# India's Personal Data Protection Act, 2018: Comparison with the General Data Protection Regulation and the California Consumer Privacy Act of 2018†

by Lothar Determann and Chetan Gupta*



* Lothar Determann and Chetan Gupta practice law at Baker & McKenzie LLP in Palo Alto and advise clients on data privacy. Chetan Gupta is admitted to the bar in California and India. Lothar Determann is admitted to the bar in California and Germany; he is also the author of DETERMANN'S FIELD GUIDE TO PRIVACY LAW (3d ed. 2017) and CALIFORNIA PRIVACY LAW: PRACTICAL GUIDE AND COMMENTARY, U.S. FEDERAL AND STATE LAW (3d ed. 2018). The views expressed in this article are those of the authors and not necessarily those of Baker & McKenzie LLP or its clients.

*2018 was a big year for data privacy and data processing regulation. On July 27, 2018, India published a draft bill for a new, comprehensive data protection law to be called the Personal Data Protection Act, 2018—only a few weeks after the European Union General Data Protection Regulation (GDPR) took effect and California enacted the California Consumer Privacy Act of 2018 (CCPA). Brazil followed with a new general data protection law (Lei Geral de Proteção de Dados Pessoais, Law No. 13,709/2018) only a few weeks later. In this Article, we review the history and political context of the Indian Personal Data Protection Act, summarize its key provisions, and compare the Act to the GDPR and the CCPA.*

*With the new law, the Indian government was responding to a mandate from the Indian Supreme Court, which directed the government of India to enact comprehensive data protection legislation in August 2017. India does not currently have an omnibus data protection regulation scheme like Europe or detailed sectoral privacy laws like the United States. Once enacted, the Personal Data Protection Act will therefore represent a monumental shift.*

*The Personal Data Protection Act adopts and further develops many existing principles of European Union data processing regulation and some aspects of US data privacy laws. In the interest of efficiency, global companies can and should try to address the requirements of the new Indian Data Protection Law, the GDPR, the California Consumer Privacy Act, and other privacy regimes simultaneously and holistically. But it is also clear that companies cannot just expand the coverage of their GDPR-focused compliance measures to India without addressing the nuances of the new Indian Personal Data Protection Act and the many differences between that Act and other jurisdictions' data processing regulations and data privacy laws.*

*It is noteworthy that India is not maintaining its status quo, pursuing lighter regulation, or following the US approach of sectoral, harm-specific protections for individual privacy. Instead, India is leaning heavily toward the European model of restrictive data processing regulation. This shift could well affect India's globally leading information technology sector.*

## INTRODUCTION

2018 was a big year for regulation around data privacy and data processing. On July 27, 2018, India published a draft bill for a new, comprehensive data protection law to be called the Personal Data Protection Act, 2018 [1]—only a few weeks after the European Union General Data Protection Regulation (GDPR)[2] took effect[3] and California enacted the California Consumer Privacy Act of 2018 (CCPA), which goes into effect on January 1, 2020.[4] Brazil followed with a new general data protection law only a few weeks later.[5]

According to Chapter 1, Section 1 of India's Personal Data Protection Act, the Act "extends to the whole of India."[6] In fact, the Act extends much further. It also applies worldwide to companies outside of India.[7] It includes many of the requirements contained in the GDPR and the CCPA, and it also introduces a broad data residency requirement[8] (i.e., a requirement that a copy of data processed subject to the law be stored in India) similar to the requirement that Russia enacted in 2015.[9]

With this new law, the Indian government responded to a mandate from the Indian Supreme Court, which directed the government of India to enact comprehensive data protection legislation in August 2017. In this Article, we review the history and political context of the Personal Data Protection Act,

---

[1] Personal Data Protection Act § 1(1) (2018), http://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill%2C2018_0.pdf (last visited Nov. 2, 2019). This is the title of the new law, which is currently a "bill" until it is signed into law, at which point it will become an "act." As the bill is still in draft form, it may change prior to becoming law.

[2] Commission Regulation 2016/679, On the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 2016 O.J. (L 119) 1 [hereinafter GDPR].

[3] CAL. CIV. CODE § 1798.105. *See generally* DETERMANN'S FIELD GUIDE TO PRIVACY LAW, *supra* note *, at ch. 5.04 *et seq*.

[4] *See generally* Lothar Determann, *Analysis: The California Consumer Privacy Act of 2018*, IAPP ADVISOR (Jul. 2, 2018), https://iapp.org/news/a/analysis-the-california-consumer-privacy-act-of-2018/.

[5] Lei Geral de Proteção de Dados Pessoais, Law No. 13,709/2018. *See 10 Things You Need to Know About Brazilian General Data Protection Law*, BAKER MCKENZIE (Dec. 11, 2018), https://www.bakermckenzie.com/en/insight/publications/2018/12/brazilian-general-data-protection-law.

[6] Personal Data Protection Act § 1(2).

[7] *Id*. § 2(2).

[8] *Id*. § 41.

[9] *See* Lothar Determann, Edward Bekeschenko & Vadim Perevalov, *Residency Requirements for Data in Clouds—What Now?*, PRIVACY & SECURITY LAW REPORT (BNA) (Feb. 16, 2015), https://www.bakermckenzie.com/~/media/Files/BDSUploads/Documents/equity%20equation/residency%20requirements%20for%20data%20in%20clouds%20%20what%20now.pdf.

summarize key rules, and suggest action items that businesses should consider if they have any nexus to India, such as customers, suppliers, employees, data centers, a subsidiary, or any other presence in India.

## I. PRIVACY AND ARTICLE 21 OF THE INDIAN CONSTITUTION

On August 24, 2017, a nine-judge bench[10] of the Indian Supreme Court directed the government of India to enact a robust and comprehensive data privacy law.[11] In *Justice K. S. Puttaswamy (Retd.) v. Union of India and Others*, the Court held that the Indian Constitution treats the right to privacy as a fundamental right.[12] Although the Constitution does not expressly mention the right to privacy, the Supreme Court ruled that privacy is enshrined in Article 21, which grants the right to "life and personal liberty."[13] The Court opined that privacy permits an individual to lead a life of dignity, without which the right to life and personal liberty would be meaningless.[14]

### *A. International Precedent: Census Act Decision by the German Constitutional Court*

With its interpretative approach in *Justice K.S. Puttaswamy*, the Indian Supreme Court followed a 1983 decision by the German Constitutional Court, which identified a fundamental right to self-determination with respect to personal information and privacy in Articles 1 and 2 of the German Constitution.[15] Like the constitutions of India and the United States, the German Constitution references dignity in its catalogue of civil rights, but does not expressly grant a

---

[10] It is rare for the Indian Supreme Court to form a nine-judge bench, and such benches are only formed to decide particularly important questions of law where there is a conflict between smaller benches of the Supreme Court. Under the Indian Constitution, a minimum of five judges must decide "substantial questions of law" relating to the interpretation of the Constitution. INDIA CONST. (1950) art. 145(3). In this case, the nine-judge bench was formed to decide whether the right to privacy is a fundamental right under the Constitution. The government argued that previous five-judge benches of the Supreme Court had issued conflicting precedents as to whether privacy is a fundamental right under the Constitution, which can only be interfered with on specified grounds, or whether it is a (relatively weaker) legal right.

[11] Justice K.S. Puttaswamy (Retd.) v. Union Of India And Others, (2017) 10 SCC 1, Part T(H) (India) https://indiankanoon.org/doc/91938676/ (last visited Oct. 7, 2019).

[12] *Id*. at Part T(C).

[13] *Id*.; *see also* INDIA CONST. (1950) art. 21.

[14] *Id*. at Part T(F).The Indian Supreme Court also maintained that the right to privacy was inherent to the meaningful enjoyment of aspects of some other rights under the Indian Constitution, such as the right to freedom under Article 19, the right to equality under Article 14, and the right to freedom of religion under Article 25. For example, the Court stated that the right to freedom of religion includes the privacy-dependent right to decide whether to share one's religious identity and beliefs with others.

[15] *See* Bundesverfassungsgericht [BVerfGE] (Federal Constitutional Court], 1 BvR 209/83, Dec. 15, 1983, https://www.bundesverfassungsgericht.de/e/rs19831215_1bvr020983.html, *translation at* https://freiheitsfoo.de/census-act/.

right to privacy.[16] This is unlike, for example, the California Constitution, since Californians added an express right to privacy to their State Constitution in 1972 by way of a ballot initiative.[17]

When the German government sought to significantly expand the reach of personal data collection in connection with a nationwide census, the German Constitutional Court stepped in to protect individual privacy with a newly developed constitutional right to information self-determination. This decision was rendered a few days before the beginning of 1984, the year for which George Orwell had predicted a totalitarian surveillance state in his novel *1984*—a prediction that Germans took particularly seriously, given their own horrible experiences with totalitarian regimes.[18]

Although the Indian and German courts reached similar conclusions, their approaches retain significant differences. Unlike the Indian Supreme Court, the German Constitutional Court did not have to direct the German legislature to enact privacy laws.[19] In 1983, when the German Constitutional Court affirmed a constitutional right to privacy, the German Legislature had already passed robust data protection laws at both the state and federal levels.[20] The German Constitutional Court had to decide on the validity of a statute, the German Census Act of 1983.[21] By comparison, India had enacted relatively few data privacy laws before 2018.[22] Moreover, unlike the German Constitutional Court, the Indian Supreme Court was not dealing with a nationwide census, but with a further-reaching data processing program: Aadhaar. The Aadhaar program, which was the subject matter of the Supreme Court's decision, is significant owing to its proposed scope and impact on the daily lives of Indian citizens.

