UNC SCHOOL OF LAW

NORTH CAROLINA JOURNAL OF INTERNATIONAL LAW

Volume 45 | Number 3 Article 3

2020

India's Data Wild West: The Aadhaar System and Its Questionable Data Protections

Brett Orren

India's Data Wild West: The Aadhaar System and Its Questionable Data Protections

Brett Orren†

I. Introduction

Between social media data scandals in the United States,[1] Marriott's data breach,[2] and the alleged election interference by Russian hackers,[3] the international community has been grappling with how to rein in the "data wild west."[4] India's Aadhaar system

---

† J.D. Candidate 2020, University of North Carolina School of Law. Managing Editor, *North Carolina Journal of International Law.*

1 *See generally Social Media Influence: Hearing 115-232 Before the S. Select Comm. on Intelligence*, 115th Cong. (2017) [hereinafter *Social Media Hearing*] (including representatives from Facebook, Twitter, and Google).

2 *See* David Volodzko, *Marriott Breach Exposes Far More Than Just Data*, FORBES (Dec. 4, 2018), https://www.forbes.com/sites/davidvolodzko/2018/12/04/marriott-breach-exposes-far-more-than-just-data/#1b2afb566297 [https://perma.cc/7PYZ-ZMWR].

3 *See* Martin Matishak, *What We Know About Russia's Election Hacking*, POLITICO (Sept. 18, 2018), https://www.politico.com/story/2018/07/18/russia-election-hacking-trump-putin-698087 [https://perma.cc/4V5T-Q57F].

4 *We Need to Fix the 'Data Wild West,'* PRIVACY INT'L (Feb. 4, 2019), https://privacyinternational.org/feature/2677/we-need-fix-data-wild-west [https://perma.cc/P6Q9-5H7P].

exemplifies the dichotomy of wanting to use big data for convenience and ease, but providing protections on who can use the data, what data can be shared, and when an individual's personal data should be used. This note explores international data privacy laws in relation to India.

Data privacy varies greatly from country to country, and there is no one international guideline or way to handle data privacy. Most countries follow the European Union ("EU") approach—increased protections to personal data privacy.[5] However, China does not follow that approach, and instead works to completely centralize the personal and biometric data of its citizens.[6] Specifically, this note examines where India's Aadhaar system has placed India on a data privacy spectrum—whether it aligns more with the EU or China—and how recent proposed legislation affects the Aadhaar system. I will use the perspective of other countries to conceptualize where India's system would fall on this comparative spectrum of countries' values of data privacy. This note places India's current system on a data privacy spectrum close to that of Malaysia and China, but by enacting currently proposed legislation, India would be slowly moving towards the privacy ideals of the EU.

Part II will explain the Aadhaar system, including the Indian Supreme Court's decision to uphold the constitutionality of Aadhaar.[7] Part III will compare systems along a spectrum of data privacy values, including those of the EU, United States, Malaysia and China. Part IV will place India on the data privacy spectrum and evaluate the effects of proposed legislation[8] on individual privacy rights, including whether the proposed legislation, if enacted, will curb the negative data privacy implications that Aadhaar has on society. Part V will conclude by noting unanswered questions that India will likely have to confront in the near future.

---

5 *See* Commission Regulation 2016/679, 2016 O.J. (L 119) 1 (EU) [hereinafter GDPR].

6 *See* Bernard Marr, *Chinese Social Credit Score: Utopian Big Data Bliss or Black Mirror on Steroids?*, FORBES (Jan. 21, 2019), https://www.forbes.com/sites/bernardmarr/2019/01/21/chinese-social-credit-score-utopian-big-data-bliss-or-black-mirror-on-steroids/#3159395d48b8 [https://perma.cc/25LY-3XXD].

7 *See* K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1, 3–4 (India).

8 Justice B.N. Srikrishna, A FREE AND FAIR DIGITAL ECONOMY PROTECTING PRIVACY, EMPOWERING INDIANS (Committee of Experts under the chairmanship of (retd.) Justice B.N. Srikrishna, 2018).

II. Aadhaar, An Introduction

Prior to Aadhaar, Manisha Kamble lived as a "street child" in Mumbai.[9] With no birth certificate, no address, and no family she was "invisible to the state."[10] Manisha was unable to receive government assistance, unable to go to school, and unable to vote.[11] Like Manisha, residents without income, citizenship, or addresses, and marginalized persons—women, children, senior citizens, persons with disabilities, migrant workers, and nomads—are particularly vulnerable because they lack access to government services.[12] Before Aadhaar, millions of citizens were uncounted by the government, and it proved to be a major hinderance for welfare programs because of the inability to credibly identify those in need of welfare.[13] Many people received welfare because of fraudulent or duplicate forms of identification ("ID") and, alternatively, many people in need could not receive government benefits because their IDs were already fraudulently in use.[14]

In 2006, the concept of Aadhaar was born "to ensure correct identification of targeted beneficiaries for delivery of various subsidies, benefits, services, grants, wages and other social benefits schemes."[15] Aadhaar launched in 2009, and now almost 1.3 billion people are enrolled.[16] It allows a person to enter into transactions without any ID documents.[17] Each person is assigned a unique and random, twelve-digit identification number and a registration card.[18]

---

9 Lauren Frayer & Furkan Latif Khan, *India's Biometric ID System Has Led to Starvation for Some Poor, Advocates Say*, NPR (Oct. 1, 2018), https://www.npr.org/2018/10/01/652513097/indias-biometric-id-system-has-led-to-starvation-for-some-poor-advocates-say [https://perma.cc/48KX-5GAT].

10 *Id.*

11 *Id.*

12 *See* Kamakshi Ayyar, *The World's Largest Biometric Identification System Survived a Supreme Court Challenge in India*, TIME (Sep. 26, 2018), http://time.com/5388257/india-aadhaar-biometric-identification/ [https://perma.cc/ZNZ5-R5KU].

13 *See Puttaswamy*, 10 SCC at 25.

14 *See id.* at 26.

15 *See id.* at 25.

16 GOVERNMENT OF INDIA, UNIQUE IDENTIFICATION AUTHORITY OF INDIA 1 (2019), https://uidai.gov.in/images/state_wise_aadhaar_saturation_as_on_22052017.pdf [https://perma.cc/K5AT-P2UU].

17 *Puttaswamy*, 10 SCC at 3.

18 *See* Ayyar, *supra* note 12.

