University of Miami Law Review

Volume 73
Number 2 *Symposium Hack to the Future: How Technology is Disrupting the Legal Profession*

Article 10

2-5-2019

Biometric Identification in India Versus the Right to Privacy: Core Constitutional Features, Defining Citizens' Interests, and the Implications of Biometric Identification in the United States

Madison Julia Levine

Biometric Identification in India Versus the Right to Privacy: Core Constitutional Features, Defining Citizens' Interests, and the Implications of Biometric Identification in the United States

MADISON JULIA LEVINE*

In 2009, the Indian government introduced a widespread biometric identification system called Aadhaar—a national scheme that issues Indian citizens and residents a unique identification number while collecting and storing their most personal biometric and demographic information. As the Aadhaar system was implemented and promoted in India, widespread concerns grew regarding the storage and protection of such private information. How can Indian citizens enforce and protect their privacy rights? In 2017, the Indian Supreme Court attempted to address this issue by holding that an individual's right to privacy is an inherent part of the right to life and personal liberty and is therefore implied under Article 21 of the Indian Constitution.

---

* J.D. Candidate 2019, University of Miami School of Law; B.S. 2012, University of Miami. I dedicate this Comment to my late father, Judge Steve Levine, who is my constant motivation to excel in Law School. I know he is always watching over me and would be so proud. I want to especially thank my mother, Tracy Howard, for being an unwavering pillar of strength, support, and guidance. It was my mom who encouraged me to explore who I am, make mistakes, be spontaneous, and embrace the joy of living. She allowed me to travel at a young age and it was one such travel adventure in Southern India that sparked the idea for this Comment. I want to thank my uncle, Jon (Tío), who helped me with the writing process. A big thank you to Frank Halpern who I bounced ideas off of and who supported and comforted me even during my most stressed out moments. I want to thank my faculty advisor, Scott Sundby, for being an inspiring professor and assisting me with the focus and scope of my writing. Finally, thank you to the *University of Miami Law Review* for choosing my Comment for publication and working so diligently throughout the editing process.

Following the Supreme Court of India's declaration that privacy is a fundamental right, the idea of a general-purpose identification database is constitutionally questionable. As there is no comprehensive legal framework for privacy protection and no explicit constitutional right to privacy in India, one must ask: is the Indian government violating individual privacy rights through Aadhaar? Regardless of this concern, in 2018 the Indian Supreme Court declared Aadhaar constitutional in connection to the mandatory linking of Aadhaar numbers with all government welfare schemes and services. In light of this decision, this Comment advocates that the Aadhaar system should have been deemed unconstitutional as a violation of individual privacy rights.

Additionally, with the growth of interconnected technology, it is important to address the consequences of a system like Aadhaar in the United States. How would a similar identification system function and would such a system even be deemed constitutional? To maintain a liberal democratic society that values and upholds privacy rights, the United States should avoid proposing such a system, no matter how beneficial or convenient it may seem.

INTRODUCTION 620
I. CORE PRIVACY RIGHTS UNDER THE INDIAN CONSTITUTION .. 621
II. THE UNITED STATES CONSTITUTION AND THE RIGHT TO PRIVACY 628
III. INDIA'S AADHAAR SYSTEM: A SPECIFIC PRIVACY ISSUE 634
A. *The Aadhaar System* 634
B. *Pros of the Aadhaar System* 636
C. *Cons of the Aadhaar System* 638
IV. CONSTITUTIONALITY OF THE AADHAAR SYSTEM 641
A. *The Aadhaar Act 2016* 641
B. *Information Collection and the Legality of the Aadhaar Act* 644
C. *Biometric Data Collection* 645
D. *Constitutional Challenge Analysis* 646
E. *New Legislative Proposals* 648
V. IMPLICATIONS OF AN AADHAAR-LIKE SYSTEM IN THE UNITED STATES 649
CONCLUSION 653

INTRODUCTION

The right to privacy was characterized in the United States during the late nineteenth century simply as the "right to be let alone."[1] Since then, the right to privacy has expanded into something much greater due to—among other sociopolitical changes—emerging technology and information systems, which have wrought a complex set of issues that illuminate the core definitional features of privacy in the twenty-first century.[2] Alan Westin, a scholar who surveyed and set the boundaries of privacy under the United States Constitution for a half-century, said that "[p]rivacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[3] In 1989, the United States Supreme Court stated that privacy is one's "control over information concerning his or her person."[4] Similarly, President Bill Clinton's National Information Infrastructure Task Force defined privacy as "an individual's claim to control the terms under which personal information—information identifiable to the individual—is acquired, disclosed, and used."[5] By any definition today, privacy includes the "ability of an individual or a group to seclude themselves or information about themselves and thereby reveal themselves selectively."[6] Accordingly, the definition that will be used throughout this Comment to encompass privacy rights in the modern international system can be stated as follows: privacy is the right to control the dissemination of personal

---

[1] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 205 (1890).

[2] Justice K.S. Puttaswamy (Retd.) v. Union of India (*Puttaswamy I*), Writ Petition (Civil) No. 494 of 2012, 1 (Sup. Ct. India Aug. 24, 2017) (describing issues such as data mining, data collection, algorithms, internet browsing, and online banking). A subsequent Indian Supreme Court decision was reached in 2018 and is referred to as *Puttaswamy II*.

[3] ALAN WESTIN, PRIVACY AND FREEDOM 7 (1967); *see* Karen Sparks, *Alan Furman Westin*, ENCYCLOPEDIA BRITANNICA, https://www.britannica.com/biography/Alan-Westin (last updated Dec. 14, 2018); *see also* Tabrez Ahmad et al., Right of Privacy: Constitutional Issues and Judicial Responses in USA and India, Particularly in Cyber Age 11 (2009) (unpublished manuscript), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1440665.

[4] U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 763 (1989).

[5] Ahmad et al., *supra* note 3, at 11.

[6] *Id.* at 2.

information.

This Comment addresses two primary questions. First, does India's biometric identification system violate constitutional privacy protection? Second, what are the implications of enacting a similar system in the United States? There is also the related issue of what occurs when one cannot control the dissemination of personal information. How will our privacy rights be protected and upheld? This Comment approaches these questions and issues in the context of India's Aadhaar scheme—a national identification system that issues Indian citizens and residents a unique ID number while collecting and storing their most personal biometric and demographic information.[7]

This Comment advocates for new, comprehensive privacy protections under Indian law in light of the 2017 Indian Supreme Court decision *Puttaswamy v. Union of India (Puttaswamy I)*, which upheld the right to privacy as fundamental under the Constitution of India.[8] Part I of this Comment discusses privacy rights under the Indian Constitution, including previous and current case law addressing this issue. Part II explores privacy rights under the United States Constitution and prior jurisprudence that developed this topic, as well as alternative views on constitutional interpretation. Part III highlights the specific issues associated with Aadhaar ID cards, including the pros and cons of the personal identification system. Part IV analyzes the constitutionality of current Aadhaar legislation in India and suggests changes in the law. Finally, Part V explores the implications and consequences of implementing a similar national identification system in the United States.

I. CORE PRIVACY RIGHTS UNDER THE INDIAN CONSTITUTION

Fundamental rights such as life, dignity, personal liberty, happiness, and freedom arise out of societal custom and are memorialized in constitutions and legislation.[9] Such rights have been described as basic, primordial, or inalienable rights and in modern democratic

---

[7] *See infra* Part III.

[8] *Puttaswamy I*, Writ Petition (Civil) No. 494 of 2012 1, 262–63 (Sup. Ct. India Aug. 24, 2017; *see infra* Part I.

[9] *See Puttaswamy I*, Writ Petition (Civil) No. 494 of 2012 at 23 (Bobde, J., concurring).

countries, cannot be "abridged or curtailed totally by ordinary legislation" or the acts of elected officials.[10] The framers of the Constitution of India believed that liberty cannot be fully enjoyed without the guarantee of certain freedoms.[11] The very purpose of creating a written Indian Constitution was to "secure justice, liberty, and equality to the people of India."[12]

As such, the Constitution of India contains provisions "specifying and identifying certain rights" for its citizens.[13] In attempting to understand and solidify these essential rights, it is important to look to the written text of the Constitution for a deeper understanding.[14] Such freedoms can be found in the words of the Preamble and Part III (Fundamental Rights) of the Indian Constitution, which includes Articles 14, 19, and 21.[15] These Articles enumerate a specific and precise list of rights, including the following: the right to equal protection,[16] freedom of speech and expression, freedom of movement,[17] life, and personal liberty.[18] Nevertheless, an exact constitutional provision containing a fundamental right of privacy is lacking, creating a discord of court opinions concerning the privacy rights of

---

[10] *Puttaswamy I*, Writ Petition (Civil) No. 494 of 2012 at 22–23 (Chelameswar, J., concurring).

[11] *Id.* at 24.

[12] *Id.*

[13] *Id.* at 22.

[14] *See id.* at 21.