### *B. Aadhaar Program in India*

With the Aadhaar program, the government of India is building a nationwide database with biometric information. Citizens must have an Aadhaar ID card to

---

[16] *See* GRUNDGESETZ [GG] [Basic Law] art. 1, 2, *translation* at http://www.gesetze-im-internet.de/englisch_gg/index.html.
[17] *See* J. Clark Kelso, *California's Constitutional Right to Privacy*, 19 PEPP. L. REV. 328 (1992).
[18] When the German State of Hessen enacted the world's first data protection law in 1970, Governor Albert Osswald declared that its purpose was to prevent the Orwellian vision of a totalitarian surveillance state. *See EDV im Odenwald*, DER SPIEGEL, Oct. 5, 1971, at 88, http://www.spiegel.de/spiegel/print/d-43176393.html.
[19] *See Justice K.S. Puttaswamy*, 10 SCC at Part T(H).
[20] Hessen enacted the first data protection law in 1970. Other states followed. In 1978, the federal parliament enacted the first Federal Data Protection Act (BDSG). [Act to Adapt Data Protection Law to Regulation (EU) 2016/679 and to Implement Directive (EU) 2016/680], Jun. 30, 2017 (Ger.), https://iapp.org/resources/article/the-german-act-to-adapt-data-protection-law-to-regulation-eu-2016679-and-to-implement-directive-eu-2016680-english/.
[21] *See* BVerfGE, 1 BvR 209/83, Headnote 4, *translation at* https://freiheitsfoo.de/census-act/.
[22] *See infra* Part II.

access to various public and private services, including driver's licenses, bank accounts, and phone connections.[23]

The Indian government views Aadhaar as a tool to broaden social and financial inclusion, ensuring that subsidies and services reach their intended recipients while eliminating corruption-linked leakages worth about $10 billion.[24] India's Minister of Law, Justice, Electronics and Information Technology, Ravi Shankar Prasad, promoted both the Aadhaar program and India's new Personal Data Protection Act at a town hall and panel discussion in Palo Alto, California in August 2018, which was hosted by the US-India Business Council and the Hewlett Foundation. Minister Prasad presented alongside Justice Cuéllar of the California Supreme Court; Raj Sabhlok, President of Zoho Corporation; and Lothar Determann, one of the authors of this Article.[25] Minister Prasad emphasized that the Aadhaar program enables female empowerment and corrects social imbalances by delivering services and resources to traditionally marginalized sectors of society.[26] He held up an Aadhaar ID card as he vouched for data security and emphasized the importance of the program for welfare, innovation, justice, and the economy in India.[27] Minister Prasad noted that privacy and innovation have to be balanced and listed five principles as key governmental

---

[23] *See* Preeti Motiani, *Four Aadhaar linking deadlines you should not miss*, ECONOMIC TIMES (Dec. 2, 2017, 5:11 PM), https://economictimes.indiatimes.com/wealth/personal-finance-news/four-aadhaar-linking-deadlines-you-should-not-miss/articleshow/60478187.cms; *see also* Press Trust of India, *Aadhaar-driving licence linking to be mandatory soon: Ravi Shankar Prasad* INDIA TODAY (Jan. 6, 2019), https://www.indiatoday.in/india/story/govt-to-make-aadhaar-driving-licence-linking-mandatory-ravi-shankar-prasad-1424739-2019-01-06.

[24] *See JAM trinity helped government save $10 billion leak: Modi*, GULF NEWS (Nov. 23, 2017, 2:43 PM), https://gulfnews.com/business/economy/jam-trinity-helped-government-save-10-billion-leak-modi-1.2129377; *see also* Ravi Shankar Prasad, *Core Biometrics Under Aadhaar Safe, Savings of Rs 90,000*, HINDUSTAN TIMES (Aug. 3, 2018); *see also* Press Trust of India, *Jan Dhan, Aadhaar, mobile ushered in a social revolution: Jaitley*, HINDUSTAN TIMES (Aug. 27, 2017, 1:55 PM), https://www.hindustantimes.com/business-news/jan-dhan-aadhaar-mobile-ushered-in-a-social-revolution-jaitley/story-5itVdxDEuDMtdnc42YClpO.html; Ajay Bhushan Pandey, *Criticism without Aadhaar:*
*The unique identification number empowers the people, not the state,* INDIAN EXPRESS (May 13, 2017, 1:42 AM), https://indianexpress.com/article/opinion/columns/criticism-without-aadhaar-4653369/.

[25] *See* Ritu Jha, *India's digital data debated at town hall*, INDICA NEWS (Aug. 29, 2018), https://indicanews.com/2018/08/29/indias-digital-data-debated-at-town-hall/. Minister Prasad was in California to meet with tech leaders and discuss data privacy and security issues. *See also* PTI, *Need to work together to better manage challenges like data privacy security issues*, ECONOMIC TIMES (Aug. 28, 2018, 9:37 PM), https://economictimes.indiatimes.com/news/economy/policy/need-to-work-together-to-better-manage-challenges-like-data-privacy-security-issues-ravi-shankar-prasad/articleshow/65583364.cms.

[26] Ravi Shankar Prasad, Minister, Law, Justice, Electronics and Information Technology, Promoting Digital India and Economic Growth, Address at USIBC and William and Flora Hewlett Foundation Town Hall Discussion (August 27, 2018).

[27] *Id*.

policy objectives regarding personal data: availability, innovation, usability, anonymity, and privacy.[28]

Critics of the Aadhaar program view the program as a tool for large-scale State surveillance and complain about inadequate privacy protections.[29] While India already has various identity cards and numbers—including tax identification numbers, driver licenses, and identity cards for voting in elections—citizens have not historically needed to provide this identification to receive services, nor have these databases been interlinked with other systems as the government proposes to do with Aadhaar.[30]

The Aadhaar program was initially implemented through an executive order establishing the Unique Identification Authority of India, which had the responsibility of setting up the Aadhaar program.[31] Retired Justice K.S. Puttaswamy and thirty additional petitioners—including prominent Indian activists, such as Aruna Roy, civil rights organizations, such as the Centre for Civil Society, and sitting members of the Indian Parliament[32]—filed constitutional challenges in the Indian Supreme Court, complaining that Aadhaar was being implemented through executive action without a fundamental debate about privacy implications in the Indian Parliament, even though the program could have a significant impact on the privacy of Indian citizens.[33] These petitions were ultimately combined into a single case: *Justice K. S. Puttaswamy (Retd.) v. Union of India and Others*.

While *Justice K.S. Puttaswamy* was pending, the Indian government enacted a law regulating the Aadhar program, the Aadhaar (Targeted Delivery of Financial

---

[28] *See Fine balance must for data availability, innovation and privacy: IT Minister Ravi Shankar Prasad*, ECONOMIC TIMES TELECOM (Apr. 19, 2018, 2:49 AM), https://telecom.economictimes.indiatimes.com/news/infrastructure/telecom-equipment/fine-balance-must-for-data-availability-innovation-and-privacy-it-minister-ravi-shankar-prasad/63829583.

[29] *See* Jean Dreze, *Dissent and Aadhaar*, INDIAN EXPRESS (May 8, 2017, 10:37 AM), https://indianexpress.com/article/opinion/columns/dissent-and-aadhaar-4645231/; *see also* Rahul Bhatia, *Critics of Aadhaar Project Say They Have Been Harassed, Put Under Surveillance*, REUTERS INDIA (Feb. 12, 2018, 9:41 PM), https://in.reuters.com/article/india-aadhaar-breach/critics-of-aadhaar-project-say-they-have-been-harassed-put-under-surveillance-idINKBN1FX0FU; Reetika Khera, *Why'India's Big Fix is a Big Flub*, N.Y. TIMES (Jan. 21, 2018), https://www.nytimes.com/2018/01/21/opinion/india-aadhaar-biometric-id.html.

[30] *See* Asheeta Regidi, *Aadhaar Hearing: Petitioners Argue For A Voluntary ID Card System That Does Not Collect User Data,* TECH2 (May 11, 2018, 10:39 AM), https://www.firstpost.com/tech/news-analysis/aadhaar-hearing-petitioners-argue-for-a-voluntary-id-card-system-that-does-not-collect-user-data-4343721.html.

[31] *See Journey of Aadhaar*, Software Freedom Law Center (May 21, 2016, 1:22 PM), https://sflc.in/journey-aadhaar.

[32] *See* Anoo Bhuyan, Aadhaar Isn't Just About Privacy. There Are 30 Challenges the Govt Is Facing in Supreme Court, THE WIRE (Jan. 18, 2018), https://thewire.in/government/aadhaar-privacy-government-supreme-court.

[33] *See* T. A. Johnson, *Right to Privacy: 91-year-old Retd Justice KS Puttaswamy Is the Face Behind Legal History*, INDIAN EXPRESS (Aug. 25, 2017, 12:18 PM), https://indianexpress.com/article/india/right-to-privacy-justice-k-s-puttaswamy-retd-vs-union-of-india-91-year-old-judge-is-the-face-behind-legal-history-4812440/.

and Other Subsidies, Benefits and Services) Act, 2016, which contained provisions relating to the security and privacy of identity information collected for Aadhaar.[34] But the 2016 law did not sway the Supreme Court. The Court found a fundamental right to privacy in the Constitution and directed the government of India to enact comprehensive data privacy legislation.[35]

### *C. Identifying a Fundamental Right to Privacy Under Article 21 of the Indian Constitution*

In *Justice K. S. Puttaswamy*, which was heard by a nine-judge bench, the government asserted that privacy was not a fundamental right, citing precedent from smaller benches of the Indian Supreme Court.[36] The Supreme Court overruled conflicting precedent and decided against the government, unanimously holding that privacy is a fundamental right under the Indian Constitution.[37]

The fact that the Indian Supreme Court anchored the right to privacy in Article 21 of the Constitution is significant because Article 21 deals with the fundamental right to life and personal liberty, and this right enjoys heightened protection under the Indian constitutional scheme.[38] The right to life and personal liberty must not be interfered with, except in accordance with a law that meets the constitutional test of reasonableness and satisfies three requirements: (1) the intrusion must be sanctioned by a statute or other formal law that was enacted in accordance with all formal requirements of the Indian Constitution,[39] (2) the intrusion must be necessary for legitimate government purposes, and (3) the intrusion must be proportionate, based on a balancing of the objects of the law and the means adopted to achieve them.[40]

---

[34] *See* Aadhaar (Targeted Delivery of Financial & Other Subsidies, Benefits & Services) Act, No. 19, Acts of Parliament, §§ 28, 29, 33, 2016. https://uidai.gov.in/images/the_aadhaar_act_2016.pdf.

[35] *See* Justice K. S. Puttaswamy (Retd.) v. Union of India and Others, (2017) 10 SCC 1, Part T(H) (India).

[36] *See* M P Sharma v. Satish Chandra, 1954 AIR 300 (Del.); Kharak Singh v. State of Uttar Pradesh, 1963 AIR 1295 (U.P.). These cases were decided by benches of eight and six judges respectively. Both judgments contained observations that the right to privacy was not a fundamental right under the Constitution.

[37] *See Aadhaar update: Supreme Court declines Centre's offer to file panel's report on data protection*, FINANCIAL EXPRESS (Jul. 30, 2018, 6:48 PM), https://www.financialexpress.com/aadhaar-card/aadhaar-update-supreme-court-declines-centres-offer-to-file-panels-report-on-data-protection/1263318/. Interestingly, the Indian Supreme Court declined to take the new Personal Data Protection Act on record when considering the constitutionality of Aadhaar. However, when the Court ultimately ruled on the validity of the Aadhaar program, it cited to and relied on the Personal Data Protection Act to uphold the Aadhaar Act, on the basis that a robust data protection regime would help mitigate any data privacy concerns that may arise under Aadhaar.

[38] *See* INDIA CONST. (1950) art. 21. "Law" is not restricted to Acts of Parliament. INDIA CONST. (1950) art. 13(3) (defining "law" as including "any Ordinance, [executive] order, bye-law, rule, regulation, notification, custom or usage having in the territory of India the force of law").

[40] *See Justice K. S. Puttaswamy* (nine judge bench addressing the fundamental right to privacy).