Meanwhile, the government collects and stores demographic (name, address, phone number, birthday, etc.) and biometric (fingerprint and iris scans) data.[19] The system enables every Indian citizen to be recognized by their government, regardless of their income, citizenship, or address.[20] Aadhaar is used to open bank accounts, receive welfare benefits, enroll in school, and more.[21] For example, the individual's card or identification number is given to a store employee who runs the card through a credit-card-like-machine.[22] The employee authenticates the card using biometrics of either the fingerprint or iris scan of the cardholder, and the machine tells the employee how much and for what rations the person is eligible.[23] Proponents of Aadhaar advertise the system as fraud proof.[24]

Opponents to Aadhaar argue that the system puts a person's most sensitive data at risk to hackers, and it prevents marginalized individuals from receiving government assistance because of administrative problems.[25] Specifically, they argue the system is an Orwellian Nightmare—leading India closer to a totalitarian state, watched over by "Big Brother," and further from the data privacy rights admired in Western democracies.[26] Opponents paint a dreary picture of a system that could coerce an individual "to part with core information,"[27] which the State could use to "profile citizens, track their movements, assess their habits and silently influence their behaviour."[28] It "diminishes the status of the citizen" by making

---

19 *Id.*

20 *Id.*

21 *Id.*

22 Jahnavi Sen, *In Rural Jharkhand, Aadhaar Link to Welfare Schemes is Excluding the Most Needy*, THE WIRE (Sept. 26, 2018), https://thewire.in/government/jharkhand-aadhaar-pds-pensions [https://perma.cc/H348-6QZ7].

23 *Id.*

24 *See* K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1, 3–4 (India).

25 Ayyar, *supra* note 12.

26 *See generally Puttaswamy*, 10 SCC at 53 (noting the benefits of Western democracies in terms of privacy from the government).

27 *Id.*

28 *Id.* In other countries, most notably following Venezuela's elections, food rations were conditioned on who the citizens voted for, which the State knew from its identification system. There is worry in India that Aadhaar may someday be used similarly to influence political decisions. *See* Francisco Toro, *Venezuela's Democracy is Fake, But the Government's Latest Election Win was Real*, WASH. POST (Oct. 17, 2017), https://www.washingtonpost.com/news/democracy-post/wp/2017/10/17/venezuelas-democracy-is-fake-but-the-governments-latest-election-win-was-real/

rights of liberty, free choice, and government-mandated entitlements all conditioned on "voluntarily" allowing the government to access personal biometric and demographic information.[29]

Not only is the voluntary nature of the program an advertising farce for those who rely on government benefits, but the information is authenticated by private corporations where data leaks are common.[30] For example, in a test run by *The Tribune*, a reporter texted a WhatsApp number with his name, email address, and a money transfer of *only* 500 rupees ($7 USD).[31] Within ten minutes, he was emailed back by the hacker with an "Enrolment Agency Administrator ID" and password, giving him access to the Aadhaar site and "details of every Indian citizen registered"—including bank account and entitlement information.[32] Additionally, a high-ranking Aadhaar official, R.S. Sharma, dared "ethical hackers" on Twitter to hack his account, claiming that Aadhaar was so safe that it would be unsuccessful.[33] The hackers accepted the challenge and, within minutes, his personal information was released, including his address, Aadhaar ID number, phone number, frequent flyer identification, and, to prove that the system was completely penetrable, the hackers deposited a single rupee into his bank account.[34]

When the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act was passed in 2016,[35] the Indian Supreme Court was left with the task of determining whether

---

[https://perma.cc/Y8JK-7UR2].

29 *Puttaswamy*, 10 SCC at 54.

30 *Id.*

31 Rachna Khaira, *Rs 500, 10 Minutes, and You Have Access to Billion Aadhaar Details*, TRIBUNE (Jan. 4, 2018), https://www.tribuneindia.com/news/nation/rs-500-10-minutes-and-you-have-access-to-billion-aadhaar-details/523361.html [https://perma.cc/MF5C-2RSF].

32 *Id.*

33 Rachel Chitra, *Hackers Deposit Re 1 in Trai Chief's Account*, TIMES INDIA (July 30, 2018), https://timesofindia.indiatimes.com/india/hackers-deposit-re-1-in-trai-chiefs-account/articleshow/65190556.cms [https://perma.cc/Z8T9-UJU4].

34 *Id.*

35 The Aadhaar (Targeted Delivery of Financial And Other Subsidies, Benefits and Services) Act, 2016, No. 18, Acts of Parliament, 2016 (India) [hereinafter The Aadhaar Act].

the Aadhaar system was constitutionally valid.[36] On September 26, 2018, the Indian Supreme Court upheld the constitutionality of Aadhaar.[37] The Court focused extensively on the Right to Privacy, memorialized in Articles 14, 19 and 21 of the Indian Constitution.[38] Specifically, Article 21 protects life and personal liberty, mirroring the United States' Declaration of Independence.[39] Privacy is within "personal liberty," and the Court included "*informational privacy, and privacy of choice*" within the privacy protections.[40] The Court went on to hold that Aadhaar gives Indians a privacy of choice through "universal proof of identity" throughout India.[41] The biometric system protects citizens' identities from fraud and illegal activities.[42] Additionally, citizens have an opportunity to travel anywhere throughout the country without needing extensive documentation.[43] In the Court's interpretation, Aadhaar is a way for all citizens to be counted as a part of society.[44] The most marginalized now receive the benefits "which are actually meant for [them]," no matter where they are in India.[45]

The Court discussed the administrative problems likely to arise during the initial Aadhaar implementation,[46] including: no access to an Aadhaar ID card because the mail backup takes so long that many addresses change before the card and information are received;[47] limited or intermittent internet access that prevents citizens, whose

---

36 *Id.*

37 *See* K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1, 3–4 (India).

38 *Id.* at 19. *See also* Shayara Bano v. Union of India, 9 SCC 1 (2017) (India) (determining that the Right to Privacy is a fundamental right that cannot be taken away without the existence of a law that is a legitimate State interest, and the law should pass the test of proportionality. The Supreme Court used *Shayara Bano* to set the stage for holding that data privacy is included in the "Right to Privacy.").

39 *See* INDIA CONST. art. 21.

40 *Puttaswamy*, 10 SCC at 164 (emphasis added).

41 *Id.* at 14.

42 Ayyar, *supra* note12.

43 *Puttaswamy*, 10 SCC at 164.

44 *Id.* at 196–97.

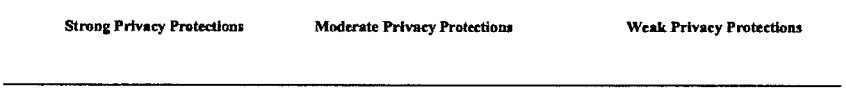
45 *Id.* at 85.

46 *See* Ayyar, *supra* note 12 (noting that some administrative challenges led people to return several days in a row to receive rations because of poor internet connection).

