UNSW Law & Justice Research Series

India's 2023 Data Privacy Act: Business/government Friendly, Consumer Hostile

Graham Greenleaf

[2024] *UNSWLRS* 8
(2023) 185 *Privacy Laws & Business International Report* 1, 3-12

UNSW Law & Justice
UNSW Sydney NSW 2052 Australia

E: LAW-Research@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

India's 2023 data privacy Act: Business/ government friendly, consumer hostile

Graham Greenleaf, Professor of Law & Information Systems, UNSW Sydney
(2023) 185 *Privacy Laws & Business International Report* 1, 3-12

Suddenly, it was completed. Within a week of introduction into Parliament, India's *Digital Personal Data Protection Act, 2023*[1] was passed by both houses with no debate, and no requirement of committee consideration. It received Presidential assent on 11 August 2023. The Act, or particular provisions, will come into force on dates notified in the Official Gazette. India's Minister for Electronics and IT says the government may allow as little as six months for compliance, but not as long as two years, after consultation with industry.[2]

Other than the United States, India has until now been the most significant country, economically and politically, not to have a comprehensive data privacy law.

Five years after the committee chaired by former Justice BN Srikrishna delivered its report, recommending a strong international-standard Bill, this proposed law was progressively weakened by a succession of Government-redrafted Bills, and by recommendations of a joint Parliamentary committee report.[3] The final Act inherits many of these accumulating weaknesses,[4] but is closer to a completely new draft, rather than a redraft of any previous version. The lack of any consultation on this Bill is therefore a result of a more authoritarian political system.

This article focuses on the resulting Act, rather than its history, and aims to identify which are the main societal interests that the Act is likely to benefit the most, including the Indian business sector, foreign businesses, individuals (consumers and citizens), and the Indian government.

Scope and special categories

The Act applies to all levels of government in India (Central, State and local), and to the private sector, all of which come within the meaning of 'Data Fiduciaries' (s2(i)). In Indian

---

[1] *Digital Personal Data Protection Act, 2023* <https://prsindia.org/files/bills_acts/bills_parliament/2023/Digital_Personal_Data_Protection_Act,_2023.pdf>

[2] 'Government may give six months to industry to align with data protection rules: MoS IT Rajeev Chandrasekhar' *Economic Times,* 5 September 2023

[3] The main stages in this evolution were: report by a Committee of Experts on Data Protection (Srikrishna Report), July 2018; Personal Data Protection Bill, 2019 to Lok Sabha, Dec 2019; Bill reported on by a Joint Parliamentary Committee, Dec 2022; Bill withdrawn, August 2022; Nov 2022, new Draft Bill released for public consultation; August 2023, Digital Personal Data Protection Bill, 2023 introduced in Parliament.

[4] PRS Legislative Research (*Summary) Digital Personal Data Protection Act, 2023* <https://prsindia.org/billtrack/digital-personal-data-protection-bill-2023> includes a comparison of reports and bills from 2018 which demonstrates how previous versions were stronger.

legislation, 'the State' encompasses all these levels of government,[5] and this is crucial in this Act.

The Act only applies to the processing of 'digital personal data' which means that it is collected in digital form (or subsequently digitised) (s3(a)), so paper-based transactions are exempt, except for such data as is digitised.

'Personal data' is given a conventional definition, meaning 'any data about an individual who is identifiable by or in relation to such data' (s2(t)). Such individuals are 'Data Principals' (data subjects), and those who control the use of personal data about them are Data Fiduciaries (controllers), assisted by contracted Data Processors.

There are no separate categories of data, such as 'sensitive data'. Special protection of specified categories of data based on sensitivity is typical in post-1995 data protection laws. As a result, there is no requirement in India to take special care with data about such matters as race, caste or tribe, criminal records, religious or political beliefs, sexual orientation, health, financial affairs, biometrics, genetic characteristic or any other characteristics. The previous Indian draft Bill did protect 'sensitive personal data' including the above matters, except race or criminal record. This Act is therefore an abrupt departure from both the previous draft and international standards.