The Supreme Court applied these tests in a September 2018 ruling on the constitutional validity of the Aadhaar program. In a 1,400-page judgment, a bench of five judges upheld the constitutionality of the Aadhaar program in a four-to-one split.[41] The majority held that the Aadhaar program was constitutionally valid, necessary for the delivery of government services, and proportionate for achieving the government's aims.[42] However, the majority limited the purposes for which Aadhaar data can be used and struck down Section 57 of the Aadhaar Act, which allowed private companies to use Aadhaar data for authentication purposes.[43] Citing German and other European definitions of proportionality, the Court found that Section 57 was not a proportional means of achieving the aim of authenticating identity, and thus represented an unjustified intrusion on the right to privacy.[44]

The dissenting judge, Justice Chandrachud, found the entire Aadhaar Act unconstitutional and disproportionate, holding that the government's stated aim of delivering public services could be achieved by less intrusive means and without building a large-scale biometric database.[45] The contours of the constitutional right to privacy will continue to be defined in subsequent cases.[46]

### *D. Constitutional Right to Privacy Against Companies*

In addition to finding that privacy was a constitutional right, five out of nine judges in *Justice K. S. Puttaswamy* held that the right to privacy applies not only to government action but also to private sector action.[47] Fundamental rights under the Indian Constitution are normally enforceable only against the government, *i.e.*, against State actors.[48] But with *Justice K.S. Puttaswamy*, the Indian Supreme

---

[41] *See* Justice K S Puttaswamy (Retd.) v. Union of India and Others, (2018) 9 SCJ 224 (India) [hereinafter *Aadhar Judgment*] (five judge bench addressing the validity of the Aadhaar program), https://indiankanoon.org/doc/127517806/.

[42] *Id.* ¶ 447(2).

[43] The decision makes Aadhaar mandatory for those filing Income Tax Returns (ITR) and requires the tax filing Permanent Account Number (PAN) to be linked with Aadhaar numbers. It also makes Aadhaar mandatory for those availing facilities of welfare schemes and government subsidies. However, Aadhaar numbers are no longer required to open a bank account, get phone connections, or be admitted to school.

[44] *Aadhar Judgment*, *supra* note 41, at ¶ 447(4)(h).

[45] *See Aadhar Judgment*, *supra* note 41, separate opinion of Justice Chandrachud ¶ 339.

[46] The Supreme Court has already relied on the newly declared right to "read down" an Indian legal provision criminalizing sexual acts "against the order of nature," holding that the provision would not apply to persons engaging in homosexual relations. A bench of five judges unanimously held that criminalizing homosexual conduct violated the right to privacy and the related rights of self-determination and personal autonomy. Navtej Singh Johar v. Union of India, (2018) 10 SCC 791 (India), https://indiankanoon.org/doc/168671544/.

[47] *See Justice K. S. Puttaswamy*, at Part T(H).

[48] *See* INDIA CONST. (1950) part III, art. 12. Only some rights, such as the right to access public restaurants, shops and hotels on a non-discriminatory basis, can be applied "horizontally" to non-State actors. *See, e.g.*, INDIA CONST. (1950) art. 15(2) (barring discrimination with respect to accessing certain public places).

Court signaled that companies can also be challenged for violations of the constitutional fundamental right to privacy.[49] Major international social networks have already been sued in India under this principle.[50]

By applying constitutional principles to relations and disputes between non-State actors, the Indian Supreme Court increased legal uncertainties for companies, given the relative vagueness of constitutional principles compared to typically more detailed statutes.[51] At the same time, the Court conferred significant powers on the judiciary to create new privacy laws.[52] Perhaps the Court intended such powers only as a temporary measure, given its simultaneous direction to enact privacy legislation.[53] But even after privacy legislation is enacted, Indian courts will retain the power to overrule or reinterpret statutory provisions based on constitutional principles, which could permanently affect the balance of power between the judiciary and legislative branches of the government.[54]

By way of international comparison, the German Constitutional Court has also assumed greater control, for itself and for lower courts, over rights and disputes between non-State actors. The German Constitutional Court has emphasized that courts, as State actors, are bound by constitutional provisions regarding civil rights when deciding disputes between non-State actors ("third party effects doctrine").[55] As a result, the German Constitutional Court can overrule interpretations of the German Civil Code and other statutes by other

---

[49] *See Justice K. S. Puttaswamy*, at Part T(H). This would allow persons aggrieved by the data privacy practices of private companies to directly approach the State High Courts under Article 226 of the Indian Constitution and seek injunctive relief or declarations of illegality with respect to the data practices of private companies. The High Courts have sweeping powers to issue directions under Article 226 and could ask companies to modify their data practices or alter their privacy policies, for example. This holding will also make it easier to directly approach the Indian Supreme Court under Article 32 of the Constitution in the form of a "Public Interest Litigation" seeking relief against both State and non-State actors. The Supreme Court has similarly broad powers to grant relief under Article 32. This is likely to lead to an uptick in privacy-related litigation against private companies, since petitioners will find it easier to overcome the burden of proving that they have standing and can easily assert that a private company has violated their fundamental right to privacy. A common approach to filing such cases is to implead both the central government (or one of its agencies, such as the IT Ministry or the Telecom Regulatory Authority) and the private companies in question.

[50] *See, e.g.*, Amit Anand Choudhary, *Supreme Court asks WhatsApp, Facebook to undertake not to share consumer data with third party*, TIMES OF INDIA (Sept. 6, 2017, 9:10 AM), http://timesofindia.indiatimes.com/articleshow/60396539.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst. These lawsuits are ongoing and may be amended to rely on the Act if it becomes a law while they are pending.

[51] *See e.g.*, Information Technology Act, No. 21 of 2000, INDIA CODE (2005) (consisting of 94 detailed sections, while Article 21 merely expresses a general principle).

[52] *See Justice K. S. Puttaswamy*, at Part T(G), (H).

[53] *Id.*

[54] *Id.*

[55] *See* Lothar Determann, *Kommunikationsfreiheit im Internet: Freiheitsrechte und gesetzliche Beschränkungen* [Freedom of Communications on the Internet: Civil Rights and Statutory Limitations] (1999).

appeals courts of last instance, even though these courts have the same level of judicial authority under the German Constitution.[56] Furthermore, the German Constitutional Court requires lower courts to apply constitutional civil rights guarantees when applying any statute (*i.e.*, constitutional rights always apply when lower courts are interpreting statutes), which arguably results in a shift of power from the legislative branch to the judiciary.[57] Because constitutional rights are based on the courts' interpretation, this effectively gives courts more power to decide what the law means, even in the face of potentially contrary intent by the legislature.

The US Supreme Court, on the other hand, has remained dedicated to the principle that civil rights under the US Constitution can only be enforced against State actors.[58] Therefore, US courts do not apply privacy protections arising under the Fourth, Fifth, or Fourteenth Amendments to disputes between companies and individuals.[59] When US courts apply privacy statutes, they defer to Congress and do not typically consider constitutional privacy principles in the context of interpreting privacy statutes.[60]

California takes a different approach to the constitutional right to privacy, and interprets the right more broadly.[61] In 1994, the California Supreme Court held that the right to privacy in Article 1, Section 1 of the California Constitution applies to private companies, even though other civil rights afforded by the California Constitution generally apply only vis-à-vis state actors.[62] The California Supreme Court made this exception with respect to the State's right to privacy in recognition of a 1972 ballot initiative through which the people of California added a right to privacy to the California Constitution.[63] In practice, the State's constitutional right to privacy did not add any substantive rules or prohibitions to the already robust and detailed body of California privacy law.[64] However, the California Supreme Court's recognition that the State's constitutional right to privacy is applicable between private persons and entities has allowed plaintiffs to add vague claims based on the broad right to privacy

---

[56] *See* Lothar Determann and Markus Heintzen, *Constitutional Review of Statutes in Germany and the United States Compared* 2 (U.C. Hastings Research Paper No. 299, 2018).
[57] *See id*.
[58] *See, e.g.*, DeShaney v. Winnebago County, 489 U.S. 189 (1989) (holding that a state government agency's failure to prevent child abuse by a custodial parent does not violate the'child's right to liberty for the purposes of the Fourteenth Amendment to the U.S. Constitution, as the abuse was committed by the'child's parent, who was "ot a "State" actor).
[59] *See* Hill v. Nat'l Collegiate Athletic Assn., 865 P.2d 633, 641–44 (1994).
[60] *See* Orin S. Kerr, *The Effects of Legislation on Fourth Amendment Protection*, 115 Mich. L. Rev. 1117, 1125-1127 (2017).
[61] *See Hill v. Nat'l Collegiate Athletic Assn.*, 865 P.2d at 642–44.
[62] *See id*. Californian voters added an express right to privacy to the California Constitution in 1972 by way of a ballot initiative. *See generally* Determann, CALIFORNIA PRIVACY LAW: PRACTICAL GUIDE AND COMMENTARY, U.S. FEDERAL AND STATE LAW, *supra* note *.
[63] *See* Kelso, *supra* note 17, at 328.
[64] Determann, CALIFORNIA PRIVACY LAW: PRACTICAL GUIDE AND COMMENTARY, U.S. FEDERAL AND STATE LAW, *supra* note *, at Ch. 2–2:3.

under the California Constitution, which lacks substantive rules pertaining to privacy. Defendants struggle to get these claims dismissed during the early stages of litigation, thereby strengthening class action plaintiffs and imposing greater settlement costs on businesses.[65] Because the Indian Supreme Court adopted a similarly broad definition of privacy, similar results can be expected for Indian litigation based on *Justice K. S. Puttaswamy*.[66]

### *E. Judicial Directive to the Indian Legislature to Enact Data Privacy Law*

In *Justice K.S. Puttaswamy*, the Supreme Court of India directed[67] the central government to propose a comprehensive data protection law in order to create a legislative framework protecting the constitutional right to privacy from interference.[68] In response, the government set up the Srikrishna Committee, which was headed by retired Indian Supreme Court Justice Srikrishna and consisted of six government members and three industry representatives.[69] The Srikrishna Committee prepared the draft bill for the 24,000-word Personal Data Protection Act; the word count fell between the operative segment of the GDPR (about 30,000 words) and the California Consumer Privacy Act (about 10,000 words). The Srikrishna Committee also produced a 213-page explanatory report

---

[65] *See* Helen Trac, *Six Modern Technology Cases Involving the California Constitutional Right to Privacy*, PRIVACY & DATA SECURITY LAW REPORT (BNA) (Nov. 7, 2016) (discussing *In re Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125 (3d Cir. 2015); *In re Yahoo Mail Litig.*, No. 5:13-cv-04980-LHK, 2016 WL 4474612 (N.D. Cal. Mar. 15, 2016) (order granting motion for final approval of class action settlement); *Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010 (N.D. Cal. 2012); *Goodman v. HTC Am., Inc.*, No. C11-179MJP, 2012 WL 2412070 (W.D. Wash. June 26, 2012); *Cahen v. Toyota Motor Corp.*, 147 F. Supp. 3d 955 (N.D. Cal. 2015); *In re Carrier IQ, Inc.*, 78 F. Supp. 3d 1051 (N.D. Cal. 2015)).

[66] *See Justice K. S. Puttaswam*y.