47 Kritika Roy, *Revisiting Aadhaar System: Post the Supreme Court Verdict*, INSTITUTE FOR DEFENSE STUDIES AND ANALYSES (Nov. 2, 2018), https://idsa.in/idsacomments/revisiting-aadhaar-system-kroy-021018 [https://perma.cc/7LN4-VYGB].

biometric data was not input into the offline version, from receiving assistance;[48] and lack of access for the old and young—faded fingerprints and cloudy irises prevent biometric matches with some over 60 years old, and children's fingerprints change as they grow older.[49] However, despite these administrative issues, the Modi Court ruled the positives of Aadhaar far outweighed its weaknesses.[50]

III. A Data Privacy Survey



Historically in the United States, privacy was seen as "the right to be let alone."[51] This definition was accepted globally, and it has been expanded as countries adapt to changing technologies. More recently, the Supreme Court of the United States defined privacy as "the right of the *individual* . . . to be free from unwarranted governmental intrusion into matters so fundamentally affecting a person."[52] However, the extent of individual privacy rights depends on the region of the world. To help compare India's individual data privacy rights with other nations, I have created a data privacy spectrum, on which I have placed four countries' systems: the EU, the United States, Malaysia, and China. These four countries or systems were chosen for their comparative value. The countries are placed on the spectrum based on the data privacy protections they provide: the EU would lie on one end, providing strict individual protections,[53] and the United States would fall somewhere in the middle of the spectrum.[54] On the far end of the spectrum would lie

48 *Puttaswamy*, 10 SCC at 370 (citing Professor Reetika Khera that the system is "wholly inappropriate technology for rural India").

49 Ayyar, *supra* note 12 (warning that if a person's biometric verification is denied for any reason, they are denied rations); *see also Puttaswamy*, 10 SCC at 313 (noting that authentication failures were as high as 49% in 2016).

50 *Puttaswamy*, 10 SCC at 313.

51 S. Warren and L. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 220 (1980).

52 Eisenstadt v. Baird, 405 U.S. 438, 453 (1972) (emphasis added).

53 GDPR, *supra* note 5. *See also* Case C–131/12, Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González, 2014 ECLI:EU:C:2014:317.

54 While the United States is mostly state-driven in the field of data privacy, federal regulations include The Health Insurance Portability and Accountability Act (HIPAA),

both Malaysia's *MyKad* system[55] and China's Social Credit System, which offer very few individual data protections.[56]

Like the United States,[57] India does not yet have a single federal data protection law, but instead takes a sectoral approach.[58] The minimal protections that individual Indian citizens do have are limited "sensitive personal information."[59] Even this information only protects against corporate businesses that automatically process consumer data.[60] The protections still do not allow individuals to control their own data.[61] The Aadhaar Act allows the Indian government to compile all sensitive personal data in a centralized database that it can use without individual consent.[62] Thus, the Aadhaar Act creates a question about how much India values individual privacy rights. It is necessary to address this question because technology is constantly changing, companies are

---

The Genetic Information Nondiscrimination Act of 2008 (GINA), The Children's Online Privacy Protection Act of 1998 (COPPA), The Family Educational Rights and Privacy Act of 1974 (FERPA), the Fair Credit Reporting Act, and The Foreign Intelligence Surveillance Act of 1978 (FISA), among others. *See* Nancy Perkins et al., *California's New Privacy Statute: Is It a US GDPR?*, ARNOLD & PORTER (Oct. 3, 2018) https://www.arnoldporter.com/en/perspectives/publications/2018/10/californias-new-privacy-statute?utm_source=Mondaq&utm_medium=syndication&utm_campaign=View-Original [https://perma.cc/5WNY-JL43]; Jeewon Kim Serrato et al., *US States Pass Data Protection Laws on the Heels of the GDPR*, NORTON ROSE FULBRIGHT (July 9, 2018), https://www.dataprotectionreport.com/2018/07/u-s-states-pass-data-protection-laws-on-the-heels-of-the-gdpr/ [https://perma.cc/PTZ9-BFQG] (demonstrating that some states are using the GDPR as a role model for their own systems).

55 *Introduction to MyKad*, NATIONAL REGISTRATION DEPARTMENT OF THE MINISTRY OF HOME AFFAIRS, https://www.jpn.gov.my/en/informasimykad/introduction-to-mykad/ [https://perma.cc/W5U9-JB89].

56 *Outline of the Construction of Social Credit System (2014-2020)*, CREDIT CHINA, https://www.creditchina.gov.cn/zhengcefagui/redian/zhengcefagui/201711/t20171122_96782.html [https://perma.cc/UX3U-BCBJ] [hereinafter Social Credit System].

57 *See infra,* Part II(b).

58 *Data Protection Regulations and International Data Flows: Implications for Trade and Development*, UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT (UNCTAD) 44 (Apr. 2016) [hereinafter UNCTAD].

59 *Id.*

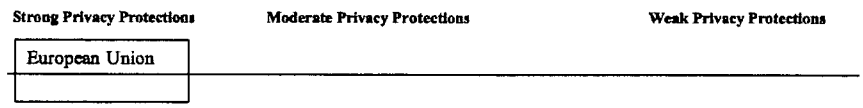
60 *Id. See also* Vindu Goel, *India Proposes Chinese-Style Internet Censorship*, N.Y. TIMES (Feb. 14, 2019), https://www.nytimes.com/2019/02/14/technology/india-internet-censorship.html?utm_campaign=The%20Interface&utm_medium=email&utm_source=Revue%20newsletter [https://perma.cc/JSD4-ZWMD].

61 UNCTAD, *supra* note 58.

62 *Id. See also* The Aadhaar Act, *supra* note 35.

becoming more reliant on consumer data, and therefore, personal data privacy is increasingly at risk. Technology changes much faster than laws and regulations, so the government must react quickly to the changing technological landscape to ensure individuals can safely and securely benefit from its advancements.

A. European Union



The General Data Protection Regulation ("GDPR") is based on the belief that "personal data is a fundamental right," established through the Charter of Fundamental Rights of the European Union[63] and the Treaty on the Functioning of the European Union ("TFEU").[64] The GDPR presumes that "[n]atural persons should have control of their own personal data[,]" even in a technology-focused world where personal information is often publicly available and incredibly valuable.[65] The protections are very broad—regulating the processing of personal data by an individual, a company, or an organization in the EU.[66] Personal data is also defined in broad terms as "any information" that, when collected together, could lead to an individual being identified,[67] including data that has been de-identified or encrypted through "pseudonymization," but could still be used to identify a person when put together with other information.[68] It forces all public data to be anonymized through an irreversible process.[69]

Additionally, the GDPR restricts any means of processing data in the public sphere, without freely-given consent by the individual in an effort to ensure the information collected is limited to what is necessary, accurate, secure, and not stored for longer than is

---

63 Charter of Fundamental Rights of the European Union, Dec. 7, 2000, 2000 O.J. (C 364/01) Art. 8(1).

64 Treaty on the Functioning of the European Union, Dec. 13, 2007, 2012 O.J. (C 326/10).

65 GDPR, *supra* note 5, at recital 7.

66 *See id.* arts. 1–2.

67 *Id.* art. 4(1).

68 *Id.* art. 26.

69 *Id.*

necessary.[70] It covers all international companies doing business in the EU that process data—whether automated or non-automated.[71] In particular, the GDPR goes further than other regulations in the rights given to the data subject. Article 14 allows the data subject to receive information regarding his or her collected personal data,[72] Article 15 allows the subject to access the data,[73] and Article 16 allows the data subject to rectify any inaccurate personal data "without undue delay."[74] Finally, Section 3, Article 17, "Right to Erasure ('right to be forgotten')," allows the data subject to erase certain personal information "without undue delay."[75] If the personal data is no longer necessary, consent is withdrawn by the subject, the data was unlawfully processed, or when the subject is a minor and his or her guardians did not provide consent, the data must be erased immediately upon request.[76] The GDPR places a high value on an individual's personal data, allowing each individual substantial freedom to control what information can be processed and when that data must then be erased.