There is however, in effect, a separate category of special protections for the personal data of children: verifiable consent of the child's parent or lawful guardian must be obtained before any processing (and of persons with disabilities who have lawful guardians); processing likely to cause any detrimental on the well-being of a child must not occur; tracking, behavioural monitoring or targeted advertising must not occur in relation to children (s9(1)-3). However, the Government makes exceptions (s9(4)-(5)). On its face, this is strong protection for children's privacy. But it is also bizarre and undesirable that all persons with any disabilities are equated with children.

Another important weakness in the meaning of 'personal data' is that it does not include any data which the Data Principal has made publicly available, or anyone else has done so as a result of a legal obligation (s3(c)). Internationally, most countries take the EU GDPR approach that such information is still 'personal data', but a significant minority of countries[6] (e.g. Australia, Singapore, Malaysia) take an approach similar to India. Because of the rise of social media services, this is now a far more dangerous provision.

---

[5] Article 12, *Constitution of India*: The State includes the Government and Parliament of India and the Government and the Legislature of each of the States and all local or other authorities within the territory of India or under the control of the Government of India.

[6] Greenleaf, G 'Private Sector Uses of 'Public Domain' Personal Data in Asia: What's Public May Still Be Private' (2014) 127 *Privacy Laws & Business International Report*, 13-15, <https://ssrn.com/abstract=2438368>

Exemptions: Numerous weaknesses

The Central Government has very broad powers to utilise exemptions[7] from the Act, both complete and partial:

- It may completely exempt processing by specified State instrumentalities, on very broad grounds of State interests (s17(2)(a)).
- It may notify as exempt certain Data Fiduciaries, or classes of Data Fiduciaries (s17(3)), either from the public or private sectors. It can also, within five years, declare that any provisions of the Act will not apply to Data Fiduciaries or classes of same, for a specified period (s17(5)). Either provision may result in broad exemptions, for reasons which are not controlled by any objective standard. They could also result in undesirable and potentially anti-competitive case-by-case exemptions.
- It may also completely exempt processing necessary for research, archiving or statistical purposes if the personal data is 'not to be used to take any decision specific to' an individual', and is carried out in accordance with prescribed standards. (s17(2)(b)). It will be very important, and potentially dangerous, if such processing can be for commercial 'research', for example the creating of Large Language Models (LLMs) for generative AI.

'Automatic' exemptions, not depending on Government notifications, are also very significant:

- The State or its instrumentalities are automatically exempt (17(4)) from data erasure obligations, both automatic and on request (s8(7) and s12(3)), and from making corrections etc on request, unless the data is being used to make decisions about a person (s12(2)).
- There are also numerous automatic exemptions from parts of the Act for processing in relation to enforcing legal rights, judicial or regulatory functions, law enforcement, company reorganisations, and credit defaults (s17(1)). These are exemptions from most of the Act, but not from Data Principal's rights, some Data Fiduciary obligations, or from the s16 export prohibition.

The combination of the first category s17(2)(a)) of notified exemptions, and the first category of automatic exemptions (s17(4)) means that the Central Government (and to a lesser extent, other governments) can collect much personal data without consent, and can accumulate personal data without ever deleting it, or even ensuring its accuracy in most cases. It is a recipe for creating comprehensive government surveillance. This may be one of the most important deficiencies of the Act. It may also make the Act vulnerable to claims that it unconstitutional because of lack of proportionality, based on *Puttaswamy*'s setting out of the constitutional right of privacy (see later).

---

[7] In India, exemptions made by Government delegation are only subject to Parliamentary disallowance if they are 'specified'. Other forms of delegation, such as by matters being 'prescribed' (usually Rules) are not disallowable but only require tabling in Parliament. Matters that may be 'notified' are not disallowable.

Data localisation

Some concept like 'critical data' is increasingly used to identify data which (in various places[8]) can only be stored within the country (so no exports are allowed, and processing must occur within the country), or a copy of which must be kept within the country (and exports and overseas processing are then allowed). No such explicit 'data localisation' provisions are included in this Act, but that is not the end of the matter. First, it is possible that data export restrictions (see below) could be used for this purpose.