[15] INDIA CONST. pmbl. ("We, the People of India, having solemnly resolved to constitute India into a sovereign socialist secular democratic republic and to secure to all its citizens: Justice, social, economic, and political; Liberty of thought, expression, belief, faith, and worship; Equality of status and opportunity; and to promote among them all fraternity assuring the dignity of the individual and the unity and integrity of the Nation."); *id.* art. 14 ("The State shall not deny to any person equality before the law or the equal protection of the laws within the territory of India."); *id.* art. 19 ("All citizens shall have the right to freedom of speech and expression; to assemble peaceably and without arms; to form associations or unions or co-operative societies; to move freely through the territory of India; to reside and settle in any part of the territory of India; and to practice any profession, or to carry on any occupation, trade or business."); *id.* art. 21 ("No person shall be deprived of his life or personal liberty except according to procedure established by law.").

[16] *Id.* art. 14.

[17] *Id.* art. 19.

[18] *Id.* art. 21.

Indian citizens.[19]

However, on August 24, 2017, the Indian Supreme Court decision in *Puttaswamy v. Union of India (Puttaswamy I)*[20] brought some clarity to the issue of fundamental privacy rights. Prior to *Puttaswamy I*, there was a general understanding of an implied right to privacy in India, but its boundaries remained imprecise.[21] For example, the ancient and religious texts of India contained a well-developed sense of privacy.[22] In the *Ramayana* (an ancient Indian epic poem), a woman should not be seen by a male stranger, and the *Grihya Sutras* (sacred Hindu texts concerning domestic rituals) describe the correct way to build one's home to protect privacy.[23] Members of one particular Hindu denomination, known as the *Ramanuj Sampradaya*, refuse to eat or drink in the presence of others.[24] Despite the evident historical emphasis on privacy, the Court in *Puttaswamy I* solidified this legal issue by holding that an individual's right to privacy is an inherent part of the right to life and personal liberty and therefore is implied in Article 21 of the Indian Constitution.[25]

In the judgment, Justice Chandrachud declared that privacy is an intrinsic right to life and liberty.[26] This judgment arose as a reaction to the overarching presence of state and private actors attempting to regulate individual freedoms.[27] There was a need to address privacy

---

[19] Ujwala Uppaluri & Varsha Shivanagowda, *Preserving Constitutive Values in the Modern Panopticon: The Case for Legislating Toward a Privacy Right in India*, 5 NUJS L. REV. 21, 33, 42–44 (2012).

[20] *Puttaswamy I*, Writ Petition (Civil) No. 494 of 2012.

[21] Graham Greenleaf, *Confusion as Indian Supreme Court Compromises on Data Privacy and ID Number*, 137 PRIVACY LAWS & BUS. INT'L REP. 24, 24–26 (2015).

[22] *Puttaswamy I*, Writ Petition (Civil) No. 494 of 2012 at 21 (Bobde, J., concurring).

[23] *Id.*

[24] *Id.*

[25] *Puttaswamy I*, Writ Petition (Civil) No. 494 of 2012 at 262 (majority opinion) ("Privacy is a constitutionally protected right which emerges primarily from the guarantee of life and personal liberty in Article 21 of the Constitution."); INDIA CONST. art. 21. (stating that "no person shall be deprived of his life or personal liberty except according to procedure established by law".)

[26] *Puttaswamy I*, Writ Petition (Civil) No. 494 of 2012 at 262–63; *Right to Privacy a Fundamental Right, Says Supreme Court in Unanimous Verdict*, WIRE (Aug. 24, 2017), https://thewire.in/170303/supreme-court-aadhaar-right-to-privacy/.

[27] *Puttaswamy I*, Writ Petition (Civil) No. 494 of 2012 at 4–5.

rights in the context of the changing technological landscape of India, where the debate on privacy was "being analyzed [within] the context of a global information based society."[28] The task before the Court was to "impart constitutional meaning to individual liberty in an interconnected world."[29] As Justice Chelameswar stated in his concurring opinion, "fundamental rights are the only constitutional firewall to prevent [state] interference with those core freedoms constituting liberty of a human being."[30] His concurrence concluded by emphasizing that the right to privacy is a core freedom and is part of the meaning of liberty within Article 21.[31]

The *Puttaswamy I* judgment recognized the importance and value of privacy as a constitutional entitlement, not through the process of amendment, but through judicial interpretation by determining the nature and the extent of the freedoms available to each person protected under the Indian Constitution.[32] The Court looked to Article 21 to interpret and establish this fundamental right.[33] Justice Chandrachud explained that the right to privacy is implicit in the right to life and liberty guaranteed to citizens by Article 21 and that citizens have a right to safeguard that privacy.[34] Justice Bobde further expounded that the original and proper home for a right of privacy is in Article 21 at the very core of personal liberty and life itself.[35] He stated that "[l]iberty and privacy are integrally connected in a way that privacy is often the basic condition necessary for exercise of the right of personal liberty."[36] Earlier in the opinion, Justice Bobde asserted that an individual must ensure his or her privacy in order to experience fulfillment and happiness and to perform at the highest level.[37]

The Court also turned to the Preamble of the Indian Constitution

---

[28] *Id.*

[29] *Id.*

[30] *Puttaswamy I*, Writ Petition (Civil) No. 494 of 2012 at 40 (Chelameswar, J., concurring).

[31] *Id.* at 40–41.

[32] *Puttaswamy I*, Writ Petition (Civil) No. 494 of 2012 at 109–10 (majority opinion).

[33] *Id.*

[34] *Id*. at 51–52.

[35] *Puttaswamy I*, Writ Petition (Civil) No. 494 of 2012 at 25 (Bobde, J., concurring).

[36] *Id.*

[37] *See id.* at 23.

in interpreting privacy as a fundamental right.[38] In reference to the Preamble, Chief Justice Khehar explained "the constitutional vision seeks the realization of justice (social, economic and political); liberty (of thought, expression, belief, faith, and worship); equality (as a guarantee against arbitrary treatment of individuals); and fraternity (which assures a life of dignity to every individual)."[39] The principles enumerated in the Preamble exist cohesively to "facilitate a humane and compassionate society."[40] By focusing on human dignity in realizing fundamental individual rights, the "collective well-being of the community is determined," ensuring that Indian society is a reflection of dignity, fairness, liberty, and justice.[41] Chief Justice Khehar claimed that such reflections are also found in Article 14 (equal protection), Article 19 (guarantees of freedom), and Article 21 (the right to life and personal liberty) of the Constitution.[42]

Justice Sapre further explored this concept, stating that the significance of the Preamble was to focus on two aspects—first, "the unity of the Nation" and second, the "dignity of the individual."[43] Both expressions are interdependent and intertwined in that the Nation is required to respect the freedom and ability to attain self-fulfillment of every individual.[44] Dignity of both the individual and the Nation is considered essential to the fraternity of the Indian people.[45] Justice Sapre found no difficulty in tracing the right to privacy as emanating from two expressions of the Preamble: "liberty of thought, expression, belief, faith and worship" and "fraternity assuring the dignity of the individual."[46] Additionally, he also found that the right to privacy emanates from Article 19(1)(a), which gives to every citizen "a freedom of speech and expression," Article 19(1)(d), which gives to every citizen "a right to move freely

---

[38] INDIA CONST. pmbl.

[39] *Puttaswamy I*, Writ Petition (Civil) No. 494 of 2012 at 94 (majority opinion).

[40] *Id.*

[41] *Id.*

[42] INDIA CONST. arts. 14, 19, 21; *Puttaswamy I*, Writ Petition (Civil) No. 494 of 2012 at 94.

[43] *Puttaswamy I*, Writ Petition (Civil) No. 494 of 2012 at 6 (Sapre, J., concurring).

[44] *Id.*

[45] *Id.* at 7.

[46] *Id.* at 19.

throughout the territory of India," and finally, from the expression "personal liberty" under Article 21.[47] The right to privacy is intertwined with these expressions and "flows from each of them and in juxtaposition."[48]

Importantly, the Indian Supreme Court's decision in *Puttaswamy I* overruled the holdings of the 1954 case *M.P. Sharma v. Satish Chandra* and the 1962 case *Kharak Singh v. State of Uttar Pradesh*, both of which were landmark decisions holding that the right to privacy is not protected under the Indian Constitution.[49] In *M.P. Sharma*, the Indian government seized documents belonging to a company suspected of falsifying records.[50] Sharma challenged the constitutional validity of the search and seizure, claiming that it violated his fundamental rights under Article 19(1)(f), the right to acquire, hold, and dispose of property, and Article 20(3), protection against self-incrimination.[51] The Court in *M.P. Sharma* held that in the absence of a provision similar to the Fourth Amendment of the United States Constitution, the right to privacy could not be read into the provisions of Article 20(3) of the Indian Constitution.[52] Although Article 19(1)(f) was also in question, the Court only rejected the right to privacy in the context of searches and seizures of documents.[53] The Court took a narrow and formalistic approach, stating

---

[47] *Id.*

[48] *Id.* at 20.

[49] *Puttaswamy I*, Writ Petition (Civil) No. 494 of 2012 at 261 (majority opinion); M.P. Sharma v. Satish Chandra, District Magistrate, Delhi (1954) 1 SCR 1077, 1096–97 (India); Kharak Singh v. State of U.P., (1964) 1 SCR 332, 351 (India).

[50] *M.P. Sharma*, 1 SCR at 1079–80; Ananthakrishnan G, *M P Sharma and Kharak Singh: The Cases in Which SC Ruled on Privacy*, INDIAN EXPRESS (July 19, 2017), http://indianexpress.com/article/explained/m-p-sharma-and-kharak-singh-the-cases-in-which-sc-ruled-on-privacy-4756964/.

