University of New South Wales Law Research Series

GDPR-LITE AND REQUIRING STRENGTHENING – SUBMISSION ON THE DRAFT PERSONAL DATA PROTECTION BILL TO THE MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY (INDIA)

GRAHAM GREENLEAF

[2018] *UNSWLRS* 83

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

GDPR-Lite and requiring strengthening – Submission on the draft *Personal Data Protection Bill* to the Ministry of Electronics and Information Technology (India)

Graham Greenleaf AM, Professor of Law & Information Technology, UNSW Australia
20 September 2018*

This submission concerns the draft Personal Data Protection Bill which accompanies the Report of the Committee of Experts on Data Protection ('Srikrishna Report').[1] It follows my previous Submission to the Srikrishna Committee on its White Paper on data protection, which the Committee cited various times ('Greenleaf White Paper Submission').[2]

I wish to make a brief submission, but more details of my views are contained in the appended draft article 'India's 'Fourth Way': GDPR-Lite with Chinese characteristics?'. My submissions include general comments first, followed by specific suggestions for improvements to the Bill. For brevity and clarity, they are numbered.

General comments

1 The draft Bill is a serious and modern draft law, and should only be strengthened, not weakened by MeitY in preparing a Bill for submission to the legislature. The Indian government has compelling reasons to enact a Bill resembling this draft, both to protect legislation and practices on which government programs depend against unconstitutionality, and in order to maximize India's prospects of obtaining a positive 'adequacy assessment' from the European Union under the GDPR. This Bill gives India reasonable prospects of achieving both objectives by making only modest improvements to the draft Bill. The Srikrishna Report also provides cogent arguments from a policy perspective why such a Bill is in the interests of the Indian people and Indian businesses and government.

2 The Report and Bill both reflect a very different regulatory philosophy from the EU GDPR's radical dispersal of decision-making responsibility (and liability for wrong decisions) to data controllers. The Indian model is more prescriptive (perhaps closer to the 1995 EU Directive in this respect), and in many ways achieves this by effectively leaving delegated legislative responsibility to the DPIA (or in some cases the government). This is a justifiable choice of a different regulatory model, but in my view it goes too far in the direction of leaving discretion to decide key matters in the hands of the government or the Data Protection Authority of India (DPAI), rather than dealing with them in the Bill.

3 I do not criticise specific data localisation requirements, where justified as in the national interest and defined in legislation (Greenleaf White Paper Submission, p.

* This submission has benefited from valuable comments by Amba Kak, Mozilla Fellow, but all content remains the responsibility of the author.

[1] Available on MeitY website URL: http://meity.gov.in/data-protection-framework.

[2] Greenleaf, Graham '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' (January 31, 2018). UNSW Law Research Paper No. 18- 6. <https://ssrn.com/abstract=3102810>

[1] Available on MeitY w ebsite URL: http://meity.gov.in/data-protection-framework.
[2] Greenleaf, Graham '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' (January 31, 2018). UNSW Law Research Paper No. 18, 6. < https://ssrn.com/abstract=3102810>

[3] Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, *A Free and Fair Digital Economy Protecting Privacy,*

13). However, this Bill adopts an unjustifiable generic approach to data localisation, through blanket local copy requirements (with exceptions to be specified by government), and export prohibitions also specified by government. Leaving such crucial matters to delegated legislation may cause unnecessary problems: justifiable complaints of authoritarian regulation from companies affected; problems with free trade agreements; and questions raised in adequacy assessments. A more conservative and legally constrained approach is desirable.

4 The very broad exemptions from most of the Act for processing in the interests of State security or relating to crimes (or 'any other contraventions of the law', which will include non-criminal matters) in ss. 42-43, although purportedly constrained by legality, necessity and proportionality (legitimate interests apparently being assumed) are dangerously vague, and also very likely to cause great difficulties in any EU adequacy assessment, in light of the CJEU's *Schrems* decision. As the Bill stands, security and law enforcement interests are in effect given carte blanche to invade privacy, with no procedural safeguards to ensure that the above constitutional constraints are observed. In effect, the onus is on data principals to prove that constitutional constraints have not been observed.

5 The lack of complete independence of the DPIA, and the lack of any legislatively guaranteed independence by the Adjudicating Officers, represent unsound policy in relation to bodies whose function is to regulate government as well as the private sector, are very likely to cause major problems with an EU adequacy assessment, and are easily avoided.

Specific suggestions

I wish to submit that, in addition to the above, the following key aspects of the Bill need to be strengthened. The attached draft article raises queries about some other aspects of the Bill.