Technology companies that rely on consumer data information have been forced to adapt in the EU. Consent must be "freely given, specific, informed, and unambiguous."[77] As one GDPR expert has termed, this has led to a new era of "beg data."[78] "Freely given" means that the data must be "truly optional."[79] "Specific" means that companies now must state exactly for what purpose they will

---

70 *Id.* arts. 4–5 (noting that the GDPR does not apply in the private sphere).

71 *What Constitutes Data Processing*, EUROPEAN COMMISSION, https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-constitutes-data-processing_en [https://perma.cc/K6ZD-6RXA] (defining processing as the "collection, recording, organization, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of personal data").

72 GDPR, *supra* note 5, art. 14 ("Information to be provided where personal data have not been obtained from the data subject").

73 *Id.* art. 15 ("Right of access by the data subject").

74 *Id.* art. 16 ("Right to rectification").

75 *Id.* art. 17, sec. 3 (Right to Erasure ("right to be forgotten")).

76 *Id.* (listing five exceptions to when personal data cannot be erased).

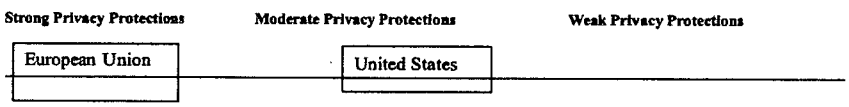
77 GDPR, *supra* note 5, art. 4.

78 Tim Walters, *Welcome To the Era of "Beg Data,"* LINKEDIN (Mar. 27, 2018), https://www.linkedin.com/pulse/welcome-era-beg-data-tim-walters-ph-d-/ [https://perma.cc/R2NN-2RLM].

79 *Consent*, GDPR EU, https://www.gdpreu.org/the-regulation/key-concepts/consent/ [https://perma.cc/P48Q-N5ZG].

use each piece of data.[80] Information collected can only be gathered for the purpose that is specifically laid out to the consumer.[81] "Informed" means that the company must use plain language that is unambiguous.[82] In other words, affirmative action such as checking an "accept" box must be taken; silence is not an option.[83] Therefore, companies must adjust to the new requirements and change how they collect and use data. They can no longer use any data for any purpose, but they must have a plan in place as to how they will collect and use consumer data. Spending has increased in order to navigate the GDPR and to comply with its restrictions. The GDPR proves that, through increased regulation, giant corporations can be tamed and the "data wild west" can be civilized.

B. United States



Similar regulations of individual data privacy do not exist in the federal system of the United States, placing the United States' system towards the middle of a data privacy spectrum.[84] The United States does not have any "centralized, formal legislation at the federal level;" instead, it follows a "sectoral approach" that relies on a combination of state-enacted regulations and self-regulation by businesses.[85] Federal statutes that do exist are aimed at specific

---

80 *Id.*

81 *Id.*

82 *Id.*

83 *Id.*

84 *See Data Protection Law*, LEGAL RESOURCES, https://www.hg.org/data-protection.html [https://perma.cc/F38J-TTY6].

85 *Id.* However, as noted in *Social Media Hearing, supra* note 1, Facebook and other technology companies are not quick to self-regulate. *See also* Mike Isaac, *Why Everyone Is Angry at Facebook Over Its Political Ads Policy*, N.Y. TIMES (Nov. 22, 2019), https://www.nytimes.com/2019/11/22/technology/campaigns-pressure-facebook-political-ads.html [https://perma.cc/ZN72-KW6R] (noting that Facebook will not fact-check political ads, but after lots of internal pressure, Google has decided to fact-check political ads). In general, when businesses are left to self-regulate, they are slow and often have a financial incentive, so it is unsettling to think that individual data privacy will be left for businesses to self-regulate under the current system in the United States.

sectors of the economy, and do not have the breadth of the GDPR.[86] Also contrary to the GDPR, the United States' hands-off approach allows the private sector to lead the way in data protection, encouraging individuals to self-regulate which companies and electronic sources have access to their personal information, and to what extent.[87]

Unlike the EU, which considers data privacy a guaranteed "fundamental" human right, the United States Constitution does not explicitly enumerate privacy as a fundamental right.[88] While privacy is implied in the penumbras of the Constitution, the Supreme Court has never held that data privacy is included as a fundamentally protected Constitutional right.[89] Several states have enacted legislation mirroring the protections of the GDPR in an effort to provide their constituents with greater transparency, notifications, and control over their data, but no federal legislation has been enacted.[90] The results yield great confusion over when protections must be afforded, and more money spent by companies to determine when and how privacy must be protected.[91] In fact, over 25% of U.S. companies have spent over $1 million since 2018 to ensure compliance with the GDPR—if they have businesses abroad—and state privacy protections, and 10% of companies have been forced to spend above $2.5 million.[92]

While most of these states have only enacted "breach

---

86 *Data Protection 2018: USA*, INTERNATIONAL COMPARATIVE LEGAL GUIDES (Dec. 6, 2018), https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa [https://perma.cc/NR7H-CAU6]. For example, federal laws protecting data privacy in the healthcare industry include the Health Insurance Portability and Accountability Act ("HIPAA") and the Genetic Information Nondiscrimination Act ("GINA"). The Fair Credit Reporting Act ("FCRA") regulates credit information and credit reports. Minors' data is specifically protected by the Family Educational Rights and Privacy Act ("FERPA") and the Children's Online Privacy Protection Act ("COPPA").

87 *Id.*

88 *See* U.S. CONST. amend. I.

89 *See* Griswold v. Connecticut, 381 U.S. 479, 484 (1965).

90 ALISSA M. DOLAN, CONG. RESEARCH SERV., R44326, DATA SECURITY AND BREACH NOTIFICATION LEGISLATION: SELECTED LEGAL ISSUES (2015) (noting specifically California leading the way with the California Consumer Privacy Act of 2018).

91 Michael Becker, *GDPR Compliance: How It's Affecting U.S. Companies*, EMARSYS, https://www.emarsys.com/resources/blog/gdpr-united-states-companies/ [https://perma.cc/CUN2-2NXE] (noting the increased spending to ensure compliance with the state-specific data privacy laws and regulations).

92 *Id.*

notification laws" that require businesses to alert their consumers when any personal information is compromised,[93] California has gone further by enacting the California Consumer Privacy Act of 2018 ("CCPA").[94] The CCPA resembles the GDPR because it: applies to domestic and international companies doing business in California; expands what qualifies as personal information; mandates disclosure to consumers regarding use of personal information; allows consumers to access information that details how their information is being used; prohibits businesses from changing how they treat consumers based on whether or what data they consent to share; and permits consumers to opt-out of sharing their data which, at times, must be completely erased.[95] Specifically, the CCPA restricts access to sensitive data without consent, and selling and sharing personal information like email addresses and telephone numbers.[96]

The CCPA was passed in response to massive breaches of personal information and, while not all fifty states have a breach notification law in place, other states may soon follow California's lead.[97] Further, with the recent congressional hearings involving social media sites,[98] it is possible that Congress could enact more sweeping data privacy legislation. For now, the United States' passive, piecemeal approach to regulation is not as protective as the GDPR, but it affords some moderate protections.