[51] *M.P. Sharma*, 1 SCR at 1080–81 (discussing INDIA CONST. arts. 19, 20).

[52] INDIA CONST. art. 20, § 3; *Puttaswamy I*, Writ Petition (Civil) No. 494 of 2012 at 261; *see* Gautam Bhatia, *State Surveillance and the Right to Privacy in India: A Constitutional Biography*, 26 NAT'L L. SCH. INDIA REV. 127, 130 (2014).

[53] *See* Bhatia, *supra* note 52, at 128. *But see* Govind v. State of M.P., (1975) 3 SCR 946, 951–56 (suggesting that there is a zone of privacy that is protected under the Indian Constitution).

that India has no equivalent of the American Fourth Amendment's specific prohibition of unlawful searches.[54]

The decision in *M.P. Sharma* did not specifically adjudicate whether a right to privacy would arise from any other constitutional provision such as the rights guaranteed by Article 19 or Article 21.[55] The decision only held that a right to privacy cannot be read into the Indian Constitution under Article 20(3).[56] Accordingly, the holding could not be interpreted to specifically exclude the protection of privacy under the framework of constitutional guarantees including those in Articles 19 or 21.[57] *M.P. Sharma* left undetermined whether a constitutional right to privacy is protected by other provisions of the Indian Constitution, leaving room for future judicial interpretation.[58] Therefore, in the absence of an express constitutional guarantee of privacy, the Court could still consider whether privacy is an element of personal liberty, a part of human dignity, or understood within the protection of human life.[59]

In *Kharak Singh*, the petitioner challenged the constitutionality of police monitoring.[60] After being released from custody for lack of evidence, the petitioner was placed under police surveillance, which included unannounced home visits, movement reports, and periodic inquiries into his communications.[61] Singh challenged the constitutionality of the surveillance, claiming that it violated his fundamental rights of freedom of movement under Article 19(1)(d) and the protection of life an personal liberty under Article 21.[62] The Court held that the content of the expression "life and personal liberty" under Article 21 is a guarantee against intrusion into personal

---

[54] Bhatia, *supra* note 52, at 128; Sheetal Asrani-Dann, *The Right to Privacy in the Era of Smart Governance: Concerns Raised by the Introduction of Biometric-Enabled National ID Cards in India*, 47 J. INDIAN L. INST. 53, 62 (2005).

[55] INDIA CONST. art. 19 (protecting freedom of speech and expression, the ability to move freely through the territory of India, and to practice any profession, or to carry on any occupation, trade or business); *Puttaswamy I*, Writ Petition (Civil) No. 494 of 2012 at 262 (majority opinion).

[56] *Puttaswamy I*, Writ Petition (Civil) No. 494 of 2012 at 262.

[57] *Id.*

[58] *Id.*

[59] *Id.*

[60] Kharak Singh v. State of U.P., (1964) 1 SCR 332, 336 (India); Ananthakrishnan G, *supra* note 50.

[61] *Kharak Singh*, 1 SCR at 337–39; Ananthakrishnan G, *supra* note 50.

[62] *Kharak Singh*, 1 SCR at 336.

security.[63] The Court further held that unauthorized entrance into a person's home is a violation of that fundamental right to personal liberty.[64] However, the Court refused to accept an infringement of Article 19, stating that unannounced visits did not impede Singh's movements, and therefore did not abridge his personal liberty or privacy.[65]

As such, the second part of the decision in *Kharak Singh*, which invalidated home visits on the ground that they violated personal liberty under Article 21, seems to be an implicit recognition of the right to privacy.[66] However, the first part of the decision, emphasizing that the right to privacy is not a guaranteed right under the Indian Constitution, invalidates the right to privacy as a fundamental freedom.[67]

The 2017 Supreme Court decision in *Puttaswamy I*,[68] which directly addresses whether the right to privacy is a fundamental right under the Indian Constitution, overrules both *M.P. Sharma* and *Kharak Singh*, creating a new stage on which to analyze and adjudicate privacy issues in India.

II. THE UNITED STATES CONSTITUTION AND THE RIGHT TO PRIVACY

Similar to the Indian Constitution, the United States Constitution does not contain an explicit right to privacy.[69] However, the development of American jurisprudence has revealed that the right to privacy is implicitly protected under several Amendments to the United States Constitution.[70]

---

[63] *Id.* at 348–51; Bhatia, *supra* note 52, at 130.

[64] *Kharak Singh*, 1 SCR at 348–51.

[65] *Id.* at 343–44.

[66] *Id.* at 348–51; Bhatia, *supra* note 52, at 130.

[67] *Kharak Singh*, 1 SCR at 348–51; *see MP Sharma and Kharak Singh's Case: 'Privacy Not a Fundamental Right' Supreme Court Had Held Decades Ago*, FIRST POST (Aug. 24, 2017), http://www.firstpost.com/india/mp-sharma-and-kharak-singhs-case-privacy-not-a-fundamental-right-supreme-court-had-held-decades-ago-3966467.html.

[68] *Puttaswamy I*, Writ Petition (Civil) No. 494 of 2012 1, 261 (Sup. Ct. India Aug. 24, 2017).

[69] *Id.* at 141; Uppaluri & Shivanagowda, *supra* note 19, at 33.

[70] *See generally* Todd B. Ruback & Sarah Mahony, *An Overview of Recent Statutory Changes to Privacy Law in India in Comparison to Similar US and EU Privacy Rules*, N.J. LAW. MAG., Oct. 2011, at 48, 48; Uppaluri & Shivanagowda, *supra* note 19, at 34.

The 1965 case *Griswold v. Connecticut* was one of the earliest privacy cases before the United States Supreme Court.[71] Griswold brought a constitutional challenge of a state law that forbade the use of contraceptives.[72] The Court found that even though the right to privacy is not expressly mentioned in the Constitution, it emanates from the Fourth Amendment's ban on unreasonable searches.[73] The Court also held that the right to privacy is protected under the First, Third, Fifth, and Ninth Amendments.[74] These Amendments create a zone in which privacy is protected from governmental intrusion.[75]

Griswold is similar to the 1975 Indian Supreme Court case of *Govind v. State of M.P.*,[76] which also recognized a "penumbra or zone of privacy" under the Indian Constitution.[77] *Govind* challenged the constitutional validity of state surveillance and unannounced home visits.[78] The Court held that Articles 19 and 21 of the Indian Constitution created an independent right to privacy and the "fundamental nature of [this] right is implicit in the concept of ordered liberty."[79] Yet, the Indian Supreme Court did not go so far as to specifically declare privacy an inherent right, as was pronounced in *Puttaswamy I* and as the United States Supreme Court pronounced in *Griswold*, but did indicate that a fundamental privacy right could be overridden by a compelling state interest.[80]

The 1967 decision in *Katz v. United States* also broadened the interpretation of the right to privacy in the United States Constitu-

---

71 381 U.S. 479, 480 (1965); Uppaluri & Shivanagowda, *supra* note 19, at 34.
72 *Griswold*, 381 U.S. at 480.
73 *Id.* at 484.
74 *Id*.
75 *Id.* at 485.
76 (1975) 3 SCR 946 (India).
77 *Id.* at 947; Asrani-Dann, *supra* note 54, at 63.
78 Asrani-Dann, *supra* note 54, at 63.
79 *Govind*, 3 SCR at 954.
80 *See* Bhatia, *supra* note 52, at 134. *Govind* set the tone for future Indian Supreme Court decisions. *See, e.g.*, People's Union for Civil Liberties v. Union of India, (1997) 1 SCC 301 (holding that improper wiretapping implicates Article 21 of the Indian Constitution, violating personal liberty and the right to privacy).

tion, with specific emphasis on the Fourth Amendment and governmental intrusion.[81] Previous case law in the area of government surveillance was based on *Olmstead v. United States*, which interpreted the Fourth Amendment to apply only to an actual physical examination of one's person, papers, tangible effects, or home.[82] However, as the common law notion of privacy shifted from a physical- and property-based understanding to a personal liberty understanding, there was a reexamination and reinterpretation of the Constitution, specifically Fourth Amendment protections.[83] *Katz* established the "reasonable expectation of privacy," illuminated in Justice Harlan's concurrence, which built off Justice Stewart's majority opinion:

> "[T]he Fourth Amendment protects people, not places." The question, however, is what protection it affords to those people. Generally, as here, the answer to that question requires reference to a "place." My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person has exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as "reasonable."[84]

Following the *Katz* decision, the United States Supreme Court heard a number of cases to determine the extent that state actors may intrude upon an individual's privacy under the Fourth Amendment. In *Kyllo v. United States*, the Court held that the thermal imaging of a house is a violation of the Amendment.[85] Writing for the majority, Justice Scalia stated that the sanctity of the home is always protected, as was originally intended by the Fourth Amendment.[86] While the decision in *Katz* may have expanded the understanding of

---

[81] 389 U.S. 347, 347 (1967); U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated . . . .").

[82] 277 U.S. 438, 466 (1928).

[83] Asrani-Dann, *supra* note 54, at 54–55.

[84] *Katz*, 389 U.S. at 516 (Harlan, J., concurring).

[85] 533 U.S. 27, 40 (2001).