1 Requirements for 'fair and reasonable processing' should be expressed as 'shall', for certainty, and consistency of terminology (s. 4).

2 The DPAI can specify a broad range of 'reasonable purposes' as grounds for processing of (non-sensitive) personal data, other than consent (s. 17), within factors it must consider, but with no real limits on subject matter. More specific definition, in the legislation, is preferable. In comparison, the GDPR specifies grounds for processing other than consent which are specific in the objectives that are to be achieved (GDPR, art. 6). Some similar balancing tests that the DPAI must undertake, involving balancing of legitimate interests, and reasonable purposes of fiduciaries, should be included in the Bill.

3 The grounds for processing sensitive data (ss. 18-21) generally require more 'explicit consent' (defined), or other 'explicit' or 'strictly necessary' (as opposed to 'necessary') conditions. The intended differences should be better defined.

4 Whether there is to be data breach notification to data principals is at discretion of DPAI. The Bill should state objective criteria as to when DPAI must require notification to the data principals directly (s. 32(5)).

5 The role of Data Protection Officer (DPO) should be stated to require independence from the data fiduciary, and guarantee protection of DPOs from reprisals (s. 36).

6 Access rights are limited to access to a 'brief summary' of personal data, and of processing activities (s. 24). They should instead guarantee access to 'a copy' of both, otherwise this provision is open to abuse.

7 The Government power to exempt specified processing of personal data of foreign nationals not present in India (the 'outsourcing exemption') (s. 104) is undesirable if India wishes to be seen as a global leader in the ethical processing of personal data.

8 The Data Protection Authority of India (DPAI) is described as an 'independent regulatory body' by the Srikrishna Report, but in fact it is not fully independent (though with many indicia of independence). The Government can issue directions to it, as it thinks fit, to protect a wide range of state interests; it is bound by any written directions from the government 'on questions of policy'; and such directions are (purportedly) not subject to judicial review (s. 98). All of these provisions should be deleted, and the DPAI should have the full independence of almost all other DPAs across the globe.

9 The separate 'adjudication wing' of the DPAI which has the crucial roles of deciding penalties and compensation (s. 68(1)) must have unimpeachable independence. The appointment of Adjudicating Officers (AOs) and the manner of adjudication should not be controlled by government regulations (s. 68(2)) but should be controlled by the independent DPAI, and the independence of AOs should be guaranteed.

10 'Anonymisation' is defined as a process 'meeting the standards specified by the Authority', whereas it should be stated as an objective test of an irreversible process preventing identification (in light of current knowledge) (s. 3(3)). The standard that the DPAI sets will not be able to be challenged by expert evidence.

11 Re-identification of de-identified data (which would including purportedly anonymised data which is in fact not anonymised) is made an offence (s.52). This offence at least requires a defence for bona fide security research, otherwise it becomes a 'shoot the messenger' approach.

12 Privacy by default should be specifically included in privacy by design, because although it can be implied by some provisions of s. 29, it does not state that the most privacy-protective legal option should be presented to users as the default. It is desirable that users should not have to opt-in to obtain maximum protection of privacy, but instead should have to opt-out to surrender their privacy.

13 The right not to be subjected to automated processing, at least without human intervention, should be included in the Bill. This is very unlikely to be dealt with by enforcement of privacy by design as the Srikrishna Report suggests. It requires a specific legislative provision because of its high importance, since future processing is well known to be increasingly dominated by algorithms, 'big data' and AI .

14 Rights to object to or block processing should be included in the Bill. The Srikrishna Report suggestion that this can be achieved by data principals seeking interim orders from the DPAI based on correction rights is unrealistic, because applications to block processing (temporarily or permanently) are not necessarily based on correctible errors.

15 The Srikrishna Report argued that no direct marketing opt-out is needed because the Bill's strict approach to consent in effect requires an opt-in to direct marketing. For certainty, this also require a specific provision that marketing is not a secondary use anticipated by principals.

Rectification of these deficiencies in the Bill will strengthen it a great deal, and will give it more of a justified claim to chart a 'Fourth Way' deserving of emulation in the Global South. However, as noted in the conclusion to the attached article, such emulation might be valuable in countries with democracy, constitutional protections and rule of law as strong as in India, but dangerous in more autocratic countries in the Global South.

India's 'Fourth Way': GDPR-Lite with Chinese characteristics?