Second, there are already separate laws of major importance in India which do require data localisation,[9] including the *Companies Act 2013* s94 and the *Companies (Accounts) Rules 2014*,which require covered organizations to store financial information at the registered office of the company; an April 2018 circular by the Reserve Bank of India (RBI), 'Storage of Payment System Data', which 'ordered all payment companies to keep all information relating to payment systems[10] on servers in India'; and the *IRDAI (Maintenance of Insurance Records) Regulation, 2015*, s3(9) which requires covered organizations to store insurance data within India.

International aspects: Extra-territoriality, export blacklist and outsourcing exemption

Processing of data outside India on Data Principals (data subjects) in India is within the extra-territorial jurisdiction of the Act, but only for transactions offering goods and services (s3(b)), and not for monitoring as in the EU.

The Government may by notification restrict transfer of personal data to any overseas country or territory (s16) – 'blacklisting'. Until such notifications are made, data may be transferred anywhere. The Data Protection Board (see below) has no role in determining which countries are blacklisted. There is no 'positive' test (e.g. 'adequacy' or equivalence to this law) to justify transfers, only a negative blacklist (once made) for which the Act does not state any objective criterion for inclusion. The export blacklist is therefore completely within the discretion of the Central Government, and all other countries are, by default, included on the data export 'whitelist'. For example, there is no restriction at present, on data exports to the US, despite its lack of general data privacy laws. In fact, India's position on data exports, until it creates a blacklist, is closest to that of the US.

The Act includes an 'outsourcing exemption' from its operation, excluding from its scope any processing within India of personal data of persons outside India, pursuant to a contract (s17(1)(d)). So, outsourced processing in India of data on EU residents is not protected by the Act, which should be fatal to India obtaining a positive 'adequacy' assessment from the EU (which it has failed to do twice before, the most recent being in 2013). EU companies wanting to outsource processing to India would have to rely on the use of GDPR Standard Contractual Clauses (SCCs, as revised, June 2021) for each outsourcing contract, which

---

[8] For example. in China, Russia, Kazakhstan, and Sri Lanka (public sector).

[9] The following is paraphrased from Ravi Singhania 'All about Data localisation in India' Singhania & Partners LLP, 14 April 2023 <https://irglobal.com/article/all-about-data-localisation-in-india-2/>

[10] *ibid*, the RBI clarified what kinds of information must be kept in India in 'Storage of Payment System Data' <https://m.rbi.org.in/Scripts/FAQView.aspx?Id=130>

means the situation will be unchanged from what it is now. The 'new' SCCs, revised by the European Commission in 2021 in light of the *Schrems II* decision of the CJEU (Case C-31/18) includes additional clauses such as Clause 14 which requires the Indian importer, and the EU exporting party to prepare a data transfer impact assessment (DTIA) which, among other things, assesses Indian laws requiring disclosure of data to public authorities, or authorising access by such authorities. The difficulties in applying SCCs in the Indian context are beyond the scope of this article, but they are not trivial.

Countries which have positive adequacy findings from the EU (e.g. the UK, Japan and Korea) will not be able to outsource to India without taking similar precautions, or they may risk their EU adequacy status. In contrast, outsourcing from the US could carry on without additional restriction.

Legitimate processing

Processing by Data Fiduciaries must be either with consent of the Data Principal, or for specified legitimate uses (s4), and must not be for an unlawful purpose.

Consent by Data Principals, for specific purposes, has a strong definition: 'The consent given by the Data Principal shall be free, specific, informed, unconditional and unambiguous with a clear affirmative action, and shall signify an agreement to the processing of her personal data for the specified purpose and be limited to such personal data as is necessary for such specified purpose' (s6(1)). This is comparable to the definition of consent in the EU GDPR (art. 4(11)) and is stronger because the inclusion of 'necessary for such specified purpose' adds a data minimisation requirement. Consent may be withdrawn at any time, with equivalent ease to consenting (s6(4)). Consents to waive rights under the Act, or obligations of Data Fiduciaries, or of any other law, are invalid (s6(2), s8). A Data Principal 'may give, manage, review or withdraw her consent to the Data Fiduciary through a Consent Manager'[11] (s6(7)), who must be registered with the Board (s6(9)).