[86] *Id.*

the Fourth Amendment to include a reasonable expectation of privacy, the majority believed it did not supplant the original intention of the Amendment—to secure people in their "persons, houses, papers, and effects, against unreasonable searches and seizures."[87]

In addressing the concerns with government surveillance and monitoring, the United States Supreme Court, in *United States v. Jones*, held that GPS monitoring of a vehicle constituted a search under the Fourth Amendment.[88] GPS monitoring allows the government to create a comprehensive record of a person's public movements that reflect a great amount of detail about "her familial, political, professional, religious, and sexual association."[89] In her concurrence, Justice Sotomayor emphasized that "physical intrusion is now unnecessary to many forms of surveillance" and allowing the government to track a vehicle's movements through GPS may "alter the relationship between citizen and government in a way that is inimical to democratic society."[90]

Perhaps most telling of the United States Supreme Court's view on surveillance and data gathering in an era of increased technology is the 2014 case of *Riley v. California*.[91] There, the Supreme Court unanimously held that a warrantless search and seizure of digital contents of a cell phone was unconstitutional.[92] Cell phones contain much more information than just a record of outgoing and incoming calls; they contain photographs, video tapes, address books, emails, bank records, browsing histories, and voicemails.[93] As a result, the Court believed that allowing state actors to conduct a search of a person's entire cell phone would be like "ransacking his house for everything which may incriminate him" instead of just searching his pockets.[94]

In addition to the Fourth Amendment line of cases defining privacy, the Court developed the right to privacy in other areas as well;

---

87 U.S. CONST. amend. IV; *see Kyllo*, 533 U.S. at 40.

88 565 U.S. 400, 412–13 (2012).

89 *Id.* at 415 (Sotomayor, J., concurring).

90 *Id.* at 416.

91 134 S. Ct. 2473 (2014).

92 *Id.* at 2494–95.

93 *Id.* at 2489.

94 *Id.* at 2491 (quoting United States v. Kirschenblatt, 16 F.2d 202, 203 (2d Cir. 1926)).

perhaps most controversial is its decision in *Roe v. Wade*.[95] This case dealt with the question of abortion and a woman's liberty under the Fourteenth and Ninth Amendments.[96] The Fourteenth Amendment prevents the state from depriving any person of life, liberty, or property without due process of law, while the Ninth Amendment protects the unenumerated rights of the United States Constitution (rights that may exist aside from those explicitly mentioned).[97] In *Roe*, Justice Blackmun delivered the majority opinion and held that

> [t]he Constitution does not explicitly mention any right of privacy. In a line of decisions, however, . . . the Court has recognized that a right of personal privacy, or a guarantee of certain areas or zones of privacy, does exist under the Constitution. . . . This right of privacy, whether it be founded in the Fourteenth Amendment's concept of personal liberty and restrictions upon state action, as we feel it is, or, as the District Court determined, in the Ninth Amendment's reservation of rights to the people, is broad enough to encompass a woman's decision whether or not to terminate her pregnancy.[98]

In *Roe*, the Court found roots in the Constitution that protect the right to privacy: the First Amendment, the Bill of Rights, the Ninth Amendment, and the concept of liberty guaranteed by the Fourteenth Amendment.[99] This analysis is analogous to the decision in *Puttaswamy I*,[100] where Article 21 of the Indian Constitution was interpreted to include the right to privacy under the right of life and personal liberty. Although the word "privacy" is not mentioned in either the Indian or the United States Constitutions, the courts of both countries have not only recognized the right to privacy under

---

95 410 U.S. 113, 120 (1973).

96 *Id.* at 129.

97 U.S. CONST. amends. IX, XIV.

98 *Roe*, 410 U.S. at 152 (citations omitted).

99 *Id.* at 152–53; *accord* Griswold v. Connecticut, 381 U.S. 479, 484 (1965).

100 *See generally Puttaswamy I*, Writ Petition (Civil) No. 494 of 2012 1, 257 (Sup. Ct. India Aug. 24, 2017).

various amendments and articles, but they have also extended the scope of protection under the right to privacy.[101]

As demonstrated, constitutions and judicial interpretation evolve over time as specific issues and entitlements come to the forefront of the demands for justice.[102] Constitutional developments have occurred as constitutional texts are interpreted to address new concerns that require an "expansive reading of liberties and freedoms to preserve human rights under the rule of law."[103]

India's and the United States's experiences with oppressive regimes[104] is a reminder of how precious the rights to life and liberty truly are. It is the role of the judiciary to be vigilant in interpreting the meaning of constitutional text, as constitutions have evolved and continue to evolve to meet current and future challenges.[105] The draftsmen of both the Indian and United States Constitutions were influenced by a sense of history that enriched the development and adoption of the documents.[106] Further, as seen in previously mentioned case law, the concept of fundamental rights, such as the issue of privacy intertwined with liberty and dignity, has evolved over the course of constitutional history in both countries.[107]

Still, no past generation could possibly foresee the many problems that contemporary societies face, even with a rich sense of historical understanding of the meaning of life and liberty.[108] Therefore, constitutions should be interpreted with flexibility instead of limiting their meanings to the confines of their drafting date.[109] As Chief Justice Khehar eloquently put it, "above all, constitutional interpretation is but a process in achieving justice, liberty, and dignity

---

101 *See Roe*, 410 U.S. at 152; Uppaluri & Shivanagowda, *supra* note 19, at 33.

102 *Puttaswamy I*, Writ Petition (Civil) No. 494 of 2012 at 208.

103 *Id.*

104 *See* Dr. Chandrika Kaul, *From Empire to Independence: The British Raj in India 1858-1947*, BBC, http://www.bbc.co.uk/history/british/modern/independence1947_01.shtml (last updated Mar., 3, 2011); *see also* Francis D. Cogliano, *Was the American Revolution Inevitable?*, BBC, http://www.bbc.co.uk/history/british/empire_seapower/american_revolution_01.shtml (last updated Feb. 17, 2011).

105 *See Puttaswamy I*, Writ Petition (Civil) No. 494 of 2012 at 208.

106 *Id.* at 111–12.

107 *See* Roe v. Wade, 410 U.S. 113, 152–53 (1973); *see also* Katz v. United States, 389 U.S. 347, 348 (1967); Bhatia, *supra* note 52, at 130.

108 *See Puttaswamy I*, Writ Petition (Civil) No. 494 of 2012 at 208–09.

109 *See id.*

to every citizen."[110] Therefore, as society evolves, so must constitutional doctrine.

This is particularly relevant where judicial interpretation is influenced by a technological age that has the ability to reshape our primary understanding of "information, knowledge, and human relationships that was unknown even in the recent past."[111] As new challenges to privacy arise, courts must leave room for interpretation; today's problems "have to be adjudged by a vibrant application of constitutional doctrine and cannot be frozen by a vision suited to a radically different society."[112] Technological growth is so rapid that it renders advances of a few years ago obsolete.[113] The only way to maintain a relevant and applicable constitution is to view it as a living instrument capable of reinterpretation and reevaluation by applying the principles on which it was founded in light of societal change.

III. INDIA'S AADHAAR SYSTEM: A SPECIFIC PRIVACY ISSUE

A. *The Aadhaar System*

The need for additional legal analysis of privacy rights is evident with the growth and development of technology, which has created new mechanisms for the possible invasion of privacy by the state, such as "surveillance, profiling, and data collection."[114] Countries are increasing their use of technology in light of "global terrorist attacks and heightened public safety concerns."[115] Digital footprints and wide-ranging data can be analyzed to reveal "patterns, trends, and associations, especially relating to human behavior and interactions."[116] Along with these advancements in technology come new concerns of how such sensitive information is going to be dissemi-

---

110 *Id.* at 112.
111 *Id.* at 209.
112 *Id.* at 213.
113 *Id.*
114 *See Puttaswamy I*, Writ Petition (Civil) No. 494 of 2012 at 7 (Kaul, J., concurring).
115 *Id.*
116 *Id.* at 10.

nated and processed by the government, especially as engineers develop more effective algorithms and greater computational power.[117]

At the forefront of the data collection debate is the Aadhaar card. Initiated in 2009, Aadhaar is a twelve-digit number issued by the Unique Identification Authority of India ("UIDAI") to Indian residents.[118] Any individual, regardless of age or social status, may register for an Aadhaar number free of charge.[119] The applicant must provide demographic information (name, date of birth, age, gender, address, mobile number, and email) and biometric information (fingerprints, iris scan, and facial photograph).[120]

Aadhaar is a "strategic policy tool for social and financial inclusion, public sector delivery reforms, managing fiscal budgets, [increasing] convenience and [promoting] hassle-free people-centric governance [that] facilitates financial inclusion of the underprivileged and weaker sections of the society."[121] One of Aadhaar's goals is to create a national identity system that can work across state, language, and database barriers, giving an identity to the most marginalized and vulnerable of populations.[122] Millions of impoverished Indian citizens lack governmentally recognized identities, preventing them from gaining access to cell phones, lines of credit, bank accounts, or government aid.[123] With an Aadhaar ID, those lacking identification are now able to directly apply for housing subsidies, healthcare, and food through bank account deposits.[124] Aadhaar can be used in the delivery of food, employment, education,[125] social

---

117 *Id.*

118 *About Aadhaar*, UIDAI, https://uidai.gov.in/your-aadhaar/about-aadhaar.html (last visited Jan. 10, 2018). *Aadhaar* means "foundation" in Hindi. Caroline E. McKenna, *India's Challenge: Preserving Privacy Rights While Implementing an Effective National Identification System*, 38 BROOK. J. INT'L L. 729, 731 (2013).