Graham Greenleaf, Professor of Law & Information Systems, UNSW Faculty of Law[2]
An abbreviated version will be in (2018) 155 *Privacy Laws & Business International Report*.
DRAFT article only – please note as draft if citing.

Indian promises of a serious data protection law have come and gone for decades, but are finally likely to be realized. The Report[3] of the ten member Committee of Experts under the Chairmanship of Justice B. N. Srikrishna ('Srikrishna Report') in July 2018, accompanied by a draft *Personal Data Protection Bill 2018* ('draft Bill')[4] is a serious and modern draft law, and the Modi government has compelling political reasons to enact such a law. The Indian Government has called for submissions on the draft Bill by 30 September 2018, following which it will produce a Bill for introduction to Parliament.

This article first outlines the context in which such a Bill has come about, and some of the constraints shaping its content. There follows a brief comparison of main features of the draft Bill with those of the EU's General Data Protection Regulation (GDPR), a matter of particular interest because of India's two previous failed attempts to obtain a positive adequacy assessment from the EU, but also because of the significant implications that such a GDPR-like law will have for all businesses in, and involved with, India and for the people of India.

The Srikrishna Report's context: *Puttaswamy* and Aadhaar

As part of its ultimately unsuccessful attempt to convince the Supreme Court of India that it should not find that the Indian Constitution includes a fundamental constitutional right of privacy, the Modi government appointed the Srikrishna Committee to draft a data protection Bill. This tactic did not persuade the Court that a constitutional right was unnecessary. A unanimous nine judge Constitution bench of India's Supreme Court held in *Puttaswamy v Union of India*[5] on 24 August 2017 that India's Constitution recognises an inalienable and inherent right of privacy as a fundamental constitutional right.[6] This is the context for all subsequent privacy developments in India.

Puttaswamy's impact

The *Puttaswamy* decision will affect private sector practices ('horizontal effect') as well as actions by the Indian state ('vertical effect'). The Court identified three main aspects of privacy: privacy of the body; privacy of information; and privacy of choice. Subsequent to *Puttaswamy*, smaller constitution benches have already started to decide the constitutionality of various pieces of legislation, and practices, in light of the fundamental right of privacy. These include the constitutionality of India's ID system (the Aadhaar), the criminalisation of homosexual conduct, and prohibitions on consumption of certain foods, and will probably include many more issues. It is very likely that, in order to protect the constitutionality of

[3] Committee of Experts under the Chairmanship of Justice B.N. Srikrishna *A Free and Fair Digital Economy Protecting Privacy, Empowering Indians* < http://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf >

[4] Personal Data Protection Bill 2018 <http://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf>

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

[6] It is an implied right, because although privacy is not explicitly mentioned in the Constitution, it is implied by Article 21's protections of life and liberty, and is also protected by other fundamental rights in provisions providing procedural guarantees. Privacy protection is also required by India's ratification of the UN's *International Covenant on Civil and Political Rights* (ICCPR), article 17 of which protects privacy.

other legislation and practices, the Indian government will now have to legislate comprehensively to protect privacy in relation to both the public and private sectors in India.[7]

The Srikrishna Report' makes it clear that an Indian data protection law must satisfy the requirements of *Puttaswamy* to make the constitutional right meaningful: 'it is the duty of the state to put in place a data protection framework which, while protecting citizens from dangers to informational privacy originating from state and non-state actors, serves the common good'.[8] According to the Srikrishna Committee, the 'core of informational privacy … is a right to autonomy and self-determination in respect of one's personal data. Undoubtedly, this must be the primary value that any data protection framework serves.'[9]

Puttaswamy's impact on the Aadhaar

The lead judgment in *Puttaswamy*, as interpreted by the Srikrishna Report,[10] also held that governments could only interfere with the fundamental right of privacy if they observed three conditions: 'first, there is a legitimate state interest in restricting the right; second, that the restriction is necessary and proportionate to achieve the interest; third that the restriction is by law.'[11] One immediate implication of this is that the government's 'Aadhaar' biometric ID system, since it is clearly a *prima facie* interference with privacy, must observe these conditions of legitimacy, legal authority and proportionality, both in its administration and in the legislation implementing it.