[67] This is an interesting feature of the modern Indian political system and its separation of powers. Since the 1970s, the Indian Supreme Court has been increasingly active in passing far-ranging directions to the legislature or executive and "finding" or incorporating new rights into existing rights under the Indian Constitution. Sometimes the Court passes these directions on the basis of letters written to the it. *See, e.g.*, People's Union for Democratic Rights and Others v. Union of India and Others, (1982) 3 SCC 235 (India), where on the basis of a letter, the Supreme Court construed the violation of labor laws as a violation of fundamental rights and directed the executive to remedy them. Similarly, for more than two decades, the Supreme Court has heard petitions relating to deforestation in various parts of India on a weekly basis and directed the government to remedy violations. *See* P.K. Manohar and Praveen Bhargav, *The architect of an omnibus forest-protection case*, THE HINDU (Jul. 5, 2016, 12:25 AM), https://www.thehindu.com/opinion/open-page/The-architect-of-an-omnibus-forest-protection-case/article14470903.ece. While alien to the US legal system, other jurisdictions such as South Africa have also seen their constitutional courts play a more active policy role. In *Minister of Health & Others v. Treatment Action Campaign & Others* (No. 2) (2002) 5 SA 721 (S. Afr.), the South African Constitutional Court directed the South African government to provide access to a particular antiretroviral drug to prevent the transmission of HIV from mothers to children.

[68] *See Justice K. S. Puttaswamy*, at Part T(H).

[69] *See* Surabhi Agarwal, *Justice BN Srikrishna to head Committee for data protection framework*, ECONOMIC TIMES (Aug. 1, 2017, 7:32 PM), https://economictimes.indiatimes.com/news/politics-and-nation/justice-bn-srikrishna-to-head-committee-for-data-protection-framework/articleshow/59866006.cms.

titled *A Free and Fair Digital Economy, Protecting Privacy, Empowering Indians* (the "Srikrishna Report").[70]

The draft Personal Data Protection Act currently awaits approval by the Ministry of Electronics and Information Technology, under the leadership of Minster Ravi Shankar Prasad, and by the Union Cabinet, as well as subsequent debate and approval by the legislature. At the panel discussion in Palo Alto (*see supra*, Section I, Part 3), Minister Prasad emphasized that the Personal Data Protection Act is still in draft form and could see changes before it is enacted.[71] Minister Prasad also encouraged all stakeholders to share their views on the draft Personal Data Protection Act.[72]

## II. CURRENT STATE OF INDIAN DATA PRIVACY LAW

India has never had omnibus data protection regulations like Europe or detailed sectoral privacy laws like the United States.[73] This state of affairs will continue until the Personal Data Protection Act becomes effective. Currently, Indian privacy law consists of the following elements:

### *A. Constitutional and Common Law Protections*

According to *Justice K.S. Puttaswamy*,[74] Indians enjoy a fundamental right to privacy under Article 21 of the Constitution against both State and non-State actors.[75] However, courts have not yet developed the exact contours of this recently enumerated right.[76] Privacy protections under tort laws are more established,[77] including protections that follow from English common law regarding nuisance, trespass, harassment, defamation, malicious falsehood, and

---

[70] COMMITTEE OF EXPERTS UNDER THE CHAIRMANSHIP OF JUSTICE B.N. SRIKRISHNA, A FREE AND FAIR DIGITAL ECONOMY: PROTECTING PRIVACY, EMPOWERING INDIANS (2018) [hereinafter Srikrishna Report], *available* at https://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report-comp.pdf.

[71] *See* Jha, *supra* note 25; *see also* PTI, *supra* note 25.

[72] *See* PTI, *supra* note 25.

[73] For an overview of US privacy laws, see Determann, CALIFORNIA PRIVACY LAW: PRACTICAL GUIDE AND COMMENTARY, U.S. FEDERAL AND STATE LAW, *supra* note 1 at ch. 1.

[74] *Justice K. S. Puttaswamy*, at Part T.

[75] *Id*. at Part T(C), T(H).

[76] *See, e.g.*, *id*. at Part T, Conclusion G, stating that "This Court has not embarked upon an exhaustive enumeration or a catalogue of entitlements or interests comprised in the right to privacy. The Constitution must evolve with the felt necessities of time to meet the challenges thrown up in a democratic order governed by the rule of law. The meaning of the Constitution cannot be frozen on the perspectives present when it was adopted. Technological change has given rise to concerns which were not present seven decades ago and the rapid growth of technology may render obsolescent many notions of the present. Hence the interpretation of the Constitution must be resilient and flexible to allow future generations to adapt its content bearing in mind its basic or essential features…"

[77] *See, e.g.*, PEN. CODE §§ 268, 441, https://indiacode.nic.in/handle/123456789/2263?locale=en, (codifying nuisance and trespass, respectively).

breach of confidence.[78] Additionally, certain communications between spouses and with attorneys are privileged and subject to protections against disclosure.[79]

### *B. Existing Statutes*

In addition to unwritten protections, several key pieces of legislation protect specified privacy rights. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 require companies to meet certain criteria when collecting "sensitive" personal data.[80] Companies must appoint a grievance officer and provide a privacy policy, among other requirements.[81] Credit bureaus have to adopt specified "privacy principles" under Section 20 of the Credit Information Companies (Regulation) Act, 2005, including rules relating to the purpose for which credit information may be used and disclosed, as well as rules relating to data protection.[82] The use of information collected for the Aadhaar program is regulated under the Aadhaar Act, which forbids the sharing of biometric information and requires other identity information to be shared and used only for specified purposes.[83]

### *C. Draft Bills*

In addition to the Personal Data Protection Act, India is currently considering several bills that implicate privacy rights. For example, in March 2018, the Indian Health Ministry proposed a new law, the Digital Information Security in Healthcare Act, which would give data subjects "ownership" of their digital health data.[84] In July 2018, the telecom regulator issued recommendations on privacy,

---

[78] However, individuals rarely use these actions owing to long delays in the civil litigation process. For defamation, which is also a criminal offence under PEN. CODE § 499, individuals often choose to initiate criminal proceedings as a pressure tactic instead. *See* Chinmayi Arun, *A Question of Power*, INDIAN EXPRESS (May 25, 2016, 12:01 AM), https://indianexpress.com/article/opinion/columns/criminal-defamation-law-supreme-court-2817406/.

[79] Indian Evidence Act, No. 1 of 1872, INDIA CODE (1993) §§ 122, 126, https://indiacode.nic.in/handle/123456789/2188?view_type=browse&sam_handle=123456789/1362 (marital communications and attorney-client privilege, respectively)

[80] *See* Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Gazette of India, pt. III sec. 4 (Apr. 11, 2011), Rule 4 (privacy policy requirement), Rule 5(1) (requirement to obtain consent before collection of sensitive personal information), and Rule 5(9) (appointment of a grievance officer).

[81] *Id.*

[82] *See* Credit Information Companies (Regulation) Act, No. 30 of 2005, INDIA CODE (1993) § 20.

[83] *See* Aadhaar (Targeted Delivery of Financial & Other Subsidies, Benefits & Services) Act, No. 18 of 2016, INDIA CODE (1993) § 29.

[84] *See* Digital Information Security in Healthcare Act §§ 2(j), 31 (2018), https://mohfw.gov.in/newshighlights/comments-draft-digital-information-security-health-care-actdisha. Under this proposed law, "owners," similar to data subjects under the GDPR, are granted a number of rights with respect to their digital health data, including the right to privacy, confidentiality, and security, and the right to refuse or withdraw consent with respect to the storage and transmission of their health data (§ 20). Entities which have custody of health data are required

security and ownership of data in the telecom sector, which seek to impose consumer data protection requirements on "entities in the digital ecosystem" through telecom rules or licensing conditions.[85]

### *D. Data Residency Requirements*

In April 2018, the Reserve Bank of India issued a notification requiring all payment system operators to store data locally in India.[86] This effectively serves as a precursor to the data residency requirement in the new Personal Data Protection Act by requiring payment related data to be resident in India.[87] However, it does not seem intended or suited to protect individual privacy; rather, it serves to secure access to data for the Indian government.[88]

### *E. Preemptive Effect of Personal Data Protection Act*

Section 110 of the Personal Data Protection Act gives the Act overriding effect to the extent it is inconsistent with existing law.[89] The Personal Data Protection Act states that it will override the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 but does not enumerate any other existing laws that it supersedes or replaces.[90] The Srikrishna Report accompanying the Personal Data Protection Act lists fifty different laws, including the Aadhaar Act, that may be impacted by the Personal Data Protection Act and recommends that the respective ministries

---

to inform owners of data breaches and can be penalized for those breaches (§§ 35(5), 37-39). The concept of ownership of data may, however, be a misnomer. Some data protection authorities in the EU, as well as legal commentators, like to encourage the idea that natural persons "own" personal data relating to them, with the exception of exclusion rights. However, data protection and privacy laws diverge from property laws. Unlike property laws, privacy laws do not incentivize or reward creation or investment, do not regulate the acquisition or transfer of ownership rights to others, and do not apply against everyone. *See generally* Lothar Determann, *No One Owns Data* (UC Hastings, Working Paper No. 265, 2018), https://ssrn.com/abstract=3123957 (discussing why claims of ownership are inappropriate in the context of data, and how the US and European legal systems typically address rights with respect to data).

[85] *See* Press Release, Telecom Regulatory Authority of India, Recommendations on Privacy, Security and Ownership of Data in the Telecom Sector (Jul. 16, 2018), https://www.trai.gov.in/sites/default/files/PRNo7816072018.pdf.

[86] *See* RESERVE BANK OF INDIA NOTIFICATION, STORAGE OF PAYMENT SYSTEM DATA (2018), https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=11244&Mode=0.

[87] *Id*.

[88] *Id*. The Reserve Bank of India explains the rationale of the notice as follows: "In order to ensure better monitoring, it is important to have unfettered supervisory access to data stored with these system providers as also with their service providers/intermediaries/third party vendors and other entities in the payment ecosystem." See Lothar Determann, *Data Residency Rules Cutting Into Clouds: Impact and Options for Global Businesses and IT Architectures*, BLOOMBERG BNA PRIVACY & SECURITY LAW REPORT (Apr. 3, 2017), for an analysis of the impact of recent data residency laws in other jurisdictions such as Russia, Germany, Indonesia and China.

[89] Personal Data Protection Act § 110.

[90] Personal Data Protection Act § 111, First Schedule.

amend these laws as necessary.[91] Amending all of the laws identified in the Srikrishna Report is a tall order and will likely spawn litigation over whether existing legislation is inconsistent with the Personal Data Protection Act, the extent of any inconsistencies, and whether the Personal Data Protection Act completely supersedes the existing legislation. For example, if businesses comply with the data residency requirements of the Personal Data Protection Act by storing a copy of personal data in India, are they still required to comply with the Reserve Bank of India's data residency requirements by storing personal data related to payment processing *only* in India (and nowhere else)?