119 *About Aadhaar*, *supra* note 118.

120 *Id.*

121 *Id.*

122 Nishant Shah, *Identity and Identification: The Individual in the Time of Networked Governance*, 11 SOCIO-LEGAL REV. 22, 29 (2015).

123 McKenna, *supra* note 118, at 730.

124 *Id.* at 731.

125 *State Govt to Transfer Scholarship Funds to Students' Accounts*, TRIBUNE, http://www.tribuneindia.com/news/punjab/state-govt-to-transfer-scholarship-funds-to-students-accounts/68619.html (last updated Apr. 17, 2015).

security, bank accounts,[126] or healthcare, by allowing the agency or service provider to contact the central Unique Identification database to confirm a beneficiary's identity.[127] To date, 1.09 billion people across India have obtained an Aadhaar identity.[128]

B. *Pros of the Aadhaar System*

One of Indian Prime Minister Narendra Modi's policy goals is to extend Aadhaar to every Indian citizen as a method to prove his or her identity and access governmental and financial services.[129] The Aadhaar system will benefit the poorest members of Indian society by providing direct access to government services such as food grains, cash subsidies, employment wages, education, health benefits, or LPG (cooking fuel) distribution.[130] Direct distribution will eliminate the problem of corrupt middlemen who enter false names into welfare databases to collect money intended for the poor.[131] The poor, who often lack identifying paperwork, such as proof of address or birth certificates, will now be able to apply for telecom services and passports, facilitating movement and communication throughout the country.[132] As a result, people living at the bottom of the socio-economic pyramid can participate in the marketplace and enjoy the benefits of having a government identity.[133]

---

[126] Vikas Dhoot, *UIDAI Tightens Norms for Aadhaar-Bank Account Linking*, HINDU, http://www.thehindu.com/news/national/uidai-tightens-norms-for-aadhaar-bank-account-linking/article21938183.ece (last updated Dec. 20, 2017).

[127] *FAQs, Use of Aadhaar*, UIDAI, https://uidai.gov.in/your-aadhaar/help/faqs.html (last visited Jan. 10, 2018).

[128] Saurabh Kumar, *Why Aadhaar is India's Unique Innovation for a Digital Economy*, YOUR STORY (Jan. 11, 2017), https://yourstory.com/2017/01/AADHAAR-DIGITAL-ECONOMY/.

[129] Vidhi Doshi, *A Security Breach in India Has Left a Billion People at Risk of Identity Theft*, WASH. POST (Jan. 4, 2018), https://www.washingtonpost.com/news/worldviews/wp/2018/01/04/a-security-breach-in-india-has-left-a-billion-people-at-risk-of-identity-theft/?utm_term=.147fb681aeb1.

[130] Vanita Yadav, *Unique Identification Project for 1.2 Billion People in India: Can It Fill Institutional Voids and Enable 'Inclusive' Innovation?*, 6 CONTEMP. READINGS L. & SOC. JUST. 38, 45 (2014); *Supreme Court Allows Linking Aadhaar with PDS and LPS Subsidies*, TIMES INDIA (Aug. 12, 2015), https://timesofindia.indiatimes.com/india/Supreme-Court-allows-linking-Aadhaar-with-PDS-and-LPG-subsidies/articleshow/48444953.cms.

[131] Yadav, *supra* note 130, at 45; Doshi, *supra* note 129.

[132] Yadav, *supra* note 130, at 45.

[133] *Id.* at 44.

Additionally, Aadhaar cards will facilitate banking and entrepreneurial endeavors.[134] UIDAI will be able to secure money transactions through MicroATMs and mobile phones in rural areas of India.[135] Banks will be able to link their permanent account numbers with Aadhaar numbers, making it easier for people to open bank accounts without extensive identity documentation.[136] Linking one's bank account with Aadhaar can help to ensure direct and transparent transfers of subsidies, weed out false beneficiaries, and reduce tax evasion.[137]

Aadhaar can provide a secure and reliable authentication service for companies and entrepreneurs to facilitate market transactions.[138] For example, Aadhaar users are able to pay for goods with their fingerprint or ID numbers.[139] The Indian Central Bank has introduced outposts in rural grocery stores and other small business operations.[140] Merchants at these outposts are equipped with smartphones and small fingerprint scanners that link their bank accounts to their Aadhaar numbers.[141] Customers enter their Aadhaar number and bank name into the smart phone and then scan one of their fingers.[142] After authentication, the amount owed is directly credited to the

---

134 *Id.* at 46.

135 *Id.* at 45.

136 *Id.* However, the *mandatory* linking of Aadhaar numbers with bank accounts was declared unconstitutional in a September 26, 2018 judgment by the Indian Supreme Court. Vidhi Doshi, *India's Top Court Upholds World's Largest Biometric ID Program, Within Limits*, WASH. POST (Sept. 26, 2018), https://www.washingtonpost.com/world/asia_pacific/indias-top-court-upholds-worlds-largest-biometric-id-program-within-limits/2018/09/26/fe5a95b0-c0ba-11e8-92f2-ac26fda68341_story.html?noredirect=on&utm_term=.f79aa79dd0f6 [hereinafter *India's Top Court*].

137 Konark Sikka, *Making Aadhaar Mandatory: Benefits and Drawbacks*, DAILY O (Mar. 25, 2017), https://www.dailyo.in/politics/aadhar-card-uidai-bjp-finance-bill-2017/story/1/16363.html*; Aadhaar-PAN Link Will Prevent Tax Evasion, Says FM Arun Jaitley*, BUS. TODAY, https://www.businesstoday.in/current/economy-politics/aadhaar-pan-link-tax-evasion-says-fm-arun-jaitley/story/257077.html (last updated July 25, 2017).

138 Yadav, *supra* note 130, at 44.

139 *Id.* at 45; Kumar, *supra* note 128.

140 McKenna, *supra* note 118, at 732.

141 Kumar, *supra* note 128.

142 *Id.*

merchant's bank account.[143] This form of payment will not only facilitate commerce in rural areas, but will also assist farm workers and merchants in entering the formal banking system, helping them develop their credit history and allowing them to apply for loans.[144]

C. *Cons of the Aadhaar System*

This large-scale, centralized collection, storage, and use of an individual's demographic and biometric information has serious privacy implications, especially considering that India lacks any type of comprehensive privacy law or independent oversight agency.[145] Many fear that having one universal ID number will allow government or private actors to discover sensitive demographic and biometric information.[146] In fact, there have already been incidents of hacking the UIDAI system and stealing Aadhaar information.[147]Anonymous sellers having been using the WhatsApp mobile application to provide unrestricted access to information from more than one billion Aadhaar numbers.[148] For a fee of 500 Rupees (around eight U.S. dollars), anyone can gain access to an individual's name, address, date of birth, photo, personal identification number, phone number, and email address.[149] Once Aadhaar information is obtained, hackers use the numbers to print duplicate Aadhaar cards to link SIM cards and bank accounts of unsuspecting

---

143 *Id.*

144 *Id.*; *contra* Rohan Venkataramakrishnan, *How Long Can the Indian Government Continue Claiming Aadhaar Is Secure and Foolproof?*, SCROLL (Jan. 4, 2018), https://scroll.in/article/863779/how-long-can-the-indian-government-continue-claiming-aadhaar-is-secure-and-foolproof (emphasizing the downsides of biometric identification in relation to bank and identity fraud).

145 Asrani-Dann, *supra* note 54, at 61.

146 McKenna, *supra* note 118, at 732; *see Aadhaar Data Theft Hasn't Compromised UIDAI Server: Cops*, TIMES INDIA (Aug. 8, 2017), https://timesofindia.indiatimes.com/city/bengaluru/aadhaar-data-theft-hasnt-compromised-uidai-server-cops/articleshow/59963733.cms; *see also* Rachna Khaira, *Rs 500, 10 Minutes, and You Have Access to Billion Aadhaar Details*, TRIBUNE, http://www.tribuneindia.com/news/nation/rs-500-10-minutes-and-you-have-access-to-billion-aadhaar-details/523361.html (last updated Jan. 5, 2018).

147 *Aadhaar Data Theft Hasn't Compromised UIDAI Server: Cops*, *supra* note 146.