The five judge constitution bench in the Supreme Court case challenging the constitutionality of the Aadhaar ID system, and the *Aadhaar Act 2016* (Puttaswamy again the lead petitioner) reserved its decision in May 2018, after a 40 day hearing (second longest in Indian history). Justice Chandrachud is the only member of this five-judge bench and also of the nine-judge bench which had ruled on right to privacy.'[12] The Court's decision must be delivered by 2 October, on which date Chief Justice Mishra, who is part of the bench on this case, will retire. It is possible that a strong general data protection law, as well as specific improvements to the Aadhaar legislation, will be required by the Supreme Court as conditions for the constitutionally valid operation of the Aadhaar system. The Srikrishna Report recommends fourteen pages of amendments[13] to the *Aadhaar Act* to increase its consistency with the draft Bill (and improve its prospects of constitutionality).

The Srikrishna draft Bill compared with the GDPR

In a short article it is challenging to convey comparisons between two such complex pieces of legislation as the draft Bill and GDPR, each of approximately 100 clauses. In the following point form analysis of the draft Bill, items marked '[√GDPR]' reflect new elements also found in similar form in the EU GDPR (or its predecessor, the 1995 Directive), and items marked '[?GDPR]' reflect issues which differ from the GDPR and would require consideration if India

---

[7] See G. Greenleaf 'Constitution Bench' to decide India's data privacy future' (2017) 148 *Privacy Laws & Business International Report*, 28-31, for details of the committee established to draw up such a law, and background to the Court's decision.

[8] Srikrishna Report, p. 5.

[9] Srikrishna Report, p. 10

[10] For discussion of the various judgments see Malavika Raghavan 'The Right to Privacy Judgment: Initial Reflections on Implications for Digital Financial Services' Dvara Research 25 August 2017 < https://www.dvara.com/blog/2017/08/25/the-right-to-privacy-judgment-initial-reflections-on-implications-for-digital-financial-services/>

[11] ibid

[12] Dhananjay Mahapatra 'Supreme Court reserves verdict on Aadhaar validity' Times of India, 11 May 2018 https://timesofindia.indiatimes.com/india/supreme-court-reserves-verdict-on-aadhaar-validity/articleshow/64116972.cms

[13] Srikrishna Report – Appendix 'Suggested amendments to the Aadhaar (Targeted Delivery of Financial and 'Other Subsidies, Benefits and Services) Act, 2016'

applied for an adequacy assessment from the EU. There is no space here to justify these assessments.

An innovation in terminology is that the Bill refers to individuals as 'data principals' (s. 3(14)), not 'data subjects', and to what are elsewhere called 'data controllers' as 'data fiduciaries' (s. 3(13)), so as to better reflect the obligations and rights of the parties. However, it is questionable whether a mere nomenclature change, with nothing more, would be sufficient to create the existence of a duty of care on data fiduciaries, as the Srikrishna Report asserts.[14]

Scope and limitations

The following factors determine the scope of the Bill:

- General coverage of both **private and public sectors** (currently only private sector). [√GDPR]
- Broad **exemptions** for processing authorised by, and in accordance with, law, for state security, law enforcement and legal proceedings, and (probably) more narrowly for research, archiving or statistical purposes (ss. 42-45). Both 'personal or domestic purposes' (s. 46) and 'journalistic activities' (s. 47) have appropriate exemptions.
- 'Personal data' (defined s. 3(29)) is based on **identifiability**, direct or indirect. [√GDPR]
- Anonymous data is not personal data, but '**anonymisation**' (defined in s. 3(3)) is a process 'meeting the standards specified by the Authority', rather than an objective test of an irreversible process preventing identification (in light of current knowledge). [?GDPR]
- Broad definition of '**processing**' of personal data (s. 3(32)) central to the Bill. [√GDPR]
- Many forms of **sensitive data**, similar to EU, sometimes broader (eg 'financial data') but not including criminal records (s. 3(35)). DPA can specify additional categories (s. 22). **Biometric and genetic data** are included as sensitive data (s. 3(35)). [√GDPR]
- '**Overriding effect**': The PDP law will prevail over other inconsistent existing laws or regulations (s. 110). [√GDPR]

Grounds for processing personal data

All processing of personal data must be justified, on these criteria:

- Requirements for 'fair and reasonable processing' would be better expressed as 'shall', for consistency of terminology (s. 4). [?GDPR] Fairness is based on **purpose limitations** (s. 5(1))
- **Secondary processing** ('incidental purpose') limited to purposes that data principal would 'reasonably expect', given original specific purpose and context (s. 5(2)).
- Collection is limited to what is 'necessary ' for purpose (s. 6), and deletion of personal data where no longer necessary (s.10) ('**data minimisation'**). [√GDPR]

[14] Srikrishna Report, pp. 7-10: 'the hallmark of a fiduciary relationship', 'notwithstanding any contractual relationship'.