Consent must be obtained by the Data Principal being given a notice accompanying or preceding the request, specifying the proposed purpose of processing, how rights may be exercised, and how complaints may be made (s5(1)). These requirements are repeated in s6(3) which adds that the contact details of a Data Protection Officer (DPO) or equivalent person must be given. For data already collected prior to the Act's commencement, the Data Fiduciary must, as soon as reasonably practicable, give the same notice (s5(2)). The Data Principal may request the notice in a common language in India (s5(3)).

The 'legitimate uses' on the basis of which personal data may be processed without consent are very broad. They are (s7):

- It can be processed 'for the specified purpose for which the Data Principal has voluntarily provided her personal data to the Data Fiduciary' (s7(a)). It seems that such voluntary provision of personal data differs from personal data provide pursuant to a request by the Data Fiduciary. The notice required by s5 would not have to be

[11] ' "Consent Manager" means a person registered with the Board, who acts as a single point of contact to enable a Data Principal to give, manage, review and withdraw her consent through an accessible, transparent and interoperable platform;' (s2(g)). Another class of consent managers, Account Aggregators (AAs) are already operational in the financial sector.

given (after the volunteering), and nor would the requirements of the s6 definition of 'consent' need to be observed, including withdrawal of consent. These are very undesirable consequences, effectively creating two ill-demarcated classes of data about each Data Principal, one of which has far fewer protections.

- Data matching and profiling by any government instrumentalities (central, state or local), for the purpose of allocation of government benefits is facilitated, provided conditions are met: it is a 'subsidy, benefit, service, certificate, licence or permit' that has been prescribed for this purpose (s7(b)); the Data Principal must have previously consented to the processing of their data for benefit purposes, or a government must already hold data that the Central government notifies; and standards set by the Central government must be observed.

- Use for any government function 'in the interests of sovereignty or integrity of India or security of the state' (s7(c)).

- Use by any person to fulfil specific public interest tasks: legal obligations to disclose personal data to governments; for compliance with judgments etc; medical emergencies; threats to public health; and disasters (7(d)-(h)).

- Other than for 'voluntary provision' (above), the main business exception from consent is for employment purposes, uses 'for the purposes of employment or those related to safeguarding the employer from loss or liability' (s7(i)). This gives employers a broad ambit within which to use personal information without consent.

None of these 'legitimate uses' are exemptions from the obligations of a Data Fiduciary, they only allow personal data to be used without consent. However, unlike uses by consent, they do not require any notification of the use (or right to complain) to the Data Principal, either before or after the use is made. Unless the Data Principal requests a copy of their record, these uses will usually remain secret uses. Nor are these 'legitimate uses' required to have any close connection to the original purpose of use.

These 'legitimate uses' are particularly dangerous for the uses by government instrumentalities under s7(b) and s7(c), which could result in very large dossiers. This is particularly so because the right to automatic erasure of data once its specified purpose is no longer being served is waived wherever retention is required by law (s12(3) – more details below). Some critics consider that the potential for data to be combined, with exemptions from erasure, creates the risk of 'profiling of citizens'.[12]

[12] PRS Legislative Research, *op cit*.

Obligations of Data Fiduciaries (controllers) and SDFs

All Data Fiduciaries (data controllers), including those in government, have the following normal obligations:

- To 'ensure its completeness, accuracy and consistency', if it is 'used to make a decision that affects the Data Principal or disclosed to another Data Fiduciary' (s8(3)).
- To 'ensure effective observance of the provisions' of the Act and rules, by implementing 'appropriate technical and organisational measures' (s8(4)). This could come close to the EU GDPR's 'demonstrable accountability'.
- To take 'reasonable security safeguards to prevent personal data breach' (s8(5));
- To 'give the [Data Protection] Board and each affected Data Principal' notice of any data breaches, in a prescribed manner and form (s8(6)). The obligation to notify individuals of every breach is immediate, on the face of the section, but the manner and form to be prescribed may well cut this back somewhat.
- To 'erase personal data, upon the Data Principal withdrawing her consent or as soon as it is reasonable to assume that the specified purpose is no longer being served, whichever is earlier' (s8(7)). Data Processors are required to do likewise. Erasure is therefore supposed to be automatic, not dependant on a request. However, erasure is not required if the data is necessary for the specified purpose or is required by law (s12(3)), which is a significant loophole.
- To publish in a prescribed manner the business contact information of a Data Protection Officer, or other respondent on behalf of the Data Fiduciary (s8(9)).
- To 'establish an effective mechanism to redress the grievances of Data Principals' (s8(10)).