---

93 Serrato et al., *supra* note 54. *See also* Volodzko, *supra* note 2 (demonstrating the breach exposed more than half a billion guests and Marriott was required to report to consumers that their information was compromised).

94 Spencer Persson et al., *California Passes Major Legislation, Expanding Consumer Privacy Rights and Legal Exposure for US and Global Companies*, NORTON ROSE FULBRIGHT (June 29, 2018), https://www.dataprotectionreport.com/2018/06/california-passes-major-privacy-legislation-expanding-consumer-privacy-rights/ [https://perma.cc/MNJ2-CFNW].

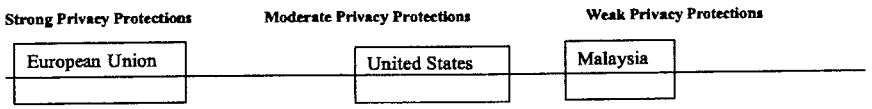
95 *Id.*

96 *Id.*

97 *Id. See also* Nuala O'Connor, *Reforming the U.S. Approach to Data Protection and Privacy*, COUNCIL ON FOREIGN RELATIONS (Jan. 30, 2018), https://www.cfr.org/report/reforming-us-approach-data-protection [https://perma.cc/88U2-4NUC] (reporting that data breaches at Equifax in 2017, Yahoo, and Deep Root Analytics' "accidental leak" paved the way for many of the state-enacted data breach laws).

98 *Social Media Hearing, supra* note 1.

C. *Malaysia*



On the other side of the data privacy spectrum—opposite the EU—are Malaysia and China. Malaysia was the first country to develop a Government Multi-Purpose Smart Card (MyKad)—similar to the Aadhaar Card in India—that incorporates services from various sectors of the government into a single card.[99] The card stores biographical information[100] and fingerprints.[101] The government's main uses for the MyKad card in 2018 were to confirm identities, births, and deaths, but the card has many more functions as well.[102] MyKad is used for email, e-banking, online transactions, electronic public services, business licenses, overseas travel, and other services, including highway tolls, public transportation, and even theme parks.[103] Separate cards are issued to children, immigrants, and temporary residents.[104]

There is little doubt among Malaysians that MyKad's ability to put all documents on a single card provides convenience, but having to carry an identity card everywhere—that identifies a person's immutable characteristics, including demographic and biographic information, health records, banking links, public transportation records, and digital identification mechanisms—is often associated with authoritarian regimes.[105] It is easy to conjure up many

---

99 *Introduction to MyKad*, *supra* note 55.

100 *See id.* The biographical information includes: Name, Address, Race, Citizenship Status, Religion, Marital Status, Criminal Record, and Fingerprint Minutiae. The type of biographical information, especially Race, Citizenship Status, and Religion separates MyKad users into groups based on personal immutable characteristics. Other biographical information includes "[b]asic health information such as blood type, allergies, organ implants, chronic diseases and information on beneficiary." *Id.*

101 *Id.*

102 *Statistics for Year 2018*, NATIONAL REGISTRATION DEPARTMENT OF THE MINISTRY OF HOME AFFAIRS, https://www.jpn.gov.my/en/statistic-2018/ [https://perma.cc/U5TG-F9SV].

103 *Introduction to MyKad*, *supra* note 55.

104 *See id.* (MyKID is for children; MyPR is for permanent residents; and MyKAS is for temporary residents).

105 Kuthubul Zaman Bukhari, *MYKAD & Privacy Rights*, THE MALAYSIAN BAR (Apr. 2, 2004),

instances in which a person's personal data can be used by a third party.[106] Now, with MyKad, all of that information is on a single card, where the chip can be "read," "recorded," and sold to third parties.[107]

In 2013, Malaysians received some limited protections through the Personal Data Protection Act 2010 ("PDPA").[108] However, the PDPA only prevents the misuse of personal data in commercial transactions, including "matters relating to the supply or exchange of goods or services, agency, investments, financing, banking and insurance."[109] It does not apply to the federal or state governments, leaving open the threat of malfeasance by the government.[110] "Big Brother" still has access to the data, without regulations because Malaysia does not have the protections like the GDPR.[111] There is no right of rectification if data is incorrect, no right to view that information, no right to consent to what information is made available, no restrictions on sale of data, and no right to be forgotten.[112] Simply, the PDPA protections are weak.

When he was asked about the lack of individual privacy, the MyKad project director simply stated that the personal information on a MyKad card "is no big deal and *doesn't compromise your privacy in any way* . . . military people have always carried a special ID and in no way has it impeded their freedom."[113] Recently, Human Resources Minister M. Kulasegaran recognized the security issues faced by the MyKad card, especially involving personal information, and stated he is "keen to update [the] MyKad

---

http://www.malaysianbar.org.my/index2.php?option=com_content&do_pdf=1&id=989 [https://perma.cc/GB76-Y9XW].

106 *See id.*

107 *See id.*

108 *See generally* Personal Data Protection Act, June 10, 2010, Act 709 (Malaysia) (noting some small protections to personal data such as in automatic commercial business transactions).

109 Muhammad Hafiz Mohd Shukri, *The Privacy and Security of an Identification Card: Malaysian Perspective*, MUNICH PERSONAL REPEC ARCHIVE 7 (July 30, 2015).

110 *Id.*

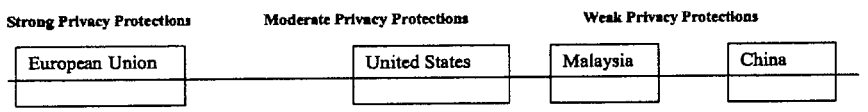
111 *See* Mathews Thomas, *Is Malaysia's MyKad the 'One Card to Rule Them All'? The Urgent Need to Develop a Proper Legal Framework for the Protection of Personal Information in Malaysia*, 28(2) MELBOURNE UNIV. L. REV. 474, 484–91 (2004).

112 *Id.*

113 *Id.* at 491 (quoting Wan Mohamad Ariffin Wan Ismail, MyKad project director) (emphasis in original).

identification card system with something similar to India's sophisticated Aadhaar model that uses unique random 12-digit numbers."[114] Even India's card, which this Article critiques for its few protections, affords more protections to Indian citizens than the MyKad card because MyKad does not even have minimal security protections from hackers, thieves, and third party data buyers. For now, without many security and privacy protections in place, Malaysia places more emphasis on government surveillance than it does on protecting an individual's data privacy.