- Grounds of **lawful processing** are specified, differing for sensitive personal data (Ch IV) and other personal data (Ch III) (s. 7). As in the EU, all processing must be demonstrably lawful, rather than assumed to be.

- **Grounds** for processing of (non-sensitive) personal data include: **Consent** (s. 12), strictly defined (similar to GDPR requirements); including prohibiting non-supply because of refusal to provide non-necessary data (s. 12(3)), as in Korea and Singapore; fiduciary has burden of proof of consent. [√GDPR]; **Alternative grounds** include State functions; compliance with law; emergencies ('prompt action'); and employment. [?GDPR]

- The DPAI can specify a broad range of **'reasonable purposes'** as grounds for processing of (non-sensitive) personal data, other than consent (s. 17), within factors it must consider, but with no real limits on subject matter. More specific definition, in the legislation, is preferable. In comparison, the GDPR specifies grounds for processing other than consent which are specific in the objectives that are to be achieved (GDPR, art. 6). [?GDPR]

- Grounds for **processing sensitive data** (ss. 18-21) generally require more 'explicit consent' (defined), or other 'explicit' or 'strictly necessary' (as opposed to 'necessary') conditions. The differences are arguably too slight, and should be better defined. [?GDPR]

Obligations of data controllers (data fiduciaries)

There are in effect 3 categories of data fiduciaries:

- '**Significant data fiduciaries'** (SDFs), designated as such by DPA (s. 38(1)), who therefore have additional obligations (below), not imposed on other fiduciaries (s. 38(3)). There are objective criteria that the DPA must take into account in deciding which data fiduciaries are 'significant', but there is a large amount of discretion involved (s. 38(1)).

- '**Small entities'** (defined) doing manual processing are exempt from some (but not very many) obligations (s. 48). Only applies if annual turnover is less than US$30K p/a, and other conditions apply – a minimal exception.

- **(normal) data fiduciaries** – those without the additional obligations of a significant data fiduciary (unless the DPA so requires), but without the reduced obligations of a small entity.

The obligations on all (normal) data fiduciaries include:

- **Notice** obligations are extensive, both for collection from data principals, and from third parties (s. 8). [√GDPR]

- **Data quality** obligations, including requirement to notify 3rd party recipients of changes (s. 9). [√GDPR]

- Automatic requirement of **deletion** when purpose complete (s. 10). [√GDPR]

- **Demonstrable accountability** is required (s. 11). [√GDPR]

- **Privacy by design** (s. 29) [√GDPR]

- **Transparency** (s. 30) [√GDPR]

- **Security**, including periodic review (s. 31).
- **Data breach notification** to the DPA (s. 32). [√GDPR] Whether there is to be data breach notification to data principals is at the discretion of DPAI. The Bill should state objective criteria as to when DPAI must require notification (s. 32(5)). [?GDPR]

There are increased obligations of '**significant data fiduciaries'**, and some other fiduciaries:

- **Registration**: SDFs must register with DPA, as it specifies (s. 38(2)).
- **Data protection impact assessment** (DPIA) (s. 33) required not only by SDFs, but also where there is a significant risk of harm; must be submitted to DPA. [√GDPR]
- **Record-keeping** (s. 34): sufficient to demonstrate compliance, document security reviews, DPIAs, others as DPA specifies; applies to all government entities. [√GDPR]
- **Audits**: auditors independent and DPA-certified; required annually (and on DPA demand); auditors may assign 'data trust ratings' (s. 35). [√GDPR]
- **Data Protection Officer** (DPO): appointment required; tasks specified; DPA may specify qualifications (s. 36). [√GDPR] A role of DPOs independent from a data fiduciary not required. [?GDPR]

Rights of individuals (data principals)

The main rights of data principals are as follows (see below for rights and obligations omitted):

- Confirmation and **access** rights (s. 24) limit access to a 'brief summary' of personal data, and of processing activities. They should instead guarantee access to 'a copy' of both, otherwise this provision is open to abuse. [?GDPR]
- **Correction, completion and updating** (s. 25) – with third party recipients informed of changes.
- Data **portability** right (s. 26) – Goes further than the GDPR in explicitly including data generated or added by the data fiduciary. [√GDPR]
- **Right to be forgotten** (RTBF) (s. 27) – A very explicit right based on three grounds (a) purpose for which disclosure was made is no longer necessary; (b) consent on which disclosure is based has been withdrawn; or (c) disclosure was illegal. [√GDPR] There are grounds for Adjudicating Officers to decide take into account relevant public interest and other considerations.