A Data Fiduciary cannot contract out of these obligations by passing them on to a Data Processor that it employs (s8(1)).

The Central Government can designate certain Data Fiduciaries to be Significant Data Fiduciaries (SDFs) who have extra obligations, namely:

- to establish periodic independent audits (including appointing the auditor) to evaluate the SDF's compliance with the Act; and
- to establish periodic Data Protection Impact Assessments;
- to undertake such other measures as may be prescribed.

SDFs are to be appointed according to such relevant factors as the Central Government may determine, 'including the volume and sensitivity of personal data processed; risk to the rights of Data Principal; potential impact on the sovereignty and integrity of India; risk to electoral democracy; security of the State; and public order.' (s10(1)). An SDF need not satisfy any particular combination of these attributes, but they are indicative of the legislative intention.

For example, a small organisation might be involved in a mass facial recognitions scheme, or misuse people's personal data on social media in a way that could influence elections.

An overseas SDF must have a Data Protection Officer based in India, who is the point of contact for grievance-handling and is responsible to the company's overseas Board of Directors, or have similar seniority (s8(2)(a)).

Rights of Data Principals

The rights of Data Principals to access, correction, updating deletion etc (ss11-12) apply where the Data Principal has previously consented to the collection of personal data by the Data Fiduciary, and where the data has been voluntarily provided (under s7). There are no such rights where the personal data has been received from a third party, or extracted from a documentary source, even if this data requires updating or correction. Other rights do not have this restriction.

The rights of Data Principals are:

- To obtain a summary of personal data being processed and the processing activities undertaken ....' (s11)1)(a)).
- To obtain 'the identities of all other Data Fiduciaries and Data Processors with whom the personal data has been shared by such Data Fiduciary, along with a description of the personal data so shared'(s11(1)(b)), but not in relation to law enforcement.
- To obtain 'any other information related to the personal data of such Data Principal and its processing, as may be prescribed' (s11(1)(c)). For example, a right to portability could be prescribed, which the Act does not otherwise provide.
- 'The right to correction, completion, updating and erasure.' Erasure must be provided unless the data is necessary for the specified purpose or is required by law (s12(3)).
- 'The right to have readily available means of grievance redressal provided by a Data Fiduciary or Consent Manager'. 'The Data Principal shall exhaust the opportunity of redressing her grievance under this section before approaching the Board.' (s13). Responses must be within a prescribed time (s13(2)), vital because otherwise a non-responsive Data Fiduciary could prevent a Data Principal being able to get their complaint before the Board so that it knows about and deals with matters of public importance. Individuals have no right to go direct to the courts.
- 'The right to nominate, in such manner as may be prescribed, any other individual, who shall, in the event of death or incapacity of the Data Principal, exercise the rights of the Data Principal' (s14). Data privacy rights can survive death, but only it seems if the right to nominate a post-mortem representative is exercised, since it does not go automatically to a person's heir if there is no nomination. No time limit is stated.

The Data Protection Board

A Data Protection Board of India (DPB) is created by the Act with a Chairperson and an unspecified number of Members appointed by the Central Government for (renewable) two-year terms (ss18-20). It 'shall function as an independent body' (s28(1)) and is a body

corporate that can sue or be sued (s28(2). It does have some other indicia of independence as well, such as limited grounds for removal from office, a right of its Members to be heard (s21), and a prohibition on post-office employment (s22).

