily penalties or maximum penalties cannot effectively take into account the scope and seriousness of the breach or the financial resources of the data controller (which may be larger than most national governments).

2. In relation to the penalty models set out above, it may be relevant to note that while civil penalty leviable on a daily basis (i.e., model (i)) may act as a deterrent, it may lead to an overly adverse impact on small data controllers/ start-up entities who are in the process of setting up businesses or may be in their teething period. In such a case, a per day civil penalty may not be feasible and the quantum of penalty that may be imposed may be left to the discretion of an adjudicating body subject to an upper limit, where such an upper limit may be a fixed amount or may be linked to a variable parameter, such as, a percentage of the annual turnover of the defaulting data controller

Agreed, such arbitrariness can be punitive on small data controllers.

3. Where models (ii) or (iii) are proposed to be adopted, it may leave sufficient room for discretion on the part of the adjudicating authority. Consequently, it may be necessary to set out the factors that an adjudicating authority may consider while determining the appropriate quantum of civil penalty that may be imposed. This may include, nature and extent of violation of the data protection obligation, nature of personal information involved, number of individuals affected, whether infringement was intentional or negligent, measures taken by data controller to mitigate the damage suffered and previous track record of the data controller in this regard.

That is desirable, and a good list of such factors is in GDPR art. 83(2)-(5).

4. To ensure that civil penalty imposed constitutes adequate deterrence, any of the above models or a combination thereof may be adopted. An upper limit of civil penalty which may be linked to the total worldwide turnover of the defaulting party, as is the case under the EU GDPR, brings within its ambit those data

[43] Greenleaf *Asian Data Privacy Laws* (OUP, 2014), pp. 518-19.

> *controllers which handle large volumes of personal data, or who have a high turnover due to their data processing operations, or whose operations involve the use of new technology for processing and therefore may have a higher likelihood of causing harms to individuals.*

This is the best approach, and as well as being adopted by the GDPR, it is also already in force in South Korea. Internet Content Service Providers (ICSPs) may be required by the Korean Communications Commission (KCC) to pay administrative fines of up to 3% of the ICSP's annual turnover related to the infringement, under its Network Act. The first application of these major penalties was in relation to the 'Interpark data leak'[44] which resulted in KCC imposing an administrative fine of 4.5 billion won (around US$4.25 million) on one of the largest Korean online shopping malls. The fine was imposed for negligent failure to protect customer data, and was 60 times higher than previous fines. Similar fines of up to 3% of annual turnover can also be imposed under the Credit Information Act.[45]

> *5. Consequently, the highest form of deterrence in relation to civil penalties may be where a per day civil penalty is imposed subject to a fixed upper limit or a percentage of the total worldwide turnover of the defaulting data controller of the previous financial year, whichever is higher.*

The second option is preferable, for reasons stated.

Although not on the same scale as the Korean penalties, Singapore's law also allows its DPA to impose administrative penalties up to SGD100,000.

B. Compensation - 4.7 Provisional Views

> *1. An individual may be given the right to seek compensation from a data controller in case she has suffered any loss or damage due to a violation of the data controller's obligations under a data protection legal framework.*
>
> *2. A claim for compensation may be filed in accordance with the provisions set out in the previous chapter on 'Adjudication Process' (Part IV, Chapter 3 of the White Paper).*
>
> *3. It may be considered whether an obligation should be cast upon a data controller to grant compensation on its own to an individual upon detection of significant harm caused to such individual due to violation of data protection rules by such data controller (without the individual taking recourse to the adjudicatory mechanism).*

An innovative approach to damages has been taken in Korea's Network Act which has provided since 2014 that ICSPs may be required by a court to pay statutory damages of up to KRW 3 million (around US$3,000) 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 resulting from such violation. Similar amendments have been made to the Credit Information Act and the Personal Information Protection Act.[46] So in the case of large scale data breaches, it may be pointless for data controllers to contest claims, and less expensive for them to simply pay the statutory damages to each affective data subject.

C. Offences 4.11 Provisional Views

> *1. The law may treat certain actions of a data controller as an offence and impose criminal liability. This may include instances where any person recklessly obtains or discloses, sells, offers to sell or transfers personal data to a third party without adhering to relevant principles of the data protection law, particularly without the consent of the data subject.*
>
> *2. The quantum of penalty and term of imprisonment prescribed may be enhanced as compared to the provisions of the IT Act.*

---

[44] Whon-il Park 'Interpark data leak' (KoreanLII, 2017) < http://koreanlii.or.kr/w/index.php/Interpark_data_leak>.

[45] G. Greenleaf, *2014-2017 Update to Asian Data Privacy Laws - Trade and Human Rights Perspectives* (July 12, 2017) UNSW Law Research Paper No. 47, 2017 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3000766>, section 'Korea' and further references cited therein.

[46] ibid

3. A more stringent penalty may be prescribed where the data involved is sensitive personal data.

4. The power to investigate such an offence may lie with a police officer not below the rank of Inspector.

Australia's law allows a maximum court-imposed fine of up to US$1,590,000 (un-used since 2012). Asian laws have as yet generally relatively low criminal fine levels, with the maximum levels being around US$100,000 (South Korea, Malaysia, Macau), and derisorily low fines in other jurisdictions (Hong Kong, Japan).[47]

Conclusions: A leadership opportunity

The parameters set out by *Puttaswamy*, within which interferences with the inherent right of privacy may only be allowed, gives India an opportunity to craft a Data Protection Act which can be a global leader (along with the EU and other technologically advanced countries such as South Korea) in the development of a new third generation of data privacy laws. Such laws can embrace and encourage innovation while protecting fundamental human rights.

In addition to embracing rather than resisting advanced principles of data privacy protection, the necessary ingredient for success in such as approach is the commitment of resources, particularly for the creation of the necessary data protection authorities, and appeals bodies, to make data protection work efficiently in a country as populous and complex as India.

It will also be necessary for there to a belated acceptance that the operation of the Aadhaar system must be brought within the limits of Indian constitution so as to work for the benefit of all its citizens.

[47] Greenleaf *Asian Data Privacy Laws* (OUP, 2014), pp. 516-18.