## III. TERMINOLOGY OF THE PERSONAL DATA PROTECTION ACT

Like the GDPR, the Personal Data Protection Act uses the term "data processors" to refer to entities that process data on the instructions of a data controller and do not independently determine the means and purposes of data processing. However, where the GDPR refers to data "controllers," the Act refers to "data fiduciaries," and where the GDPR refers to "data subjects," the Act refers to "data principals."[92] Like data controllers under the GDPR, data fiduciaries are responsible for their own data processing activities, as well as the activities of data processors.[93] The drafters of the new Indian law chose this modified terminology to emphasize that the individual data subjects entrust their data to companies and other controllers, which therefore have a fiduciary duty of care towards those subjects.[94] In the remainder of this Article, we use the more commonly used terms "data controller" and "data subject" in place of "data fiduciary" and "data principal."

"Personal data" is defined as broadly under the Personal Data Protection Act as under the GDPR. Personal data means any data about or relating to a natural person who is directly or indirectly identifiable.[95] "Sensitive personal data"[96] receives heightened protections and "irreversibly" anonymized[97] data is excluded from protection.

---

[91] *See* Srikrishna Report, *supra* note 70, at Annexure C.
[92] *See* Personal Data Protection Act § 3; GDPR, *supra* note 3, art. 4.
[93] Personal Data Protection Act § 11.
[94] *See* Srikrishna Report, *supra* note 70, at 7–10.
[95] Personal Data Protection Act § 3(29).
[96] *See id*. § 3(35) ("'Sensitive Personal Data' means personal data revealing, related to, or constituting, as may be applicable: (i) passwords; (ii) financial data; (iii) health data; (iv) official identifier; (v) sex life; (vi) sexual orientation; (vii) biometric data; (viii) genetic data; (ix) transgender status; (x) intersex status; (xi) caste or tribe; (xii) religious or political belief or affiliation; or (xiii) any other category of data specified by the Data Protection Authority under the Act.").
[97] *See id*. § 3(3) ("'Anonymisation' in relation to personal data means the irreversible process of transforming or converting personal data to a form in which a data subject cannot be identified, meeting the standards specified by the [Data Protection] Authority [to be established under the Act by the Indian Government].").

## IV. ENTITIES AND DATA PROTECTED UNDER THE PERSONAL DATA PROTECTION ACT

The Personal Data Protection Act protects all individual persons worldwide if and to the extent that their personal data is processed on Indian territory.[98] Indian residents are also protected when their personal data is processed outside India if processing occurs (i) in connection with business carried out in India, (ii) systematic offering of goods or services to data subjects in India, or (iii) activity which involves profiling of Indian data subjects (e.g., building a data profile of Indian data subjects based on their browsing activity).[99]

## V. ENTITIES AFFECTED BY THE PERSONAL DATA PROTECTION ACT

Any company anywhere in the world must comply with the Personal Data Protection Act to the extent that the company in question processes personal data on Indian territory, including with the help of a data processor in India, offers goods or services to data subjects in India, or profiles Indian residents remotely.[100]

Any Indian company that processes personal data belonging to an Indian or a foreign data subject must likewise comply.[101] The Personal Data Protection Act applies to the processing of all personal data collected, disclosed, shared, or otherwise processed within India.[102] Since the definition of "processing" includes mere storage, the Personal Data Protection Act's requirements apply to the personal data of any foreign data subjects if that data was stored or otherwise processed in India.[103] Therefore, any outsourcing operation that transfers foreign personal data to India will be covered by the Personal Data Protection Act and will have to comply with the Act's requirements.[104] The Indian government has the discretion to exempt data processing related to foreign data subjects in an outsourcing context from obligations under the Personal Data Protection Act, but it remains to be seen whether the government will actually exempt such data processing from substantive compliance obligations.[105]

Any foreign data controller or data processor outside India will have to comply with the Personal Data Protection Act if that company processes personal data in connection with business carried out in India, a systematic offering of

---

[98] *See id*. § 2(1).
[99] *See id*. § 2(2).
[100] *See id*. §§ 2(1)-(2).
[101] *See id*. § 2(1).
[102] *See id*.
[103] *See id*. § 3(32) ("'Processing' in relation to personal data, means an operation or set of operations performed on personal data, and may include operations such as collection, recording, organisation, structuring, storage, adaption, alteration, retrieval, use, alignment or combination, indexing, disclosure by transmission, dissemination or otherwise making available, restricting, erasure or destruction.").
[104] *See id*. §§ 2(1), 3(2).
[105] *See id*. § 104.

goods or services to Indian residents, or activity involving the profiling of Indian residents.[106] This sweeps in almost any foreign company with an Indian connection, such as a company that offers goods or services to Indian residents online. Providers of global apps will also be covered, since they profile persons in India.[107] However, a foreign company that only processes the personal data of foreign data subjects collected abroad, without any other nexus or connection to India, will not have to comply with the Personal Data Protection Act.

## VII. COMPLYING WITH THE PERSONAL DATA PROTECTION ACT

Under the Personal Data Protection Act, companies have to address a series of requirements similar to those established by the GDPR, which include the following:

### *A. Identifying a Basis for Processing Data*

Data controllers must provide a lawful processing basis for both personal and sensitive personal data.[108] For each category of data, the Personal Data Protection Act specifies permissible bases for data processing (i.e., what the law considers a lawful basis for processing that category of data).[109] Consent is a lawful basis for processing both personal and sensitive personal data (i.e., if someone consents, it is legal to process their data), but heightened information requirements apply for sensitive personal data.[110] In addition, the data subject can withdraw consent,[111] which makes consent an unreliable basis for processing data.

The Personal Data Protection Act also allows companies to process personal data for a purpose "reasonably incidental" to the purpose for which the data was collected.[112] For example, if personal data is collected in connection with a candidate's employment application, it may also be permissible to process the same data to provide employment-related benefits to the subsequently employed candidate. The law also permits processing of personal data for "a reasonable purpose."[113] Some non-exhaustive examples of "reasonable purposes" are data processing for a mergers and acquisitions transaction, for network security

---

[106] *See id*. § 2(2).
[107] *See id*. § 3(33) ("'Profiling' means any form of processing of personal data that analyses or predicts aspects concerning the behavior, attributes or interest of a data principal."). For example, this would include a food delivery app that uses user data to make restaurant suggestions.
[108] *See id*. § 5.
[109] *See id*. §§ 12–17 for personal data, §§ 18–22 for sensitive personal data. The bases for both categories of data also include processing for functions of the State (which would cover Aadhaar), for compliance with law, and to address an emergency situation.
[110] *See id*. §§ 12, 18. Consent has to be free, informed, specific, clear and capable of being withdrawn.
[111] *Id*. § 12(2)(e).
[112] *See id*. § 5(2).
[113] *See id*. § 17.

purposes, or for credit scoring.[114] The Personal Data Protection Act also establishes the Data Protection Authority, which is expected to clarify what these terms mean and what processing they permit.[115]

### *B. Data Subject Notice Requirements*

Data controllers must notify data subjects about the collection and use of personal data.[116] Irrespective of whether data is being collected directly from the data subject, data controllers must provide the subject with information regarding the processing purposes; categories of data collected; the subject's rights, including the right to withdraw consent for processing; the source of the personal data if not collected from the data subject; other data controllers or data processors with whom personal data may be shared; any cross-border data transfers; and the retention period for such personal data.

Most businesses will communicate the required information in the form of a privacy policy, statement, or notice.[117] Businesses are required to make this information clear, comprehensible, and available in multiple languages "where necessary and practicable."[118] For example, if a US company transferred Japanese customer data to a data processor in India for processing, the Personal Data Protection Act would require the US company, as the data controller, to comply with notice requirements with respect to the Japanese customers.[119] According to the Personal Data Protection Act, the US company may even be required to deliver the notice in Japanese "if necessary and practicable."[120]

### *C. Develop Processes to Grant Data Subject Rights*

Data subjects receive GDPR-style rights under the Personal Data Protection Act, including the right to confirmation of and access to data,[121] the right to data portability,[122] the right to be forgotten,[123] and the right to correction of data.[124] However, these rights are not identical in scope to the corresponding rights under the GDPR. For example, under the Personal Data Protection Act, the "right to be forgotten" requires a data subject to submit a request to an adjudicating authority. This authority weighs the request against various other factors, such as the

---

[114] *See id*.
[115] *See id*. § 49.
[116] *Id*. § 8.
[117] *See* DETERMANN'S FIELD GUIDE TO PRIVACY LAW, *supra* note *, at chs. 3.10 *et seq*.
[118] Personal Data Protection Act § 8(2).
[119] *See id*. §§ 2(1), 3(2), 8.
[120] *Id*. § 8(2).
[121] *Id*. § 24.
[122] *Id*. § 26.
[123] *Id*. § 27. The "right to be forgotten" generally allows data subjects to have personal data (such as text or video) about themselves deleted from records.
[124] *Id*. § 25. When data is corrected, the data controller also has an obligation to notify other entities or individuals to whom personal data was disclosed about the correction as per § 25(4).

sensitivity of the personal data and the relevance of the personal data to the public at large, before deciding whether to grant it.[125] Under the Personal Data Protection Act, data controllers are less likely to receive such requests to be forgotten as compared to the corresponding right under the GDPR[126] or under the new California Consumer Privacy Act.[127] Unlike the Personal Data Protection Act, the GDPR and the CCPA do not have the hurdle of an adjudication process. Businesses that act as data controllers must inform data subjects of these rights and develop mechanisms to address rights requests from data subjects. There is a penalty of approximately $80 a day for failing to comply with requests from data subjects.[128]

### *D. Legitimizing Cross-Border Data Transfers*

Cross-border transfers, which are essential to most outsourcing data processing operations, remain an open issue under the Act. To conduct a cross-border data transfer under the Personal Data Privacy Protection Act, businesses must either enter into standard contractual clauses approved by the Data Protection Authority or transfer data pursuant to a EU-style adequacy decision from the Indian government.[129] Additional consent of the data subject may be required, though it is unclear from the Personal Data Protection Act whether this is still needed if using standard contractual clauses or relying on an adequacy decision.[130] The Indian government has not made any adequacy decisions to date, and the Data Protection Authority can only provide standard contractual clauses once the Personal Data Protection Act becomes law.

### *E. Developing a Data Breach Notification Plan*

Further guidance is also expected to be provided in the future with respect to data breaches, and the situations in which notifications will be required. The Personal Data Protection Act requires all data controllers to notify the Data Protection Authority of any breach if the "breach is likely to cause harm to any data subject."[131] The Act requires businesses to develop assessment models to decide and document the likelihood of harm such as identity theft .[132] This is similar to the assessment carried out under the GDPR by data controllers deciding whether to notify a European Data Protection Authority about a data breach.[133]

---

[125] *Id*. §§ 27(2), 27(3).
[126] *See* GDPR, *supra* note 2.
[127] *See* CAL. CIV. CODE § 1798.105.
[128] Personal Data Protection Act § 70.
[129] *Id*. § 41.
[130] *Id*. §§ 41(1)(d)-(e).
[131] *Id*. § 32.
[132] *See id*. §§ 32(1)-(2).
[133] GDPR, *supra* note 2, at art. 33. The GDPR requires notification by the data controller "unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons."