However, other factors mitigate against effective independence. Two years is too short a term of appointment for DPB Members to show independence (five years is normal), because the Central Government will always hold over them the threat of imminent non-reappointment. The Board's powers could be constrained by requirements for their exercise being prescribed (s28(7)(d)). Budget and staffing are under the control of the Government (s24). Whether the Board would be assessed as independent is uncertain, but this may not matter to it (EU adequacy may no longer be a live issue, and questions of constitutionality may never arise).

The Board has powers to investigate data breaches and complaints against Data Fiduciaries (and others), to 'impose penalties' (s27(1)), and 'to issue such directions as it shall consider necessary' (s27(2)), and to 'take action in accordance with the provisions of this Act' (s28(2)). It is unclear what this last adds. It has no power to investigate matters of its own volution.

In effect, there is a right of re-hearing by the Board (perhaps the whole Board) for businesses affected by any penalties or directions, after which hearing it may change its order (s27(3)). There is also a right of appeal to the Appellate Tribunal (Telecom Dispute Settlement and Appellate Tribunal[13]) within 60 days (s29). The TDSAT is regarded as already overloaded. Data Principals have no such appeal rights,

Penalties and compensation

The Board can impose a monetary penalty 'specified in the Schedule' for a 'significant' breach of the Act (s33(1). GDPR-like matters specified are to be considered (s33(2)). The maximum penalty for breaches of the Act, for failing to take reasonable security safeguards to prevent data breaches, is equivalent to US$31M (Schedule, item 1). Other breaches carrying potential maximum penalties over US$15M are for failure to notify the Board or affected Data Principals of data breaches, breaches of additional obligations to children, and breaches of additional duties of SDFs (Schedule, items 2-4). Breaches by Data Fiduciaries of any other provisions of the Act or Rules can attract maximum penalties of equivalent to US$6M, which may be too low to deter large-scale breaches of some provisions. The Board therefore has significant powers, often to international standard, to impose penalties on Data Fiduciaries for breaches of the Act, if it chooses to use them.

If the Board imposes two or more fines on a Data Fiduciary, it can recommend to the Government that public access to the Data Fiduciary should be blocked, and intermediaries must comply with such blocking orders (s37). This 'censorship' provision may prove controversial.

No civil court may entertain any legal action 'in respect of any matter for which the Board is empowered …' (s38), so injunctions against the Board exercising it powers are not possible, and nor are appeals, except to the Appellate Tribunal.

---

[13] Telecom Dispute Settlement and Appellate Tribunal <https://tdsat.gov.in/Delhi/Delhi.php>

The Board has no powers to order compensation payments to Data Principals, and no court is explicitly granted such power. This is a major deficiency of the Act, compared with international standards. However, it could be argued that, because the Board is not empowered in relation to matters of compensation, a court would not be blocked by s38 from ordering compensation if it otherwise had powers to do so (for breach of statutory duty, breach of confidence, negligence etc). This is speculative, but worth considering.

Regional considerations

India's South Asian neighbours may be affected by India finally having a law, and by its content. Sri Lanka already has a law.[14] Pakistan's Bill (recently agreed to by Cabinet, but not yet introduced to Parliament[15]), and Bangladesh's Bill (only a government proposal as yet[16]) might be amended before enactment. These are the last significant countries in Asia not to have a data privacy law, the remainder being authoritarian dictatorships,[17] a hereditary autocracy,[18] or very small democracies.[19] For most practical purposes, all of Asia will soon be a region of data privacy laws.

Comparing rights and obligations with the GDPR

Considering both these rights and also the obligations of data fiduciaries, they are quite limited compared with the EU GDPR, because they omit the following twelve rights or obligations: additional protections for defined sensitive data (including biometric and genetic data), data portability; limits on automated decision-making; restrictions on data exports; data protection by design and default; direct liability for processors; proportionality in processing; the 'right to be forgotten'; DPA cooperation in complaint resolution; representative actions before the DPA or courts; maximum fines based on global turnover; and compensation as a judicial remedy. To note this is not to suggest that India's law should include all of these rights or obligations. However, they have become the 'gold standard' for international data privacy protection, and for such an important law as that of India to contain comparatively few of these principles has to be regarded as a setback for the advance of global privacy standards.