148 Khaira, *supra* note 146.

149 *Id.*

users, most likely leading to identity theft.[150] Ironically, Aadhaar was developed by the government as a method to combat corruption and prevent false identification and fraud.[151]

Despite the recent hacking incidents,[152] UIDAI continues to claim that biometric information is encrypted at the source and "unauthorized sharing and leakage of the data does not happen."[153] UIDAI denied the media reports of any information hacking, stating the news articles were a "case of misreporting" and claiming that "Aadhaar data, including biometric information, is fully safe and secure."[154] UIDAI claims that having access to someone's Aadhaar number does not pose a threat because an individual's iris or fingerprints are also necessary for successful identification;[155] a mere display of demographic information cannot be misused without biometrics.[156] However, this has been shown to be untrue, as identity fraud is still occurring without the need for biometric authentication.[157] Conmen can print duplicate ID cards to use at airports or withdraw funds by linking bank accounts with Aadhaar numbers or phone numbers.[158] Despite UIDAI's denial of data hacking, the recent media reports regarding Aadhaar bring to light the issue of data security as an aspect of privacy rights and may hinder UIDAI's goal of extending Aadhaar to every Indian citizen.[159]

---

[150] Sanket Visjayasarathy, *Your Aadhaar Number on Sale for Rs 500, All Aadhaar-linked Details of 1 Billion Indians Leaked*, INDIA TODAY (Jan. 4, 2018), http://indiatoday.intoday.in/technology/story/aadhaar-number-on-sale-for-rs-500-linked-details-of-1-billion-indians-leaked/1/1123233.html.

[151] Doshi, *supra* note 129.

[152] Khaira, *supra* note 146.

[153] Richa Mishra, *The 12-Digit Conundrum*, HINDU BUS. LINE (Mar. 13, 2017), http://www.thehindubusinessline.com/specials/india-file/aadhaar-the-12digit-conundrum/article9582271.ece.

[154] Samden Sherpa, *Aadhaar Data Fully Safe, Cannot Be Breached or Leaked: UIDAI Responds*, GIZBOT (Jan. 5, 2018), https://www.gizbot.com/news/aadhaar-data-fully-safe-cannot-be-breached-or-leaked-uidai-responds-046950.html.

[155] *Aadhaar Data Allegedly 'Breached' for Rs 500: All Your Questions Answered*, INDIAN EXPRESS (Jan. 4, 2018), http://indianexpress.com/article/technology/tech-news-technology/aadhaar-data-allegedly-breached-for-rs-500-heres-everything-to-know-5011205/.

[156] Khaira, *supra* note 146.

[157] Venkataramakrishnan, *supra* note 144.

[158] *Id.*

[159] McKenna, *supra* note 118, at 731; Doshi, *supra* note 129.

UIDAI claims to protect users and their information[160] by providing a secure and encrypted database, providing strict security and storage protocols, penalizing anyone who tampers with data or gains unauthorized access, and collecting limited data (no information concerning religion, caste, community, class, ethnicity, income, or health is collected).[161] However, there is little legal framework in India to protect Aadhaar users from data breaches.[162] Because there are no comprehensive privacy laws in India, the activities of the state are regulated through "sector-specific laws and the jurisprudential development of the right to privacy."[163]

The only effective legislation governing security and cybercrime in India is the Information Technology (Amendment) Act, 2008.[164] The sole provision addressing the privacy of personal information is section 72A, which "prescribes a penalty for breach of privacy of an electronic record, but only applies to authorities exercising power under the Act," not to private individuals who may gain access to information illegally.[165] Section 43 of the Information Technology Act requires that corporations maintain "reasonable security practices and procedures," defined as procedures intended to protect information from "unauthorized access, damage, use, modification, disclosure or impairment."[166] However, the Information Technology Act gives corporations the freedom to determine which procedures they will implement in protecting confidential information, which may lead to the use of minimum data protection

---

160 Sherpa, *supra* note 154.

161 *FAQs, Security in UIDAI System*, UIDAI, https://uidai.gov.in/your-aadhaar/help/faqs.html (last visited Jan. 10, 2018).

162 Vrinda Bhandari & Renuka Sane, *Towards a Privacy Framework for India in the Age of the Internet* 13 (Nat'l Inst. of Pub. Fin. and Policy, Working Paper No. 179, 2016).

163 *Id.*

164 *See* Information Technology (Amendment) Act, 2008, No. 10, Acts of Parliament, 2009 (India); Greenleaf, *supra* note 21, at 24–26; Margaret Rouse, *Information Technology Amendment Act 2008 (IT Act 2008)*, WHAT IS, http://whatis.techtarget.com/definition/Information-Technology-Amendment-Act-2008-IT-Act-2008 (last updated Jan. 2010).

165 Information Technology (Amendment) Act § 72A; Asrani-Dann, *supra* note 54, at 65.

166 Information Technology (Amendment) Act § 43A.

standards and lack of third-party oversight.[167] As discussed, there are many cons to the Aadhaar system not just in its existence, but also in its application to the right to privacy.

IV. CONSTITUTIONALITY OF THE AADHAAR SYSTEM

As there is no comprehensive legal framework for privacy protection and no explicit constitutional right to privacy in India,[168] one must ask: is the Indian government violating individual privacy rights through Aadhaar? Following the Supreme Court of India's declaration that privacy is a fundamental right,[169] the idea of a general-purpose identification database is constitutionally questionable.[170] Determining privacy as a constitutionally protected right has laid the foundation for more specific challenges to

> various architectural and implementational aspects of Aadhaar, and its impact on privacy—such as the mandatory collection of biometric data, deployment of private players for collection of information, online authentication and the extent of authentication data storage, and the possibility of data convergence and profiling as a result of Aadhaar-seeding of various databases.[171]

A. *The Aadhaar Act 2016*

The Aadhaar Act 2016 ("the Act" or "the Aadhaar Act"), a money bill passed by the Parliament of India, aims to provide legal

---

[167] Vikas Asawat, Information Technology (Amendment) Act, 2008: A New Vision Through a New Change 4 (2010) (unpublished article), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1680152.

[168] *See supra* notes 161–66 and accompanying text; Bhatia, *supra* note 52, at 128.

[169] *Puttaswamy I*, Writ Petition (Civil) No. 494 of 2012 1, 262–63 (Sup. Ct. India Aug. 24, 2017).

[170] Prasanna S, *Right to Privacy: What the Judgment Means for Aadhaar, Its Constitutionality*, INDIAN EXPRESS, http://indianexpress.com/article/explained/fundamental-right-to-privacy-what-the-judgment-means-for-aadhaar-its-constitutionality-4812231/ (last updated Aug. 25, 2017).

[171] *Id.*

backing to the Aadhaar project.[172] The Act describes the Aadhaar enrollment process, authentication procedures, the organizational structure of UIDAI, methods for the protection of information, and offenses and penalties.[173] The Act places UIDAI in charge of securing identity information, authenticating records, and implementing "appropriate technical and organisational security measures."[174] There are restrictions in place that regulate the sharing of information with third parties, with an exception for the disclosure of information "made in the interest of national security."[175]

However, the Act was met with controversy, as section 7 specifies that the government may "require" an individual to enroll in Aadhaar to obtain government subsidies or services.[176] For example, a 2016 finance bill has made Aadhaar mandatory for filing tax returns and obtaining a permanent bank account number.[177] The Indian Supreme Court has directed that Aadhaar cannot be compulsory for beneficiaries or as a precondition to access welfare programs.[178] Initially, the Aadhaar project was presented to the public as a voluntary program;[179] however, Aadhaar has now become man-

---

[172] 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].

[173] *Id.*

[174] *Id.* § 28(4)(a).

[175] *Id.* § 33(2).

[176] *Id.* § 7; *see* V Nalinakanthi, *All You Wanted to Know About Aadhaar Bill*, HINDU BUS. LINE (Mar. 21, 2016), http://www.thehindubusinessline.com/opinion/columns/all-you-wanted-to-know-about-aadhaar-bill/article8381808.ece; *Supreme Court Counters Push for Aadhaar*, HINDU, http://www.thehindu.com/news/national/aadhaar-cannot-be-mandatory-for-welfare-schemes-supreme-court/article17671381.ece (last updated April 7, 2017).

[177] *Supreme Court Counters Push for Aadhaar*, *supra* note 176; Preeti Motiani, *Don't File ITR? You Still Need to Link PAN, Aadhaar Else PAN May Become Invalid*, ECON. TIMES, https://economictimes.indiatimes.com/wealth/personal-finance-news/dont-file-itr-you-must-link-pan-aadhaar-else-pan-may-become-invalid/articleshow/59157881.cms (last updated June 18, 2017).

[178] *Supreme Court Counters Push for Aadhaar*, *supra* note 176.

[179] Jean Dreze, *The Aadhaar Coup*, HINDU (March 15, 2016), http://www.thehindu.com/opinion/lead/jean-dreze-on-aadhaar-mass-surveillance-data-collection/article8352912.ece.

datory for an ever-widening range of services such as salary payments, pensions, school enrollment and scholarships, filing income tax returns, and other welfare schemes.[180]

Nevertheless, the Indian Supreme Court has pushed against making Aadhaar mandatory for certain services.[181] Specifically, there are currently a handful of petitions challenging the government's decision to make Aadhaar cards mandatory for government services and welfare schemes, claiming the mandatory linking of Aadhaar numbers to bank accounts and cell phones is illegal and unconstitutional.[182] On September 26, 2018, the Indian Supreme Court ruled on some of these petitions, declaring the mandatory linking of Aadhaar numbers with all government welfare schemes and services to be constitutional, while linking Aadhaar numbers with private services such as bank accounts, employee pension plans, or cell phone SIM cards *cannot* be a requirement.[183] Similar to a 2015 interim order where the Indian Supreme Court struck down the mandatory requirement of Aadhaar for private services,[184] the 2018 judgment will restrict Aadhaar's mandatory usage to government services only.[185]

---

[180] *Id.*

[181] *Supreme Court Counters Push for Aadhaar*, *supra* note 176.