Foreign effects (I): Extraterritorial scope and outsourcing exemption

The Bill's **extra-territorial scope** (s. 2) is very broad, including: processing by Indian entities (no matter where occurring); and processing by fiduciaries or processors not present in India if it involves offering goods or services to data principals within India, or profiling them. [√GDPR]

A significant data fiduciary (SDF) located outside India must **appoint a DPO** 'who shall be based in India' to represent the SDF (s. 36(4)).

The Government has power to exempt specified processing of personal data of foreign nationals not present in India (the '**outsourcing exemption'**) (s. 104). [?GDPR] This is

undesirable if India wishes to be seen as a global leader in the ethical processing of personal data.

Foreign effects (II): Data exports and data localisation

Data localisation and data export requirements create complex combinations of obligations:

1. **Local copy requirement (localisation #1)**:
    a. All personal data must be located on a server in India (s. 40(1)). Localisation is already being required for some financial transactions. [15]
    b. Government may exempt categories of data (s. 40(3)).
    c. Sensitive personal data (SPD) cannot be exempted (s. 40(4)).
2. **Export prohibitions (localisation #2):** Categories of '**critical personal data'** (CPD) specified by government (either personal data or SPD) 'may only be processed in India' (s. 40(2));
    a. [Most] CPD cannot be exported; export permissions (below) do not apply.
    b. [Exception] Transfers of CPD can occur to a country/sector which is found 'adequate' under s. 41(1)(b); or where 'strictly necessary' to a health/ emergency services provider anywhere (s. 41(3)).[16]
    c. If data is not CPD, then export permission requirements still apply.
3. **Export permission requirements:** Data which is **not CPD** can be exported:
    a. Pursuant to '**standard contractual clauses**' or 'intra-group schemes' (or **BCRs**) (s. 41(1)(a)), approved by DPA as providing 'effective' [not 'adequate'] protection (s. 41(5)), and the fiduciary certifies that it will **bear liability** for any non-compliance by the transferee (s. 41(6)).
    b. Pursuant to an **'adequacy' finding** by the government of a foreign country/ sector (s. 41(1)(b) and s. 41(2)).
    c. Where the DPA approves transfers due to 'a situation of necessity' (s41(1)(c)).[17]

There are no 'adequacy issues' [?GDPR] noted next to data localisation requirements, because any objections that the EU might have would not be based on lack of protection to the interests of EU data subjects, but rather in relation to the economic interests of EU countries in wanting to maximise free flow of personal data. The EU, US and other countries may take such provisions to WTO dispute resolution bodies, depending on their application.

---

[15] See 'Google seeks extension on meeting RBI's data localisation mandate' *The Hindu – Business Line* 10 September 2018; Data localisation provisions in an April 2018 directive by the Reserve Bank of India (RBI), anticipate to some extent the data localisation recommendations in the SriKrishna report. They require detail of all financial transactions, 'end to end', to be located on a server in India by October 15. Some foreign companies are seeking delays until the Bill is enacted.

[16] There is a logical error in the proviso to s. 41(1), because s40(2) refers to *all* personal data, not only SPD, and s. 41(1) must do likewise, or it would be a partial repeal of s40(2). Similarly, it does not make sense for s 41(3) to only apply to 'sensitive personal data', because the same reasons for making exceptions apply even more strongly to normal personal data. I have assumed in the above that s. 41(1) and s. 41(3) apply to all personal data. [An alternative approach is to assume that *only* sensitive personal data can be CPD, in which case there are no logical problems – but neither the Report nor the Bill say this.]

[17] The logical structure of s. 41(1) makes s. 41(d) and (e) redundant. If there was an 'and' after (c), then consent would be required in addition to (a) or (b) being satisfied.

Enforcement: DPA, administrative penalties and offences

Data Protection Authority of India (DPAI) is established (no DPA at present), with seven members (s. 49). [√GDPR] Key features of its powers and operations are as follows:

- The DPAI is described as an 'independent regulatory body' by the Srikrishna Report,[18] but in fact it is not fully independent (though with many indicia of independence). The Government can issue directions to it, as it thinks fit, to protect a wide range of state interests; it is bound by any written directions from the government 'on questions of policy'; and such directions are (purportedly) not subject to judicial review (s. 98). All of these provisions should be deleted, and the DPAI should have the full independence of almost all other DPAs across the globe.This puts the DPAI in the small rump of 100+ DPAs in the world that are subject to government directions (Malaysia, Singapore, Morocco, few others). The EU interpretation of complete independence has been very strict in a series of CJEU cases [?GDPR].