The inalienable constitutional right of privacy: Is it met?

An unusual nine judge 'constitution bench' of India's Supreme Court unanimously decided in *Puttaswamy v Union of India*[20] on 24 August 2017 that India's Constitution recognises an

---

[14] G. Greenleaf 'Sri Lanka's Personal Data Protection Act is Finalised with a Stronger DPA' (2022) 177 *Privacy Laws & Business International Report* 25-2

[15] G. Greenleaf 'Pakistan and Sri Lanka's Data Privacy Bills Move Forward' (2021) 173 *Privacy Laws & Business International Report* 24-27

[16] G. Greenleaf 'Bangladesh's Data Protection Bill' (2022) 179 *Privacy Laws & Business International Report* 26

[17] Afghanistan, Cambodia, Laos, Myanmar, and North Korea.

[18] Brunei

[19] Timor Leste and the Maldives.

[20] *Puttaswamy v Union of India* , Supreme Court of India, [2017] INSC 689, <http://www.liiofindia.org//in/cases/cen/INSC/2017/89.html>

inalienable and inherent right of privacy as a fundamental constitutional right.[21] Although privacy is not explicitly mentioned in the Constitution, this case holds that it is implied by Article 21's provision that '[n]o person shall be deprived of his life or personal liberty except according to procedure established by law' (and is also protected by other constitutional provisions providing procedural guarantees).[22] Privacy is a subset of liberty.[23] Privacy is not an absolute right, but '[a]n invasion of life or personal liberty must meet the three-fold requirement of (i) legality, which postulates the existence of law; (ii) need, defined in terms of a legitimate state aim; and (iii) proportionality which ensures a rational nexus between the objects and the means adopted to achieve them'.[24] The Court identified three main aspects of privacy: privacy of the body; privacy of information; and privacy of choice. Most aspects of data protection therefore come within the constitutional protection of privacy.

Subsequent smaller constitution benches of the Supreme Court may now decide the constitutionality of various pieces of legislation, and practices, in light of the fundamental right of privacy.[25] This may include the *Digital Personal Data Protection Act, 2023,* if a suitable case is brought before the Court. Whether this Act satisfies these requirements is unknown but is certainly debatable. The proportionality of exemptions is one of the most obvious grounds for challenge, and the lack of any principled restrictions on data exports might be another. As detailed above, there are a dozen ways in which India's law falls short of the GDPR's standards, and some might become part of an argument about constitutionality. Whether an Indian NGO will challenge the Act, or the current Court, now led by Chandrachud CJ, will be willing to fully apply the Constitution (both of which occurred in *Puttaswamy*) it is too early to say but should not be disregarded.

Conclusions: An Act to benefit business and government

First, it is too early to be sure about some benefits, because so many key factors await future government decisions. For example, which state instrumentalities, and which classes of Data Fiduciaries, will be exempted? Which companies will be designated as Significant Data Fiduciaries? Will the Board recommend that the Government issues 'blocking orders' against some companies? Which countries (if any) will be on the data export blacklist? More than twenty matters are 'as may be prescribed'. The answers to these questions will put a very different complexion on the Act.

---

[21] *Puttaswamy v UoI,* per Chandrachud J at p. 262; From this 547-page decision, the most comprehensive judgment 265 pages is that of Justice Chandrachud, in which Chief Justice Khehar and Justice Agrawal joined, and the other six Justices agreed. Quotes here are from the judgment of Chandrachud, J.

[22] The Court held that privacy's constitutional protection 'emerges primarily from the guarantees of life and personal liberty in Article 21' and that '[e]lements of privacy also arise in varying contexts from the other facets of freedom and dignity recognized and guaranteed by the fundamental rights contained in Part III'. *Puttaswamy v UoI,* per Chandrachud J at p. 262.

[23] The relationships between privacy and liberty were stated by Justice Chandrachud to be that '[p]rivacy constitutes the foundations of all liberty because it is in privacy that that the individual can decide how liberty is best exercised', although '[l]iberty has a broader meaning of which privacy is a subset'. *Puttaswamy v UoI,* per Chandrachud J at p. 243.