[182] Dhananjay Mahapatra, *Supreme Court Reserves Verdict on Aadhaar Validity*, TIMES INDIA (May 11, 2018), https://timesofindia.indiatimes.com/india/supreme-court-reserves-verdict-on-aadhaar-validity/articleshow/64116972.cms; Samanwaya Rautray, *Aadhaar Lacks Regulatory Oversight: Supreme Court*, ECON. TIMES (May 11, 2018), https://economictimes.indiatimes.com/news/politics-and-nation/aadhaar-lacks-regulatory-oversight-supreme-court/articleshow/64117381.cms.

[183] Justice K.S. Puttaswamy (Retd.) v. Union of India (*Puttaswamy II*), Writ Petition (Civil) No. 494 of 2012 1, 90–92 (Sup. Ct. India Sept. 26, 2018); Manveena Suri, *Aadhaar: India Supreme Court Upholds Controversial Biometric Database*, CNN (Sept. 26, 2018), https://www.cnn.com/2018/09/26/asia/india-aadhaar-ruling-intl/index.html.

[184] Krishnadas Rajagopal, *Right to Privacy Verdict; A Timeline of SC Hearings*, HINDU BUS. LINE (Aug. 24, 2017), http://www.thehindubusinessline.com/news/national/right-to-privacy-verdict-a-timeline-of-sc-hearings/article9829124.ece ("[T]he purely voluntary nature of the use of Aashaar card to access public service will continue [until] the court takes a final decision on whether Aadhaar scheme is an invasion into the right to privacy.").

[185] *India's Top Court*, *supra* note 136. *See generally Puttaswamy II*, Writ Petition (Civil) No. 494 of 2012.

B. *Information Collection and the Legality of the Aadhaar Act*

A primary concern is that the requirement of Aadhaar will result in mass surveillance by the government, possibly leading to breaches of confidentiality and privacy.[186] An identity scheme that employs mass surveillance impairs an individual's autonomy and self-development and violates the constitutional protection of privacy and human dignity.[187] There is no telling how the Indian government will handle such information or the political and personal consequences of government misuse of such large quantities of personal data.[188]

As Justice Chandrachud explained in *Puttaswamy I*, "informational control empowers the individual to use privacy as a shield to retain personal control over information pertaining to the person."[189] As per his opinion, information can be collected subject to three requirements: (1) legality—there should be the existence of law; (2) need—the aim of the law for which information is being collected is reasonable; and (3) proportionality—"the means which are adopted by the legislature are proportional to the object and needs sought to be fulfilled by the law."[190]

It is essential to analyze these requirements in relation to the Aadhaar Act. As previously discussed, section 7 of the Act states that in order to establish identity as a "condition for receipt of a subsidy, benefit or service," the central or state government may "*require* that such an individual undergo authentication, or furnish proof of possession of an Aadhaar number."[191] This provision opens the door for the government to require Aadhaar registration for beneficiaries, which the Supreme Court has already pushed against.[192]

Additionally, the Act was passed in Parliament as a money bill (a draft law that contains provisions concerning the regulation of a tax, lending money to the Government of India, or withdrawal of

---

[186] Dreze, *supra* note 179.

[187] INDIA CONST. pmbl. (recognizing human dignity in the Constitution); Asrani-Dann, *supra* note 54, at 87.

[188] Asrani-Dann, *supra* note 54, at 87–88.

[189] *Puttaswamy I*, Writ Petition (Civil) No. 494 of 2012 1, 201 (Sup. Ct. India Aug. 24, 2017).

[190] *Id.* at 264.

[191] The Aadhaar Act, 2016, No. 18, Acts of Parliament, 2016, § 7 (India) (emphasis added).

[192] *See* Rajagopal, *supra* note 184.

money from the Consolidated Fund of India), which has been challenged as unconstitutional because the Act contains provisions unrelated to government taxation and expenditure.[193] This leads us to question Justice Chandrachud's first requirement—is the Act even legal?[194] According to the recent September 2018 Indian Supreme Court decision in *Puttaswamy II*, it is.[195] In the judgment, the Court declared that Aadhaar could legally be brought in as a money bill.[196]

Nevertheless, it is essential to consider the Act's need and proportionality, which are directly related to requirements two and three. While the aim of the Act is a reasonable one—to provide every Indian with a unique identity number that enables a fair and equitable distribution of benefits and subsidies—the use of biometric information is not a reasonable means of data collection. Along with being unreasonable, the means of data collection are not proportional to the object or needs of the law.

C. *Biometric Data Collection*

Biometric information is the collection of data that is intrinsic to each person, such as fingerprints, retina scans, voice analysis, DNA analysis, or facial recognition.[197] The appeal of biometric information is that it is hard to falsify; however, there are serious concerns on the efficacy of biometric analysis.[198] The technology is not foolproof—any biometric authentication process is prone to error.[199] For example, manual laborers may encounter problems with fingerprint scanning, as their hands may be worn or change over time.[200] In fact, fingerprint scanning has a false rejection rate of eleven percent (11%).[201]

---

[193] Suhrith Parthasarahy, *What Exactly Is a Money Bill?*, HINDU, http://www.thehindu.com/opinion/lead/what-exactly-is-a-money-bill/article17372184.ece (last updated Feb. 27, 2017).

[194] *Puttaswamy I*, Writ Petition (Civil) No. 494 of 2012 at 264.

[195] *Puttaswamy II*, Writ Petition (Civil) No. 494 of 2012 1, 487 (Sup. Ct. India Sept. 26, 2018).

[196] *Id*.

[197] Asrani-Dann, *supra* note 54, at 75–76.

[198] *Id.* at 81–82.

[199] *Id.*

[200] *Id.* at 81; McKenna, *supra* note 118, at 755.

[201] Asrani-Dann, *supra* note 54, at 82.

Because biometric schemes are expensive, there is a greater tendency towards data sharing among organizations, leading to a larger interconnected web of personal information.[202] Even though other countries have implemented successful ID card schemes, most do not use biometric identifiers or have multiple applications.[203] UIDAI can still reach its goal of creating a database of every Indian citizen with the use of demographic information. Other options include storing biometric information on an offline terminal, where the information is not stored in a single centralized online database, or using smartcards, where biometric information is kept directly on the card itself.[204] These alternatives present fewer security concerns and are more reasonable methods of data collection and storage.[205]

D. *Constitutional Challenge Analysis*

Contrary to the Indian Supreme Court's findings in *Puttaswamy I* and *II*, the Aadhaar system is unconstitutional and a violation of privacy rights. Informational privacy is a facet of the right to privacy.[206] While there exists a sensitive balance between individual interests and legitimate concerns of the state, the Indian government would have a difficult time establishing a compelling state interest that would outweigh the protection of privacy rights. A legitimate aim of the state would include, for instance, protecting national security, preventing and investigating crime, encouraging innovation and the spread of knowledge, and/or preventing the dissipation of social welfare benefits.[207] While these state interests are of importance, a constitutionally protected right should take precedence over such state aims.

---

[202] *Id.* at 77.

[203] *Id.* at 69 (countries such as Belgium, Greece, Luxembourg, Germany, France, Portugal, and Spain all have official, compulsory national ID cards).

[204] Kritika Bhardwaj, *The Mission Creep Behind the Aadhaar Project*, WIRE (Sept. 2, 2016), https://thewire.in/63223/the-mission-creep-behind-the-uidais-centralisation-ideology/.

[205] *Id.*

[206] *Puttaswamy I*, Writ Petition (Civil) No. 494 of 2012 1, 201 (Sup. Ct. India Aug. 24, 2017).

[207] *Id.* at 265.

While it has been argued that the Aadhaar Act violates the Indian Constitution under Article 14 (right to equal protection),[208] Article 19(1)(d) (right to move freely),[209] Article 19(1)(g) (right to practice any profession, occupation, trade or business),[210] and Article 21 (right to life and personal liberty),[211] the Indian Supreme Court has declared the Act constitutional. Article 141 of the Indian Constitution states the following: "The law declared by the Supreme Court shall be binding on all courts within the territory of India."[212] This ensures that the Supreme Court of India may pass a decree or order as is necessary for doing justice in any cause or matter before it, and any decree or order passed is enforceable throughout all of India.[213]

However, despite the fact that the Supreme Court's ruling is binding, Article 13(2) of the Indian Constitution may provide a legal mechanism to declare the Aadhaar Act unconstitutional. Article 13(2) declares that "the State shall not make any law which takes away or abridges the rights conferred by [Part III (Fundamental Rights)] and any law made in contravention of this clause shall, to the extent of the contravention, be void."[214] Therefore, a law that enables the collection of identity data without adequate safeguards violates the right to privacy under Article 21 (which is included in Part III of the Indian Constitution) and should be declared void under Article 13(2). Under this analysis, the Act should have been declared unconstitutional by the *Puttaswamy I* court.

---

[208] *The Aadhaar Debate: 'The State Has No Right of Eminent Domain on the Human Body*,*'* WIRE (Apr. 28, 2017), https://thewire.in/129622/aadhaar-income-tax-supreme-court/ (arguing that forcing taxpayers to enroll in Aadhaar violates the constitutional guarantees of equal protection under Article 14).