D. China



A financial credit score is a common function in the United States that rates a person's financial trustworthiness to give investors an indication of risk, such as how likely repayment will be and at what rate the interest will be set. China is using "high-tech and big data"[115] to create a "social credit scoring system" that, much like its financial cousin, will rate your social trustworthiness and your risk to the government.[116] The Chinese system uses personal consumer data to gauge how likely an individual is to engage in unlawful activity and determines what social advantages they will have, including shorter hospital lines, better travel deals, and rental discounts.[117] Individuals with a lower social credit score may be restricted from buying luxury items, train and airline tickets, or an apartment, and they may be blocked from dating sites, or their children may be blocked from attending the best schools.[118] When the Chinese government glimpses that an individual buys diapers or

---

114 Zurairi AR, *Minister: Malaysia Eager to Swap MyKad with India's Aadhaar Biometric ID System*, MALAYMAIL (Oct. 15, 2018), https://www.malaymail.com/news/malaysia/2018/10/15/minister-malaysia-eager-to-swap-mykad-with-indias-aadhar-biometric-id-syste/1682938 [https://perma.cc/56VJ-FFYH].

115 *See What Is Big Data?*, BERNARD MARR, https://www.bernardmarr.com/default.asp?contentID=766 [https://perma.cc/XWS3-LHHX] ("The term 'Big Data' refers to the collection of all [internet, machine, human, and smart] data and our ability to use it to our advantage across a wide range of areas.").

116 Marr, *supra* note 6.

117 *Id.*

118 *Id.*

plays video games without using cheat codes, his credit score goes up; however, if he purchases alcohol or plays video games for most of the day, his social credit score may suffer.[119] Even the choice of online friends and one's community reputation will be a factor.[120]

The data used in compiling a social credit score comes from many sources, including basic personal information, financial records, health records, and all digital communication.[121] From the cookies in online sites to the information entered on company websites, the Chinese government is constantly watching and monitoring its citizens. The system tracks social media, voting records, legal issues, criminal history, tax history, financial history, health-tracking applications, GPS applications, personal relationships with family and friends, and uses facial recognition software to constantly track movements.[122]

China views the social credit system as a way to utilize the readily available big data and artificial intelligence ("A.I.") algorithms to "lead [China] to a new era in upstanding citizenry."[123] While online data in the United States is "curated, collected, monetized and sliced and diced in all sorts of ways," it is through the private sector, not through big government, and has little relation to individuals' interactions with other sectors of the economy.[124] For China, the social credit system is an integral part of the "socialist market economic system . . . [to] promote the tradition of integrity . . . [and] improve the integrity and credit level of the whole society."[125] China is attempting to reform the economic system, achieve scientific development, accelerate social transformation, and expand globalization efforts, and it sees the

---

119 *Id.*

120 Luke Dormehl, *We're Closer to China's Disturbing 'Social Credit System' Than you Realize*, DIGITAL TRENDS (Apr. 22, 2018), https://www.digitaltrends.com/cool-tech/social-credit-system/ [https://perma.cc/699K-MJRN].

121 Social Credit System, *supra* note 56.

122 Audrey Murrell, *Pushing the Ethical Boundaries of Big Data: A Look at China's Social Credit Scoring* System, FORBES (July 31, 2018), https://www.forbes.com/sites/audreymurrell/2018/07/31/pushing-the-ethical-boundaries-of-big-data-a-look-at-chinas-social-credit-scoring-system/#2ec7305525e5 [https://perma.cc/766F-A5QE].

123 Dormehl, *supra* note 120.

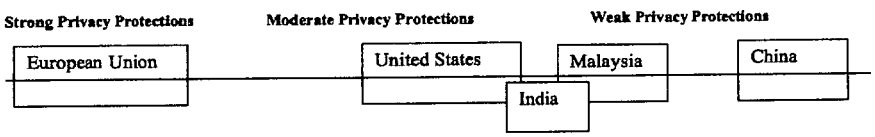
124 *See id.* (noting that Facebook and other social media giants have algorithms designed to filter out certain ideas, so an individual is left in "filter bubble").

125 Social Credit System, *supra* note 56.

social credit system as the way to develop the guiding ideology and principles that will be vital to its future development.[126] Much like Aadhaar, the government believes that the personal data gained from companies through technological advances will create ease in everyday tasks and allow for even greater wealth.

Critics of the social credit system describe big data as a nightmare, because citizens' lives will soon, if not already, revolve around their social credit worthiness, and they have no control over the information.[127] Critics also point to hacking concerns; however, when stories of hacking are raised, they are immediately deleted, and the dissenting whistleblowers quickly receive a negative change in their credit score.[128] "Big Brother" is in control over every facet of a Chinese citizen's life, and there is no individual say in what personal information is used by the government.[129] China's use of big data to restrict data privacy puts China on the opposite end of the data privacy spectrum from the EU.

IV. Placing India on the Data Privacy Spectrum



While most Western democracies have opposed any databases where personal individual information, including biometric data, is centralized, India has designed Aadhaar to use personal, sensitive, "big data" to "cut out the middleman, eradicate corruption and to ensure that subsidized goods and services reach the deserving recipients."[130] While Aadhaar is not that similar to the Social Credit

126 *Id.*

127 Marr, *supra* note 6.

128 *See* John Koetsier, *Hacking China's Social Credit: Cheaters Claim Million in Cash, Instant Promotions, and Preferential Dating*, MEDIUM (Aug. 7, 2018), https://medium.com/@johnkoetsier/hacking-chinas-social-credit-cheaters-claim-millions-in-cash-instant-promotions-and-87ad89ed5c6f [https://perma.cc/N9W5-3KHU] (noting a black market has been created where citizens pay cash to get their credit score raised).

129 Marr, *supra* note 6.

130 Jayesh Shinde, *How Does Aadhaar Compare with Other ID Systems in the World & How to Secure its Leaky Database*, INDIA TIMES LIFESTYLE NETWORK (July 19, 2019), https://www.indiatimes.com/technology/news/how-does-aadhaar-compare-with-other-id-systems-in-the-world-how-to-secure-its-leaky-database-276972.html

System, it raises many of the same data privacy concerns as the MyKad system,[131] placing India closer to Malaysia on a data privacy spectrum. First, Aadhaar, like MyKad, is designed for services across all sectors: from a welfare distribution system, to email, e-banking, and even social media.[132] Aadhaar provides easy access to a wide range of services.[133] However, needing to carry an identification card for everyday affairs is like carrying one's health records, public transportation records, banking information, and more sensitive information everywhere one goes.[134] This need for constant identification is often associated with authoritarian ideals.[135] Second, there is no protection against abuse by "Big Brother."[136] Like MyKad, the few data protections that do exist currently only apply to the use of sensitive information by private sector businesses.[137] Similarly, there is no right to consent to what information is made available.[138] While it is not yet mandatory to carry the Aadhaar card as proof of identity for Indian citizens,[139] an Aadhaar identity is becoming increasingly necessary for success in society.[140] India has not yet reached the point of GDPR-like protections.

The GDPR is the gold standard that countries should strive to

---

[https://perma.cc/D5CZ-7MB8].