Under the Personal Data Protection Act, the data controller must notify the Indian Data Protection Authority of the data breach "as soon as possible."[134] Once established, the Indian Data Protection Authority may specify more concrete deadlines. Upon notification, the Data Protection Authority will determine if the data controller must also notify data subjects.[135] The Data Protection Authority can also order remedial actions and post details of breach on its website.[136]

### *F. Assessing Whether Heightened Obligations for High-Risk Data Controllers Apply*

Additional obligations may also apply depending on whether a company is treated as high risk. The Indian Data Protection Authority may classify individual companies or categories of companies as "significant," i.e., high-risk with respect to data privacy if they process large volumes of personal data, process sensitive personal data, and—depending on turnover—create risk of harm to data subjects, among a number of other factors.[137] Heightened requirements apply to such "significant" data controllers; they have to conduct data protection impact assessments,[138] comply with record keeping requirements,[139] conduct data audits,[140] and appoint a data protection officer.[141] It remains to be seen whether the Data Protection Authority will designate individual entities as high-risk data controllers or instead publish a list of categories of high-risk data controllers.

### *G. Protecting Children's Data*

Data controllers are required to create mechanisms for age verification and parental consent to process the personal data of children, defined as persons under the age of eighteen.[142] The Personal Data Protection Act is not prescriptive with these mechanisms, giving data controllers some leeway in designing the mechanisms. "Guardian" data controllers, who operate commercial websites or online services directed at children or who process large volumes of children's personal data, are barred from profiling, tracking, monitoring behavior, directing targeted advertising, and other processing activities that can cause "significant harm" to children.[143]

---

[134] Personal Data Protection Act § 32(3).
[135] *Id*. § 32(5).
[136] *Id*. §§ 32(6)-(7).
[137] *Id*. § 38. The other factors are the turnover of the data controller and the use of new technologies.
[138] *Id*. § 33.
[139] *Id*. § 34.
[140] *Id*. § 35.
[141] *Id*. § 36.
[142] *Id*. §§ 23, 3(9).
[143] *Id*. § 23(5).

### *H. Addressing Data Residency Requirements*

The Personal Data Protection Act creates stringent data residency requirements[144] that have already been the subject of criticism.[145] Data fiduciaries must store a copy of all personal data to which the law applies in India; additional copies can be stored outside India.[146] The government can also specify categories of data that must be stored only in India.[147] This would effectively compel the creation of Indian data centers for many businesses. The government can exempt some categories of personal data (except sensitive personal data) from this residency requirement.[148]

## VII. SANCTIONS AND REMEDIES

Under the Indian Personal Data Protection Act, companies face GDPR-style penalties. Data controllers can be fined approximately $730,000 or two percent of global turnover[149] for, among other items: failing to notify data breaches to the Data Protection Authority to be established under the Act, or failing to meet obligations as a significant data controller. Similarly, data controllers are subject to a fine of approximately $2.7 million or four percent of global turnover[150] for: failing to provide notices to data subjects explaining the existence of a legitimate basis for processing; conducting unlawful cross-border data transfers; or processing children's data in contravention of the relevant sections of the Personal Data Protection Act.[151]

The Indian government can also impose criminal penalties for the sale of personal data in contravention of the law that results in significant harm to the data subject, and for reidentification of anonymized data.[152] Data subjects can also apply for compensation for violations of their rights by making a complaint to an adjudicating officer under the Personal Data Protection Act.[153]

However, data controllers cannot be sued in civil court by data subjects under any separate private right of action, as is common in the United States.[154] This is because the Personal Data Protection Act expressly bars civil courts from

---

[144] *Id*. § 40.
[145] *See, e.g*., Naomi Shiffman and Jochai Ben-Avie, *Data localization: bad for users, business, and security*, OPEN POLICY AND ADVOCACY (Jun. 22, 2018), https://blog.mozilla.org/netpolicy/2018/06/22/data-localization-india/.
[146] Personal Data Protection Act § 40(1).
[147] *Id*. § 40(2).
[148] *Id*. § 40.
[149] *Id*. § 69(1).
[150] *Id*. § 69(2).
[151] *Id*.§ 23.
[152] *Id*. § 90.
[153] *Id*. § 75.
[154] *See, e.g*., CAL. CIV. CODE § 1798.150(a)(1) (creating a private right of action with respect to data breaches).

exercising jurisdiction over matters covered by the Act, instead granting exclusive jurisdiction to authorities established under the Act.[155]

## VIII. LEGISLATIVE TIMELINE

The Personal Data Protection Act must still be reviewed and approved by the Ministry of Electronics and Information Technology, then placed before the Union Council of Ministers; once approved there, the Act must then be placed before Parliament.[156] According to some reports, the Personal Data Protection Act will be placed before Parliament once the Ministry of Electronics and Information Technology completes additional consultations with stakeholders.[157] Both houses of Parliament must debate and pass the Personal Data Protection Act before the President signs it into law. All of this should take at least a few months. Changes to the draft Personal Data Protection Act could take place during any of these steps.

However, the Act is unlikely to stall over a long period of time. As already noted, in August 2017, the Indian Supreme Court ordered the government to enact a comprehensive data protection law. If the government unduly delays enacting this law, it could potentially be in contempt of court.[158]

The substantive compliance provisions of the Personal Data Protection Act will go into effect eighteen months after its enactment.[159] This provides lead time during which the Data Protection Authority can be established to provide guidelines with respect to compliance with and enforcement of the Act.

## IX. COMPARING THE PERSONAL DATA PROTECTION ACT WITH THE GDPR AND CCPA

The Indian Personal Data Protection Act joins a growing body of national data protection legislation that impacts businesses around the globe. The GDPR went into effect on May 25, 2018 and created compliance requirements for all entities processing the data of EU citizens or processing personal data in the EU.[160]

---

[155] Personal Data Protection Act § 91.

[156] *See* PARLIAMENT OF INDIA LOK SABHA [House of the People], Abstract of Parliamentary Process, http://loksabhaph.nic.in/writereaddata/Abstract/legislative_process.pdf.

[157] *See* ET Bureau, *MeitY seeks feedback on data bill from select few*, ECONOMIC TIMES (Aug. 21, 2019, 8:46 AM), https://economictimes.indiatimes.com/tech/internet/meity-seeks-feedback-on-data-bill-from-select-few/articleshow/70763907.cms.

[158] *See* INDIA CONST. (1950), art. 129.

[159] Personal Data Protection Act § 97.

[160] *See* Lothar Determann, *GDPR Ante Portas: Compliance Priorities for the Impending EU Data Protection Regulation*, 2 PLI CURRENT: THE JOURNAL OF PLI PRESS (2018); *see also*, *Less Than 20 Weeks to the European Union GDPR—What to Do Now?* PRIVACY & SECURITY LAW REPORT (BNA) (Jan. 10, 2018), https://www.bloomberglaw.com/document/X7GK454O000000?bc=W1siQ2l0YXRpb24gUmVzdW

As of January 1, 2020, with the passage of the CCPA, companies around the world will have to comply with additional regulations related to the processing of personal data of California residents. Pursuant to the CCPA, covered companies must observe restrictions on data monetization business models; accommodate rights to access, delete, and port personal data; and issue or update privacy notices to provide detailed disclosures about data handling practices.[161]

At the panel discussion in Palo Alto with Minister Prasad (*see supra*, Section 1, Part 2), the panel discussed competing approaches to data regulation. Minister Prasad contrasted the European approach of regulating data processing through a default prohibition on processing of personal data with the US approach of sectoral, harm-specific protections for individual privacy, in which the information technology sector has flourished.[162] Lothar Determann questioned why India seems to be leaning heavily towards the European approach, as opposed to the US approach, given that India is also nourishing a globally leading information technology sector.[163] In response, Minister Prasad noted that all societies have to develop their own conceptions of privacy based their unique culture and history; he further explained that the Personal Data Protection Act is still in draft form, and that the Indian government must find a balance between fostering innovation and safeguarding privacy.[164]

With this need for balance in mind, this Article will review key similarities and differences between the draft Personal Data Protection Act, the GDPR, and the CCPA.

### *A. Extent of Privacy Protections*

The Personal Data Protection Act, like the GDPR, broadly regulates all processing of personal data with the prohibitive character of an omnibus data protection law. The Indian law will establish a Data Protection Authority and will subject companies to numerous administrative duties, including the appointment of data protection officers, local representatives (for foreign companies), data protection impact assessments, record keeping, privacy by design (i.e., the conscious consideration of privacy as a desirable feature at all stages of the design and conception of a product or service), and audits.[165]

---

x0cyIsIi9jaXRhdGlvbi9CTkElMjAwMDAwMDE2MGRiNWRkOWQxYWI3OGZiZmYxOTY5MDAwMj9ibmFfbmV3c19maWx0ZXI9ZS1kaXNjb3ZlcnktYW5kLWxlZ2FsLXRlY2giXV0--6bc8d71a6fa90bcbeba9b197976ab5fc064f8817&jcsearch=BNA%2000000160db5dd9d1ab78fbff19690002#jcite (available by subscription).

[161] *See generally* Determann, *supra* note 4 (analysis of CCPA and its history).

[162] For a description of the panel discussion held at the Hewlett Foundation in Palo Alto, see Jha, *supra* note 25. The Minister was in California to meet with tech leaders and discuss data privacy and security issues. *See also* PTI, *supra* note 25.

[163] *Id*.

[164] *Id*.

[165] Personal Data Protection Act §§ 29, 34-36.

The CCPA also applies broadly but does not create any such administrative obligations. The CCPA addresses the specific risks for individual privacy created by data trading[166] (the buying and selling of personal data by businesses), and was created to supplement—not replace—hundreds of existing data privacy laws at the federal and state level.[167] Neither California nor the United States have established data protection authorities.[168]

### *B. Scope of the Definition of Personal Data*

The Personal Data Protection Act, the GDPR, and the CCPA all regulate any information that relates to an identifiable individual.[169] The CCPA additionally regulates information relating to households.[170]

### *C. Protected Persons*

The Personal Data Protection Act, the GDPR, and the CCPA protect individuals only, and do not protect legal entities.[171] The CCPA protects only California residents.[172]

---

[166] *See* A.B. 375, 2017-18 Reg. Sess., § 2(c)–(f) (Cal. 2018) ("The Legislature finds and declares that: …(c) At the same time, California is one of the world's leaders in the development of new technologies and related industries. Yet the proliferation of personal information has limited Californians' ability to properly protect and safeguard their privacy. It is almost impossible to apply for a job, raise a child, drive a car, or make an appointment without sharing personal information. (d) As the role of technology and data in the everyday lives of consumers increases, there is an increase in the amount of personal information shared by consumers with businesses. California law has not kept pace with these developments and the personal privacy implications surrounding the collection, use, and protection of personal information. (e) Many businesses collect personal information from California consumers. They may know where a consumer lives and how many children a consumer has, how fast a consumer drives, a consumer's personality, sleep habits, biometric and health information, financial information, precise geolocation information, and social networks, to name a few categories. (f) The unauthorized disclosure of personal information and the loss of privacy can have devastating effects for individuals, ranging from financial fraud, identity theft, and unnecessary costs to personal time and finances, to destruction of property, harassment, reputational damage, emotional stress, and even potential physical harm…").