- There will be a separate 'adjudication wing' of the DPAI to decide penalties and compensation (s. 68(1)). ? The appointment of Adjudicating Officers (AOs) and the manner of adjudication is to be controlled by government regulations, and their independence is unclear (s. 68(2)). [?GDPR] AOs with the crucial roles of deciding penalties and compensation (s. 68(1)) must have unimpeachable independence

- Appeals against DPAI decisions would be to an administrative tribunal (either new or existing) (s. 79), and then to the Supreme Court (s. 87).

- The DPAI has a very wide range of enforcement powers (s. 64), influenced by 'responsive regulation' theory.[19] [√GDPR]

- Administrative penalties can be imposed by the DPAI, which (depending on the provision breached) can be up to 2% or 4% of the data fiduciaries' 'total worldwide turnover of the preceding financial year' (s. 69). [√GDPR]

Re-identification of de-identified data (which would including purportedly anonymised data which is in fact not anonymised) is made an offence. This means that sham anonymisation cannot be exposed (as in the Australian Medicare/PBS 'open data' scandal exposed by Melbourne University researchers[20]). This offence at least requires a defence for bona fide security research, otherwise it becomes a 'shoot the messenger' approach. [?GDPR]

Rights and obligations not included in the Bill

The following rights and obligations found in the GDPR have been intentionally omitted from the Bill:

---

[18] 'a high-powered, independent national body'; 'to ensure the independence of the members of the DPA…': Srikrishna Report pp.152-3.

[19] The Srikrishna Report p. 151 cites my *Asian Data Privacy Laws* (OUP, 2014) as their basis for stating that 'a responsive regulatory framework equipped with a range of tools has been found by us to be of critical importance'. In Asian Data Privacy Laws, the relevant section is Chapter 3, part 4 'Standards for enforcement mechanisms and 'responsive regulation'. The Report also frequently attributes considerable influence on the details of its regulatory approach to submissions by Dvara Research, which adopts a 'responsive regulation' approach. They have subsequently published Beni Chugh, Malavika Raghavan, Nishanth Kumar & Sansiddha Pani *Effective Enforcement of a Data Protection Regime: A Model for Risk-Based Supervision Using Responsive Regulatory Tools* Dvara Research, July 2018 <https://www.dvara.com/blog/wp-content/uploads/2018/07/Effective-Enforcement-of-a-Data-Protection-Regime.pdf>

[20] C. Duckett 'Re-identification possible with Australian de-identified Medicare and PBS open data' ZDNet 18 December 2017 <https://www.zdnet.com/article/re-identification-possible-with-australian-de-identified-medicare-and-pbs-open-data/>

- **Privacy by default** is not included in privacy by design. [?GDPR] It should be specifically included in privacy by design, because although it can be implied by some provisions of s. 29, it does not state that the most privacy-protective legal option should be presented to users as the default. It is desirable that users should not have to opt-in to obtain maximum protection of privacy, but instead should have to opt-out to surrender their privacy.

- The right not to be subjected to **automated processing**, at least without human intervention, is omitted, on the basis that this can be dealt with by enforcement of privacy by design. [?GDPR] It should be included in the Bill, because it is very unlikely to be dealt with by enforcement of privacy by design (as the Srikrishna Report suggests[21]). It requires a specific legislative provision because of its high importance, since future processing is well known to be increasingly dominated by algorithms, 'big data' and AI.

- **Rights to object to or block processing** are omitted on the basis that this can be achieved by seeking interim orders from DPA on correction etc rights. [?GDPR] The Srikrishna Report suggestion[22] that this can be achieved by data principals seeking interim orders from the DPAI based on correction rights is unrealistic, because applications to block processing (temporarily or permanently) are not necessarily based on correctible errors.

- No **direct marketing opt-out** is provided because it is claimed that the Bill's strict approach to consent in effect requires prefers an opt-in to direct marketing.[23] For certainty, this also require a specific provision that marketing is not a secondary use anticipated by principals. [?GDPR]

Conclusions

The Srikrishna Report and Bill provides a very considered and intellectual approach[24] to data privacy, which one might expect from a committee led by a distinguished Indian jurist. Both reflect a very different regulatory philosophy from the GDPR's radical dispersal of decision-making responsibility (and liability for wrong decisions) to data controllers. The Indian model is more prescriptive (perhaps closer to the 1995 EU Directive in this respect), and in many ways achieves this by effectively leaving delegated legislative responsibility to the DPIA (or in some cases the government).