131 *See id.*

132 *See, e.g.*, R. Dinakaran, *Skype Lite Integrated with Aadhaar*, HINDU BUS. LINE (Jan. 11, 2018), https://www.thehindubusinessline.com/info-tech/skype-lite-integrated-with-aadhaar/article9750022.ece [https://perma.cc/JE63-98LN].

133 *Id.*

134 Ayyar, *supra* note 12.

135 *See id.* This would be comparable to the United States requiring a driver's license that also includes health records, banking information, social security and passport numbers, immigration status, religious information, and more. It is easy to see how this type of information might be used by authoritarian regimes.

136 *Id.*

137 The Aadhaar Act, *supra* note 35.

138 *See id.* (There is no right to consent to what information is made available, and no right to be forgotten).

139 *See* Shinde, *supra* note 130 (explaining it is unlikely that India will take this step).

140 Priscilla Jebaraj, *The Aadhaar Holdouts: Living Life Without UID*, THE WIRE (June 2, 2017) https://thewire.in/tech/the-aadhaar-holdouts-profile [https://perma.cc/ZNK6-RL85] Th article shows instances where those without Aadhaar are being stranded by the government. Some instances include, not getting relief under the "Bonded Labour System Act," not securing government subsidies, and not being able to enroll a child in school.

achieve,[141] but the Aadhaar program conflicts with the goals of the international community. The Constitution of India protects "informational privacy,"[142] and assumes that Aadhaar protects informational privacy because of its fraud prevention measures.[143] Yet, no Indian law indoctrinates personal data privacy as a fundamental right, like the GDPR does.[144] Additionally, Aadhaar information is anonymized, but the process is reversible, as evidenced by the numerous data breaches.[145] Increasingly more sensitive information is included in the Aadhaar database, and more private companies require Aadhaar information as a way to check individual security.[146] Private companies profit on this information, without fully securing the information, which puts millions of citizens at risk.[147]

The global trend in democratic countries is to give more protections to individual data privacy;[148] however, India's Aadhaar system contradicts this trend by, instead, keeping India locked into the perception of being more like the state-restrictive system in Malaysia. India certainly does not come near China in terms of the restrictions on individual data privacy, but it must make certain to advance away from the surveillance state of its north-western neighbors. Aadhaar has not yet begun to influence social behavior by rewarding compliance and punishing those with social disadvantages, but the Aadhaar system does interact with other sectors of the economy.[149] The goals of the Aadhaar system and China's Social Credit System also align—both governments cite their respective systems being vital to future development.[150] The ease of providing services to citizens and the ability to know what

---

141 *See generally*, UNCTAD, *supra* note 58, at 32–34 (discussing the GDPR).

142 Constitution of India, art. 21. *See also Puttaswamy*, Writ Petition No. 494 of 2012, at 164.

143 Charter of Fundamental Rights of the European Union, Dec. 7, 2000, 2000 O.J. (C 364/01) Art. 8(1).

144 *Id.*

145 *See* Khaira, *supra* note 31.

146. *See* Jebaraj, *supra* note 140 (explaining that "private micro-payment systems, airline and telecom companies, and more are demanding Aadhaar information to ascertain your identity").

147 *See* Khaira, *supra* note 31.

148 *See* GDPR, *supra* note 5; Perkins, *supra* note 54; Serrato et al., *supra* note 54.

149 Dormehl, *supra* note 120.

150 *See* Social Credit System, *supra* note 56; *see also* Ayyar, *supra* note 12.

citizens need are the underpinnings of each system.[151] The Aadhaar system is not as intrusive as the Social Credit System; however, India must take active steps to avoid the possible abusive behavior by bad actors who may use the Aadhaar system to open the door to data privacy exploitation, as seen in China today. Luckily, India's government has recognized many of the issues with Aadhaar and has proposed steps to secure individual data.

A. Steps by India's Legislature: "A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians"

India's legislature seems to have already recognized some potential problems, and is in the process of taking concrete steps to solve its data privacy issues by borrowing many ideas from the GDPR.[152] The government appointed former Indian Supreme Court Justice, BN Srikrishna, to chair the Committee of Experts on a Data Protection Framework for India ("Committee") to "create the legal framework for data protection and data privacy in India."[153] The race for individual data in the wild west of big data is much like the gold rush, and the Committee has sought to secure these data privacy rights for the Indian citizens before data is no longer private.

The Committee released a proposed 200-page-plus bill to the legislature in July 2018.[154] It recognized the benefits of big data on India's citizens, including the ease, range, and affordability of services that could be provided one day.[155] However, the

---

151 *See* Social Credit System, *supra* note 56; *see also* Ayyar, *supra* note 12.

152 Sindhuja Balaji, *India Finally has a Data Privacy Framework—What Does it Mean for its Billion-Dollar Tech Industry?*, FORBES (Aug. 3, 2018), https://www.forbes.com/sites/sindhujabalaji/2018/08/03/india-finally-has-a-data-privacy-framework-what-does-it-mean-for-its-billion-dollar-tech-industry/#6baf4d6870fe [https://perma.cc/LE2M-GTSW].

153 Shushant Jha, *The Personal Data Protection Landscape in Developing Countries*, IBM CLOUD BLOG (Jan. 22, 2019), https://www.ibm.com/blogs/bluemix/2019/01/indias-journey-to-personal-data-protection-and-data-privacy-law/ [https://perma.cc/M64T-LQCA].

154 Srikrishna, *supra* note 8. The proposed bill has since been tabled for the time being.

155 *See generally id.* at 98–106 (outlining a few benefits from the Aadhaar system). *See also* Arghya Sengupta, *A Free & Fair Digital Economy: Draft Data Protection Bill Asserts Our Sovereignty and Safeguards Citizens' Interests*, TIMES OF INDIA (July 30, 2018), https://timesofindia.indiatimes.com/blogs/toi-edit-page/a-free-fair-digital-economy-draft-data-protection-bill-asserts-our-sovereignty-and-safeguards-citizens-interests/ [https://perma.cc/85JA-9HUG] (breaking down the intricacies of the 200-page

Committee cautioned that the harms associated with using big data include unexpected data sharing, tracking online behavior—including on intimate matters—and breaches of privacy.[156] The premise of the report is based on the Aadhaar case, *Puttaswamy v. Union of India*, and the holding that individual privacy is a fundamental right, but allowing the Aadhaar system to continue cautiously.[157]

There are four primary actions that the Committee recommended. First, the entity that seeks an individual's data is given a fiduciary role which, much like the GDPR, demands the entity respect the data entrusted to it.[158] This allows data subjects to hold the third-party liable if their data is misused in any way, and requires that data subjects be notified if their data is breached or used without permission.[159] Second, entities can only collect the information that is necessary to the service that the company provides.[160] For example, Facebook cannot collect healthcare information because that is not necessary to the social media service that it provides, but it could collect—with permission—data relating to internet cookies that could be used to improve their services.[161] Third, the committee recommended establishing a Data Protection Authority ("DPA") to adjudicate data privacy claims and both penalize entities and award damages to individuals.[162] The bill would prevent all "sensitive data" from being stored in a central facility; instead, the bill mandates that all personal, sensitive data be locally stored, restricting Big-Brother-type-data-use.[163] Finally, like the GDPR, the Committee recommends limited instances of data erasure.[164] However, unlike the EU's "Right to be Forgotten," the Committee only recommended the right of erasure when using personal data becomes "unlawful or unwarranted" because "the

---

report).