[167] *See* Determann, CALIFORNIA PRIVACY LAW: PRACTICAL GUIDE AND COMMENTARY, U.S. FEDERAL AND STATE LAW, *supra* note 1.

[168] *See* Lothar Determann, *Adequacy of data protection in the USA: myths and facts*, 6 INTERNATIONAL DATA PRIVACY LAW 244 (2016).

[169] *See* CAL. CIV. CODE § 1798.140(o)(1); GDPR, *supra* note 3, art. 4(1); Personal Data Protection Act §3(29).

[170] CAL. CIV. CODE § 1798.140(o)(1).

[171] CAL. CIV. CODE § 1798.140(o)(1); GDPR, *supra* note 3, art. 4(1); Personal Data Protection Act §3(29).

[172] Reference the definition of "consumer" in CAL. CIV. CODE §1798.140(g).

### *D. Applicability to the State*

Unlike the GDPR and the CCPA, the Indian Personal Data Protection Act also applies to the State.[173] In Europe, the GDPR does not apply to data processing by the member states, which is separately regulated in national legislation.[174] Similarly, the United States and California have enacted separate public sector privacy laws, with relatively robust protections against government access to personal data, including the new California Electronic Communications Privacy Act.[175]

The Indian Personal Data Protection Act broadly authorizes public sector data processing in Section 13, which provides:

> (1) Personal data may be processed if such processing is necessary for any function of Parliament or any State Legislature (2) Personal data may be processed if such processing is necessary for the exercise of any function of the State authorized by law for: (a) the provision of any service or benefit to the data principal from the State; or (b) the issuance of any certification, license or permit for any action or activity of the data principal by the State.[176]

Thus, data processing by the State is subject to the same law as data processing by private entities, but the State has broader permission to engage in data processing.[177]

### *E. Prohibition and Minimization of Data Processing*

The GDPR and the Indian Personal Data Protection Act prohibit companies from processing personal data unless they can claim an exception or defense, and even then, companies are required to minimize the processing of personal data.[178] Companies in Europe have been subject to such restrictions since the early 1970s.[179] Indian companies in the information technology sector have so far flourished in the current, largely unregulated legal environment. It remains to be seen how they will fare under the newer, heavily regulated regime.

---

[173] Personal Data Protection Act §2(1)(b).
[174] *See* GDPR, *supra* note 2, at art. 2(2).
[175] California Electronic Communications Privacy Act (CalECPA), S.B. 178, *available at* https://leginfo.legislature.ca.gov/faces/billCompareClient.xhtml?bill_id=201520160SB178. Under the California Electronic Communications Privacy Act, for example, no California government entity can search phones, and no police officer can search online accounts, without going to a judge, getting consent, or showing it is an emergency.
[176] Personal Data Protection Act § 13.
[177] *See id*. §12 (restrictions on private entities).
[178] GDPR, *supra* note 2, at arts. 5(1)(c) and 6(1); Personal Data Protection Act §§ 6, 7.
[179] This may partially explain why European companies are relatively less prominent in the information technology sector compared to their US counterparts. *See* Anupam Chander, *How Law Made Silicon Valley*, 63 EMORY L.J. 639 (2014).

In the United States, Congress deliberately decided against enacting data regulation in the 1970s in order to preserve and protect innovation and economic freedoms.[180] Under most US data privacy laws, companies are not prohibited from processing personal data or required to minimize data processing, but are merely required to observe narrowly tailored restrictions deemed necessary to protect individual privacy.[181] Even under the extensive CCPA, companies only have to seek prior opt-in consent from minors or their parents before selling personal information pertaining to children under sixteen years of age.[182] Otherwise, selling or processing personal data is not prohibited or limited, unless or until a data subject exercises their right under the CCPA to limit processing of individual information.[183]

### *F. Global Scope of Applicability*

Companies around the world can be subject to the Personal Data Protection Act, the GDPR, and the CCPA (and to most other privacy laws around the world) if they collect or process personal data from or in the territories governed by the respective laws. To avoid becoming subject to these laws, companies would have to stop doing business in regulated jurisdictions. After the GDPR took effect in May 2018, some US newspapers started blocking online access by E.U. residents,[184,] and in Europe, various bloggers, nonprofit organizations and smaller businesses went offline because they felt unable to comply with the new requirements.[185] Most multinational companies, however, are unlikely to consider this a viable option given the size of the European and Indian economies and business opportunities.[186]

A key difference between the three laws is that most US privacy laws, including the CCPA, only protect the privacy of residents, whereas the GDPR and the Personal Data Protection Act regulate any processing of personal data on local territories, including personal data pertaining to persons residing in other

---

[180] *See* Paul Schwartz, *Preemption and Privacy*, 118 YALE L.J. 902 (2009).
[181] *See Determann, supra* note 168.
[182] CAL. CIV. CODE §1798.120(c).
[183] *Id.*
[184] Adam Saratiano, *U.S. News Outlets Block European Readers Over New Privacy Rules*, N.Y. TIMES (May 25, 2018), www.nytimes.com/2018/05/25/business/media/europe-privacy-gdpr-us.html.
[185] Patrick Bernau, Was der neue Datenschutz angerichtet hat, FRANKFURTER ALLGEMEINE ZEITUNG (May 28, 2018, 3:19 PM), www.faz.net/aktuell/wirtschaft/diginomics/skurrile-folgen-der-dsgvo-15609815.html#void.
[186] The United States (#1), Germany (#4) and India (#7) are in the top 7 of economies by gross domestic product, and the E.U. and California would come in as #2 and #5 respectively if they were nations. See *World Bank GDP Data,* https://data.worldbank.org/indicator/ny.gdp.mktp.cd?most_recent_value_desc=true; *California is now the world's fifth-largest economy, surpassing United Kingdom*, LOS ANGELES TIMES (May 4, 2018, 1:50 PM), www.latimes.com/business/la-fi-california-economy-gdp-20180504-story.html.

countries.[187] As a result, foreign companies subject themselves to compliance obligations under the GDPR and the Personal Data Protection Act not only if they collect information about Indian or European residents, but also if they process foreign personal data in European or Indian territory. This could noticeably impair India's attractiveness as a destination for offshoring of business process outsourcing, call centers, and data processing services more generally. Foreign companies will generally not want to subject themselves to Indian privacy law applicable to data controllers on the basis that they engage a data processor, call center operator, or other service provider on Indian territory.[188]

For example, hypothetically, if a bank in Brazil were to consider engaging a cloud service provider in Europe, India, or the United States to process the data of Brazilian bank customers, the bank would need to comply with requirements on data controllers under the GDPR and Personal Data Protection Act if it selects a data processing location in Europe or India.[189] By contrast, the Brazilian bank would not have to comply with the CCPA if it engaged a cloud provider in California because the California law applies only to the personal data of California residents, not of Brazilian bank customers.[190] Neither the bank nor its Brazilian customers would likely perceive the applicability of E.U. or Indian data protection laws as an advantage. Both parties may be concerned about data access by foreign governments against which neither the GDPR nor the Indian Personal Data Protection Act provide meaningful protections.[191] More significantly, the Brazilians might be concerned about data access by the Brazilian government, which local data processing service providers in Brazil would be more exposed to than any foreign service provider. Absent any special favorable treatment under foreign data protection laws, the Brazilian bank and its customers would have rely on Brazilian law and contractual protections for data security, which applies regardless of which jurisdiction a cloud or other service provider is based in. Consequently, Indian service providers may become a less attractive option internationally if engaging those providers triggers additional substantive compliance obligations on foreign customers under the Personal Data Protection Act.

---

[187] *See* CAL. CIV. CODE §1798.140(g); GDPR, *supra* note 3, at arts. 2, 3; Personal Data Protection Act § 2.

[188] *See, e.g.*, IANS, *An Indian lobby with the likes of Facebook, Flipkart, and Microsoft as members is still arguing against storing data in India*, BUSINESS INSIDER (Oct. 7, 2019, 8:50 PM), https://www.businessinsider.in/policy/news/an-indian-lobby-with-the-likes-of-facebook-flipkart-and-microsoft-as-members-is-still-arguing-against-storing-data-in-india/articleshow/71472585.cms.

[189] *See* GDPR, *supra* note 3, at arts. 2, 3; Personal Data Protection Act § 2.

[190] *See* CAL. CIV. CODE § 1798.140(g).

[191] *See* Lothar Determann, *Data Residency Rules Cutting Into Clouds: Impact and Options for Global Businesses and IT Architectures*, BLOOMBERG BNA PRIVACY & SECURITY LAW REPORT (Apr. 3, 2017) (analysing the impact of recent data residency laws in other jurisdictions such as Russia, Germany, Indonesia and China).

### *G. Rights of Data Subjects*

Under all three laws, individuals have the rights to access (i.e., to know what data is held about them), portability (i.e., to have data transferred to another entity that provides similar services), and to be forgotten (i.e., to have information held about them deleted or restricted), subject to different nuances and exceptions.[192] Under the Personal Data Protection Act, individuals enjoy only a limited right to be forgotten with respect to further disclosure, but not a right to absolute deletion.[193] To obtain absolute deletion, individuals need to seek a decision weighing data privacy and information freedom interests from an adjudicating officer at the Data Protection Authority. Requesting individuals may have to pay a fee to compensate the data controller for the costs of handling such requests.[194]

### *H. Selling of Personal Data*

The GDPR does not regulate selling of data specifically or even reference "selling" or "sale" in its text. Companies are generally prohibited from processing personal data, and the definition of processing broadly encompasses any disclosure of relevant data.[195] Thus, under the GDPR, selling data is subject to the general broad prohibitions and exceptions.[196]

By contrast, the CCPA is very focused and prescriptive regarding "selling of information," as a reaction to the data processing activities of Cambridge Analytica, a U.K. company that focused on influencing of national elections.[197] The Cambridge Analytica scandal was specifically mentioned in the recitals to the California law and similarly provoked outrage in India.[198]

Under the Personal Data Protection Act, as under the GDPR, companies must comply with general restrictions on data processing whenever they sell data. Additionally, companies face criminal penalties if they sell personal data in violation of the Personal Data Protection Act and thereby cause significant harm to data subjects.[199]

### *I. Data Security and Breach Notifications*

Like the GDPR, the Personal Data Protection Act obligates companies to keep data secure and to notify data protection authorities and individuals of

---

[192] CAL. CIV. CODE §§1798.100 *et seq*.; GDPR, *supra* note 2, at arts. 12–23; Personal Data Protection Act §§ 24–28.
[193] Personal Data Protection Act § 27.
[194] Personal Data Protection Act §§ 27-28.
[195] *See* GDPR, *supra* note 2, at art. 6.
[196] *Id*.
[197] *See* A.B. 375, 2017–18 Reg. Sess., § 2 (Cal. 2018).
[198] Vindu Goel, *India Pushes Back Against Tech 'Colonization' by Internet Giants*, N.Y. TIMES (Aug. 31, 2018), www.nytimes.com/2018/08/31/technology/india-technology-american-giants.html.
[199] Personal Data Protection Act § 90(d). If sensitive personal data is sold, then only "harm" rather than "significant harm" to the data subject is required for criminal penalties to apply. *Id*. § 91(d).

breaches under certain circumstances, such as if the "breach is likely to cause harm to any data subject."[200] California enacted data security requirements and data breach notification obligations in 2002, and supplemented these existing laws with new statutory damages provisions in the CCPA.[201]

### *J. International Transfer Restrictions*

Like the GDPR, the Personal Data Protection Act restricts international transfers of personal data.[202] California and US laws do not impose any restrictions on international data transfers.