Business and individual implications

If India enacts a law such as the Bill accompanying the Srikrishna Report this will be seismic event for data privacy in India, in contrast with the near-complete uselessness of the current laws.[25] Businesses operating in India will have to provide meaningful privacy protections for the first time, and approximating the highest international standards. For residents of India this will be a quantum leap forward, despite weaknesses (capable of future remedy, including by Supreme Court decisions).

Foreign companies whose activities affect Indian residents by marketing actions or surveillance will frequently come within the law's extra-territorial scope, but post-GDPR new

---

[21] Srikrishna Report pp.. 74-5.

[22] Srikrishna Report p. 74.

[23] Srikrishna Report pp. 74,

[24] See in particular Chapter 1 of the Srikrishna Report.

[25] G. Greenleaf *Asian Data Privacy Laws* (OUP, 2014), Chapter 15 'India: Confusion Raj, with Outsourcing'..

laws everywhere are erecting such hazards. US and other companies obtaining processing in India will seek 'outsourcing exemptions' from all or most of the law. The EU might insist that no such exemptions apply to any processing of data originating from the EU.

Adequacy applications

Whether the EU would regard such a law as 'adequate' is unsafe to guess, because the draft Bill contains significant numbers of both strengths and weaknesses in matters that the EU may regard as important. Until the EU completes its consideration of Japan's adequacy, no GDPR precedents are available.

However, such a law would at least give India a much more plausible opportunity to argue (and negotiate) its case than on previous occasions (the last in 2013). Many aspects which could be regarded as adequacy deficiencies might be amended easily (eg deletion of government directions to the DPAI). But we do not yet know whether the Indian government will accept an approach as strong as that taken by the Srikrishna committee and its Bill, unless the dangers of unconstitutionality and its threat to the Aadhaar forces their hand. The impending Supreme Court decision in the *Aadhaar Case* will shed light on that.

A 'Fourth Way' for data protection?

The Srikrishna Report makes the ambitious claim that its approach (and that of the Bill) is a 'Fourth Way to privacy, autonomy and empowerment', distinct from the approaches of the US, EU and China, a new model which is relevant to 'all countries in the global South'.[26] The report also posits as one of the three principled objectives of a data protection law that of 'establishing a domestic model that can be replicated by other jurisdictions such that each respects international comity'.[27]

To what extent is this really a distinctive 'Fourth Way', or one worth emulation by the 'Global South'? The draft Bill is very substantially compatible with, and clearly modelled upon, the EU GDPR, without being a carbon copy (and with deficiencies). It has Chinese-influenced data localisation provisions,[28] unlikely to appeal to either the EU or US. There is very little evidence of US influence, other than an 'outsourcing exemption' which is likely to appeal to US and other businesses. There is a separate but not fully independent DPA, as in Singapore and Malaysia, which may appeal to more authoritarian governments. An alternative description is 'GDPR-Lite with Chinese characteristics'.[29] It's not really a distinctive 'Fourth Way', but it might appeal to countries in the 'Global South' looking to combine nationalistic data localisation with a moderate but incomplete level of GDPR consistency. However, it must be remembered that very few countries in the Global South share India's characteristics of a robust democracy, a well organised civil society, a very strong constitutional rights of privacy, and courts that do impose significant limitations on government and private actions. India's model might be a reasonable one for other such countries, but dangerous in the hands of the many autocracies (or worse) in the Global South.

---

[26] Srikrishna Report, pp. 13-14

[27] Srikrishna Report, p. 16.

[28] G. Greenleaf 'PRC's New Data Export Rules: 'Adequacy with Chinese Characteristics'?' (2017) *147 Privacy Laws & Business International Repor*t 9-12 <https://papers.ssrn.com/abstract_id=3026914>,

[29] I have argued elsewhere that the post-2018 global standard for data privacy will not require everything that is in the GDPR, and that a likely contender for what will be in this 'GDPR Lite' is something close to the content of the 'Modernised' Convention 108 ('108+'): G. Greenleaf 'Convention 108+ and the Data Protection Framework of the EU (Speaking Notes for Conference Presentation)' *Convention 108+ Tomorrow's Common Ground for Protection* (Council of Europe, Strasbourg, 21 June 2018) <https://papers.ssrn.com/abstract_id=3202606>. India's may influence what is 'GDPR Lite'.