156 *Id.*

157 *See* K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1, 164 (India).

158 *See* Srikrishna, *supra* note 8, at 49–67.

159 *Id.* at 67.

160 *See id.* at 35 (For instance, a ride-sharing app would not generally be able to access my text message data.).

161 *See id.*

162 *Id.* at 166.

163 *Id.* at 97.

164 Srikrishna, *supra* note 8, at 75.

right to privacy [must] be balanced with the freedom of speech."[165]

Specifically related to the Aadhaar Act, the Committee recognized the large impact on informational privacy.[166] It strongly advocated for immediate changes to protect against "companies wrongly insisting on Aadhaar numbers, [] using Aadhaar numbers for unauthorised purposes and [] leaking Aadhaar numbers."[167] The Committee recommended two major solutions to this problem. First, the Aadhaar Act must be amended to set up two groups of entities—those allowed to access Aadhaar information online and those restricted to verifying identities offline only—in an attempt to prevent Aadhaar data breaches.[168] The legislature must decide on a limited group of entities, central to national interests that have access to the online identification, but the Committee recommended that private companies be completely excluded, relying exclusively on verifying identities offline.[169]

Second, since over 1.3 billion people have Aadhaar cards, and many services require Aadhaar identification, the legislature must create a regulatory framework that includes the ability for the DPA to hear and enforce complaints regarding the misuse of data.[170] The Aadhaar number should be added to the list of "sensitive personal data," to prevent private entities from storing that information and to prevent foreign companies from accessing that information.[171] The second part of this recommendation is of particular importance. If a company wants to process Aadhaar data for security checks, or if a company wants to store any general, non-sensitive information, it must set up a physical location in India.[172] For example, Facebook, to store any general information, even if it is not sensitive, would have to set up a physical location in India to store the Indian citizen's data.[173] Facebook would not be able to store Indian data in the United States or elsewhere.

The Committee's proposed legislation would increase the *data*

---

165 *Id.* at 76.

166 *Id.* at 99

167 *Id.*

168 *Id.* at 99–100.

169 *Id.* at 100.

170 Srikrishna, *supra* note 8, at 100.

171 *Id.* at 26.

172 *Id.* at 97.

173 *See id.*

security of the Aadhaar program, compartmentalize the information, and increase the regulatory framework. While the changes would likely decrease data breaches, it does not sufficiently address data privacy concerns—what information can be accessed by private entities and what restrictions exist on the central government's access.

V. Conclusion

Implementing the Committee's recommendations would significantly improve India's protection of individual data privacy. The proposed legislation reflects much of what the GDPR regulates: citizens must consent to information being shared, personal information cannot leave the country without certain precautions, and individuals have a right to legal action when personal data is misused.[174] However, while the Committee recognized a right to be forgotten, its proposal limits when information may be erased by balancing the right of erasure against competing rights and interests, including freedom of speech.[175] The individual must formally request erasure through the DPA adjudication process, and erasure must only be performed when it is absolutely necessary to protect the individual.[176] Additionally, the Committee's data breach proposal does not go far enough in protecting the privacy of its citizens.[177]

While the Aadhaar system has and will continue to provide citizens with immense benefits, there needs to be increased regulation with regard to how the system protects data privacy. The proposed legislation by the Committee is a start, but there are many questions that remain unanswered and a lot of work that must be done.

One issue that has jumped to the forefront of Aadhaar is how the act will interact with the Citizenship Amendment Act ("CAA").[178] The CAA permits religiously prosecuted "Hindu, Sikh, Buddhist, Jain, Parsi or Christian [persons] from Afghanistan, Bangladesh or

---

174 *See generally* GDPR, *supra* note 5. More detailed discussion is contained in the discussion of the GDPR in Part II(a).

175 Srikrishna, *supra* note 8, at 77–80.

176 *Id.*

177 *See id.* at 62–67 (discussing the recommendations of data breach laws).

178 The Citizenship Act, 1955, No. 57 of 1955, § 14A, as amended by The Citizenship (Amendment) Act, No. 47 of 2019, INDIA CODE (2019).

Pakistan. . ." to receive protections in India.[179] These minority groups will not be treated as illegal immigrants and the naturalization requirement is reduced from eleven to five years of residency.[180] The Act excludes Muslims from protection, further separating religious communities by further splitting the country into Hindu vs Muslim.[181] Some Muslim residents, who have lived in India for multiple generations, are denied the benefits of an Aadhaar card because their birth certificates do not denote Indian genealogy.[182] President Modi, who campaigned against big government and government interference, has increased data surveillance, in part through Aadhaar. While the Supreme Court stated that "[t]he Aadhaar number . . . shall not, by itself, confer any right of, or be proof of, citizenship or domicile in respect of an Aadhaar number holder[,]"[183] the CAA designates the Aadhaar card as one way to prove citizenship.[184] Data privacy protections grow more important as the reach of the Aadhaar system is used as a tool for religious discrimination.

Additionally, the proposed regulations should go further to guarantee more data that can be erased, increase opportunities to consent to data, limit private sector access to prevent against security breaches, and apply strict limits to data access and use by the central government. India's constitution values privacy as a fundamental right, so data privacy should be protected as such. There is a push and pull between the proposed legislation and Aadhaar and currently, the legislation has been tabled by the Indian Parliament. If India truly desires to "shape the global digital landscape of the 21st century, it must formulate a legal framework relating to personal data that can work as a template for the developing world."[185] As the world of technology continues to

---

[179] *Id.* at § 2.

[180] *Id.*

[181] *See* Sagarika Ghose, *CAA, Aadhaar or data bill: In India, it is state vs citizen*, THE TIMES OF INDIA (Dec. 22, 2019), https://timesofindia.indiatimes.com/blogs/bloody-mary/caa-aadhaar-or-data-bill-in-india-it-is-state-vs-citizen/ [https://perma.cc/7AKA-NQLQ].

[182] Rahul Tripathi, Citizenship Amendment Act 2019: What it holds for India, THE ECONOMIC TIMES (Dec. 23, 2019) https://economictimes.indiatimes.com/news/politics-and-nation/citizenship-amendment-bill-decoded-what-it-holds-for-india/articleshow/72466056.cms?from=mdr [https://perma.cc/9X6X-3XEB].

[183] The Aadhaar Act, *supra* note 35 at ch. III (9).

[184] Ghose, *supra* note 181.

[185] *Id.* at 3.

grow, India has the ability to lead the revolution. India must institute protections so that Aadhaar can be beneficial while also upholding its citizens' fundamental right of privacy.