[24] *Puttaswamy v UoI,* per Chandrachud J at p. 262; and see pp. 254-7.

[25] See G. Greenleaf 'Constitution Bench' to decide India's data privacy future' (2017) 148 *Privacy Laws & Business International Report*, 28-31, for background to the Court's decision.

For businesses based in India (Data Fiduciaries), they now have a 'business friendly' Act imposing minimum obligations on them, although with some risks of substantial penalties for breaches.

For foreign businesses, based outside India (Data Fiduciaries) but wishing to outsource processing to India, or to remotely use personal data of persons located in India, or to import personal data from India, the position is mixed. The India Government may prohibit exports to any countries it chooses (or none), and it already has a raft of specific 'data localisation' laws. Processing overseas of data on those in India for transactions offering goods or services (including marketing) must comply in full with the Indian Act, but not for other purposes such as monitoring for political surveillance, or for training AI models.

Foreign businesses' outsourced processing in India is exempt from the Indian Act, but that is not the whole story. EU companies will need to rely on Standard Contractual Clauses and hope they do not have to face a Schrems-like challenge. Outsourcers from countries like the US with no data export restrictions will have no problems.

For Indian Governments and their instrumentalities (Data Fiduciaries), all are *prima facie* bound by the Act but benefit from a wide range of complete and partial exemptions from its provisions (with more to come), to an extent that the Act often seems like a blueprint for surveillance of citizens which, while not explicitly allowed at present, is not clearly illegal either.

For Data Principals – data subjects, consumers and citizens – this law provides at best a minimal set of rights and protections by international standards (far fewer than in the EU GDPR), riddled with deficiencies. Sensitive data is not given any extra protection, except for children. Personal data already made publicly available, including on social media or under a legal obligation, is not protected. Nor is data extracted from a documentary source. Very broad government powers to notify exemptions from the Act, both complete and partial, further reduces its scope, and risk authorising comprehensive government surveillance. Until and unless prohibited, personal data can be exported from India to anywhere in the world, with no protections required. 'Legitimate uses' allow personal data to be processed without consent on very broad grounds that have no necessary connection with the original purpose of collection, including expanding State surveillance. Some protections that do exist have crippling exemptions, for example the right of erasure. The Data Protection Board has questionable independence. Its power to fine is significant, but whether the actual penalties imposed by the Board will be more than a slap on the wrist for companies, or will ever involve forbidding government intrusions, remains to be seen. It has no power to award compensation. Individuals cannot enforce the Act directly through the courts. Overall, this Act comprehensively fails Indian citizens and consumers.

However, **all categories of Data Fiduciaries** should restrain their enthusiasm for such a 'business friendly' and 'government friendly' Act, at least temporarily. There are still hurdles that may need to be overcome. The most substantial might be the decision of India's Supreme Court in *Puttaswamy.* If the constitutional requirements it sets out for protection of privacy (including data protection), implied by India's Constitution, become a means of

interpreting this law, it could upset any of the protections given to the various classes of data fiduciaries discussed above.

With a national election soon, this 'business friendly' Act is no doubt convenient for Modi's 'backsliding democracy'.[26] How strong it will be in advancing the interests of each of these parties – and of India's overall national interests – will take some time to play out.

Information: Graham Greenleaf is Professor of Law & Information Systems at UNSW Sydney and Asia-Pacific Editor of this journal. Valuable comments concerning this article have been received from Malavika Raghavan (LSE), David Erdos (University of Cambridge), Anubhutie Singh (Dvara Research), Ralf Sauer (European Commission) Shohini Sengupta (Jindal Global University), and Elizabeth Coombes (University of Malta), but all responsibility for content remains with the author.

[26] 'The Guardian view on India's G20 summit: a backsliding democracy gets to play host' *The Guardian* 6 September 2023 <https://www.theguardian.com/commentisfree/2023/sep/06/the-guardian-view-on-indias-g20-summit-a-backsliding-democracy-gets-to-play-host?CMP=Share_iOSApp_Other>