### *K. Data Residency Requirements*

Section 41 of the Personal Data Protection Act requires that companies store on Indian territory all personal data subject to the Act, or, at a minimum, a copy of such personal data. Russia, Kazakhstan, and Indonesia have also enacted data residency laws in the past; China has included data residency requirements in draft cybersecurity laws.[203]

Neither the GDPR nor US federal or California privacy laws contain data residency requirements. Germany enacted fairly limited national laws requiring storage of Internet metadata on German territory in 2016, but these seem to be conflicting with E.U. law and have to date not been enforced.[204] If the E.U. or the United States retaliate with broad data residency requirements of their own, this could have a significant adverse impact on India's information technology and outsourcing sector.[205]

### *L. Data Processing Contracts*

Under Article 28 of the GDPR, companies must sign written contracts with processors and "stipulate" particular clauses prescribed in detail.[206] Section 37 of the Personal Data Protection Act also requires a contract, but it is less prescriptive as to its content.[207] Companies that meet the requirements of Article 28 of the GDPR with existing data processing agreements should also meet the new

---

[200] GDPR, *supra* note 2, at arts. 24, 32–34; Personal Data Protection Act §§ 31, 32.
[201] CAL. CIV. CODE §1798.150; *see* Lothar Determann, *Be Wary of Liability for Statutory Damages under California Consumer Privacy Act*, PRIVACY & SECURITY LAW REPORT (BNA) (Jul. 9, 2018), https://www.bloomberglaw.com/document/X6TG8870000000?bna_news_filter=privacy-and-data-security&jcsearch=BNA%2520000001646a6fd844a3f76e7f95030002#jcite.
[202] GDPR, *supra* note 2, at arts. 44 *et seq*.; Personal Data Protection Act §§ 41–42.
[203] Determann, *supra* note 71.
[204] Lothar Determann & Michaela Weigl, *Data Residency Requirements Creeping into German Law*, PRIVACY & SECURITY LAW REPORT (BNA) (Apr. 11, 2016), https://www.bloomberglaw.com/product/blaw/document/X1KCCTDG000000.
[205] Goel, *supra* note 198.
[206] *See* GDPR, *supra* note 2, at art. 28.
[207] Personal Data Protection Act § 37.

requirements under the Personal Data Protection Act.[208] Under the CCPA, companies do not face any new contracting obligations, but many companies may nevertheless consider updating their vendor contracts to expressly prohibit "selling" of personal information to avoid triggering disclosure obligations under the new California law.[209]

### *M. Age of Children and Consent Issues*

The Personal Data Protection Act requires companies to obtain parental consent from parents or guardians of persons under the age of eighteen.[210] According to Article 8(1) of the GDPR, the age threshold for parental consent is sixteen years.[211] According to the CCPA, companies must obtain prior consent to sell data from minors between thirteen and sixteen years old, and must obtain consent from guardians or parents of children under thirteen years old.[212]

In 1998, the US Congress enacted the Children's Online Privacy Protection Act (COPPA), under which companies must obtain parental consent with respect to children under thirteen years old.[213] The US Federal Trade Commission started enforcing COPPA, and most companies in the United States and elsewhere started to prohibit children under the age of thirteen from accessing their websites and online services.[214]

Parents around the world may have observed this development with mixed feelings, based on a desire to teach their children to use online services responsibly.[215] Many parents allowed their children to lie about their age online.[216] Companies and parents in India and Europe alike will face more difficult decisions and enforcement challenges in light of the higher age threshold: eighteen in India, as compared to thirteen in the United States and sixteen in Europe.[217]

---

[208] See Personal Data Protection Act § 37; GDPR, *supra* note 3, at art. 28.
[209] Amy de La Lama & Brian Hengesbaugh, Navigating disclosures and sales of personal information under the CCPA (The Privacy Advisor, IAPP, Aug. 28, 2019), https://iapp.org/news/a/navigating-disclosures-and-sales-of-personal-information-under-the-ccpa/.
[210] Personal Data Protection Act §§ 3(9), 23(2)e.
[211] *See* GDPR, *supra* note 2, at art. 8(1).
[212] CAL. CIVIL CODE § 1798.120 (d).
[213] Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–6506.
[214] *See* FEDERAL TRADE COMMISSION, PROTECTING CHILDREN'S PRIVACY UNDER COPPA: A SURVEY ON COMPLIANCE (April 2002), www.ftc.gov/sites/default/files/documents/reports/protecting-childrens-privacy-under-coppa-survey-compliance/coppasurvey.pdf.
[215] Danah Boyd, *Why Parents Help Tweens Violate Facebook's 13+ Rule*, HUFFINGTON POST (Dec. 6, 2017, 1:38 AM), www.huffingtonpost.com/danah-boyd/tweens-on-facebook_b_1068793.html.
[216] *Id*.
[217] *See* 15 U.S.C. § 6501(1); GDPR, *supra* note 3, at art. 8(1); Personal Data Protection Act § 3(9).

### *N. Penalties and Enforcement*

Under the Personal Data Protection Act, much like the GDPR, companies face tiered penalties of up to $2.7 million or four percent of global turnover.[218] The Indian Data Protection Authority shall set up special funds for its operative costs, supported by fees and charges, and for privacy awareness, supported by penalty funds.[219]

The GDPR also provides for fines up to four percent of global turnover, but leaves the details of applying and allocating the revenue from penalties to the member states of the European Economic Area (which includes the E,U. States plus Iceland, Norway and Liechtenstein).[220] Some member states, including Spain, allow their data protection authorities to use enforcement revenue to fund their operations, which has resulted in disproportionate enforcement activities compared to the general EEA standards.[221] The CCPA also establishes a Consumer Privacy Fund, which is funded by penalties and is designed to induce and support additional enforcement activities.[222]

Under the Personal Data Protection Act, data subjects can also be awarded individual compensation after an adjudication process if their rights are violated.[223]

## X. OUTLOOK AND ACTION ITEMS

As our comparison in Section IX of this Article indicates, the new Indian Personal Data Protection Act adopts and further develops many existing principles of EU-style data processing regulation and some aspects of US-style data privacy laws. Global companies can, and should, try to address the requirements of the new Personal Data Protection Law, the GDPR, the California Consumer Privacy Act, and other privacy regimes simultaneously and holistically, in the interest of efficiency.[224] However, it is also clear that companies cannot just expand the coverage of their GDPR-focused compliance measures to India without addressing the nuances of the Personal Data Protection Act and its many differences from other jurisdictions' data processing regulations and data privacy laws.

---

[218] Personal Data Protection Act §§ 69–74.
[219] *Id*. at § 77.
[220] GDPR, *supra* note 2, at arts. 77 *et seq*.
[221] *See Data Protection Enforcement in Spain*, GLOBAL COMPLIANCE NEWS (2006), https://globalcompliancenews.com/data-privacy/data-protection-enforcement-in-spain/.
[222] CAL. CIV. CODE § 1798.155 contemplates 20 percent of penalties to be allocated to the Consumer Privacy Fund; new legislation contemplates increasing this amount to 100 percent.
[223] Personal Data Protection Act § 75.
[224] *See* Daniel J. Solove, *The Challenge of Global Privacy Compliance: An Interview with Lothar Determann*, TECHNOLOGY ACADEMICS POLICY (Nov. 15, 2017), www.techpolicy.com/Solove_BeyondGDPR-Challenge-GlobalPrivacyCompliance-InterviewWithLotharDetermann.aspx.

Any company that has already undertaken GDPR compliance measures and created a comprehensive data inventory, carried out a data processing assessment, put in place procedures to address data breaches, and considered when it can use anonymized or pseudonymized aggregated data will be better positioned to comply with the new Indian law and any future legislation that may be modelled on it as these action items and considerations are shared by both the GDPR and the new Indian law.[225] Companies that have not yet tackled GDPR compliance need to prepare for significant projects and should consider simultaneously addressing GDPR and Personal Data Protection Act compliance.[226]

All companies that may be subject to the new Indian Personal Data Protection Act should prepare a task list and start with a few initial action items:

> **Review data sharing and processing practices** and prepare a roadmap for compliance and implementation. As anyone who has worked on the GDPR knows,[227] eighteen months is not a large amount of time to prepare for compliance with an entirely new regulatory regime.
> **Integrate compliance measures and task lists with existing efforts** to address requirements of the E.U. GDPR, the California Consumer Privacy Act of 2018, and other global data protection, privacy, and security laws holistically.
> **Prepare data maps, inventories, or other records** of all personal data covered by the Personal Data Protection Act to assess what personal data in the company's control is covered, add newly required information to privacy policies, and prepare for data access, correction, and portability requests.
> **Consider data minimization and retention duties and identify legal bases for processing of personal data** under the Personal Data Protection Act.
> **Consider how to comply** with some of the Personal Data Protection Act's substantive requirements, such as those relating to data subject rights, data residency, and mechanisms for cross-border data transfers.
> **Evaluate agreements with data processors** to see if they meet the accountability requirements for data controllers under the Indian Personal Data Protection Act

Companies outside of India will additionally have to consider whether they are comfortable subjecting themselves to the new compliance requirements with respect to personal data pertaining to data subjects outside India, which will only become subject to Indian data protection law if it is stored or processed by an affiliated or unaffiliated data processor in India. Where this is undesirable, multinationals should consider removing personal data from Indian territory.

Finally, companies should closely monitor modifications to the draft Indian Personal Data Protection Act as it moves through the legislative process and

---

[225] *See e.g.*, GDPR, *supra* note 3, at art. 28; Personal Data Protection Act § 37.
[226] *See generally* Determann, *Less Than 20 Weeks to the European Union GDPR—What to Do Now?*, *supra* note 160; DETERMANN'S FIELD GUIDE TO PRIVACY LAW, *supra* note 1.
[227] *See generally* Determann, *Less Than 20 Weeks to the European Union GDPR—What to Do Now?*, *supra* note 160.

watch out for implementation guidance to be provided by the Data Protection Authority under the Personal Data Protection Act.