[209] *Puttaswamy I*, Writ Petition (Civil) No. 494 of 2012 at 19.

[210] Asheeta Regidi, *SC Stay on Aadhaar-PAN Linkage: There Is Still Hope for Privacy, Section 139AA Detractors*, FIRST POST (June 12, 2017), http://www.firstpost.com/india/sc-stay-on-aadhaar-pan-linkage-there-is-still-hope-for-privacy-section-139aa-detractors-3543917.html (discussing the argument that the mandatory linkage of Aadhaar to permanent account numbers violates the right to freedom of profession).

[211] *See generally Puttaswamy I*, Writ Petition (Civil) No. 494 of 2012 at 1–5.

[212] INDIA CONST. art. 141.

[213] *Id.* art. 142.

[214] *Id*. art. 13 § 2.

E. *New Legislative Proposals*

Even though the Aadhar Act has been declared constitutional, there should be safeguards to the system. The portions of the *Puttaswamy I* judgment that discuss data protection and privacy state that "any collection of personal information that would impact privacy must have a law to back it."[215] Accordingly, in order to ensure the success of Aadhaar, India must pass comprehensive privacy legislation that provides "judicial remedies and other enforcement mechanisms for preventing privacy violations."[216] Considering that the right to privacy has been declared a protected right under the Indian Constitution, this task should be made easier.[217]

New legislation should include the following: (1) methods for which individuals can object to the use of certain personal information; (2) explanations regarding exactly how personal information is going to be used; (3) third party oversight of UIDAI; (4) transparency of new developments, practices, and policies; and (5) prompt judicial review of situations where information was improperly used or obtained. [218]

Additionally, different agencies and service providers should be prevented from data sharing. The interloping of data between organizations would leave an electronic trail of an individual's activities and records and allow information collected for one purpose to be used for altogether different purposes.[219] For example, interlinking of databases could occur if, when applying for a job, an employer could access medical records, banking information, or voter registration of a potential employee. Personal data should be limited or kept relevant to its purpose and used to the extent necessary for that purpose. Finally, individuals should be able to request and obtain information concerning their personal data and have a means of challenging that data. If the challenge is successful, the data should be modified or erased.

---

[215] Prasanna S, *supra* note 170.

[216] McKenna, *supra* note 118, at 734.

[217] *See generally Puttaswamy I*, Writ Petition (Civil) No. 494 of 2012 1, 262 (Sup. Ct. India Aug. 24, 2017).

[218] *Contra* The Aadhaar Act, 2016, No. 18, Acts of Parliament, 2016, § 47(1) (India) (prohibiting a complaint from being admitted before a court unless it has been filed by the UIDAI authority).

[219] Asrani-Dann, *supra* note 54, at 77.

V. IMPLICATIONS OF AN AADHAAR-LIKE SYSTEM IN THE UNITED STATES

The United States has historically rejected attempts to create a national ID system.[220] While the United States does issue Social Security numbers and stores biometric information in the criminal database, there is no universal biometric database from which to pull information.[221] With the growth of interconnected technology, it is important to address the consequences of a system like Aadhaar in the United States if an equivalent system were to be implemented.

Because an Aadhaar ID is technically voluntary for privatized services, it is essential to consider how disclosing personal information to a third party affects one's privacy rights. Even though the Aadhaar Act provides certain safeguards,[222] there are risks associated with the voluntary disclosure of information. For example, in *United States v. Miller*, it was determined that there is no reasonable expectation of privacy in bank records disclosed to a third party when done in the ordinary course of business.[223] In that case, the government was able to gain access to the individual's bank records even though they were confidential.[224] Similarly, voluntarily disclosing information to an agency like UIDAI may waive any reasonable expectation of privacy.

While the United States government may assert that the voluntary disclosure of information is not protected by the Fourth Amendment, one can argue that, in practice, the use of a national ID card may not actually be voluntary. As seen with the Aadhaar cards, the government can require ID cards to be mandatory in order to access certain welfare services or file income tax returns. When considering the services that demand an Aadhaar card, such disclosure of information is not voluntary in any meaningful sense of the word, but a requirement. Therefore, unlike the holding in *Miller*, the U.S.

---

220 *Id.* at 69.

221 Anumeha Yadav, *Despite the Comparisons, India's Aadhaar Project Is Nothing Like America's Social Security Number*, SCROLL (Dec. 20, 2016), https://scroll.in/article/823570/despite-the-comparisons-indias-aadhaar-project-is-nothing-like-americas-social-security-number.

222 *See, e.g.*, The Aadhaar Act, 2016, No. 18, Acts of Parliament, 2016, § 29(1)(a) (India) ("No core biometric information collected or created under this Act shall be—shared with anyone for any reason whatsoever[.]").

223 425 U.S. 435, 441–42 (1976).

224 *Id.* at 438.

government would fail in arguing that voluntarily providing information to a third party in order to obtain an ID card should not be granted Fourth Amendment protections.

If a national ID system were to be implemented in the United States, the government would be able to gain access to an individual's confidential information (even the Aadhaar Act has a provision that allows disclosure of information in the "interest of national security").[225] Access to such information would implicate the Fourth Amendment, as there is a reasonable expectation of privacy when disclosing personal information.[226] As Justice Sotomayor stated in *United States v. Jones*, "I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection."[227] The government's use of personal information to monitor someone's actions, habits, and communication is a violation of the Fourth Amendment unless the Amendment's requirements were satisfied, as it creates a comprehensive picture of that person's life.[228]

The gathering of biometric information into large databases has been a growing concern in the United States.[229] It has been argued that biometric ID cards contain information so personal to one's body (iris scans, facial recognition, and fingerprints), that protection extends beyond one's body and to the cards, making a violation of a card's information a personal privacy violation.[230] In 2017, the Indian Supreme Court considered two writ petitions pending before it concerning the right to bodily autonomy, claiming the collection of biometric information under Aadhaar constitutes bodily intrusion

---

225 The Aadhaar Act, 2016, No. 18, Acts of Parliament, 2016, § 33(2) (India).

226 *Miller*, 425 U.S. at 448–50 (Brennan, J., dissenting).

227 565 U.S. 400, 418 (2012) (Sotomayor, J., concurring).

228 *Id.* at 415.

229 *See* Kartikay Mehrotra, *Tech Companies Are Pushing Back Against Biometric Privacy Laws*, BLOOMBERG BUSINESSWEEK (July 19, 2017), https://www.bloomberg.com/news/articles/2017-07-20/tech-companies-are-pushing-back-against-biometric-privacy-laws.

230 *Before Aadhaar-PAN Verdict, A Lively Debate over Bodily Autonomy and Living with Dignity*, WIRE (May 3, 2017), https://thewire.in/131698/before-aadhaar-pan-card-verdict-debate-over-bodily-autonomy-and-living-a-dignified-life/ [hereinafter *Before Aadhaar-PAN Verdict*].

under Article 21.[231] The petitions argued that unless there is a compelling state interest, such as identifying a murder suspect or border control, the use of biometric information should be narrowly tailored and not be permitted as a "24/7 tracking system."[232] Because of the potential misuse of biometric information, certain states in the United States have enacted privacy laws protecting the collection and use of biometric information by companies.[233] While the Federal Bureau of Investigation and Customs and Border Patrol have been permitted to collect and access biometric information, there has yet to be a nationwide collection system.[234]

Data sharing is also an issue, as data commoditization has created an entire industry around the buying and selling of personal information.[235] As stated in *Riley v. California* (which extended Fourth Amendment protection to cell phones), technology allows individuals to carry massive amounts of data that is stored in one central location, such as a cell phone.[236] Similarly, information that is gathered and stored in one centralized database and shared between agencies and service providers should also be afforded Fourth Amendment protections. A centralized database is similar to a cell phone—large amounts of information are stored in one location, giving the government free reign to use and explore that data. Not only is this information at risk in the state's hands, but private actors may be able to gain access to the database via hacking, such as the recent reports of unauthorized access of the UIDAI system.[237]

Normalization of the collection, use, and synchronization of data is dangerous. When citizens become accustomed to the government

---

[231] *Id.*; *see Puttaswamy II*, Writ Petition (Civil) No. 494 of 2012 1, 221–22 (Sup. Ct. India Sept. 26, 2018).

[232] *Before Aadhaar-PAN Verdict*, *supra* note 230.

[233] Mehrotra, *supra* note 229 (discussing Illinois' passage of the Biometric Information Privacy Act of 2008 to regulate the commercial use of finger, iris, and facial scans).

[234] *Id.*

[235] Bhandari & Sane, *supra* note 162, at 8.

[236] 134 S. Ct. 2473, 2493 (2014).

[237] *See* Khaira, *supra* note 146; *see also* Mayur Shetty, *Aadhaar Cyber Hit Will Cause Incalculable Loss*, TIMES INDIA (Jan. 10, 2018), https://timesofindia.indiatimes.com/india/aadhaar-cyber-hit-will-cause-incalculable-loss/articleshow/62436726.cms.

requiring the collection of sensitive personal data, they become desensitized to the experience.[238] It then becomes the norm for the state to monitor and collect information about one's life and preferences, leading to an Orwellian[239] way of life where state surveillance is omnipresent.[240] It is essential to a democratic form of government to allow citizens to speak their mind and dissent without fear of retribution from the state.[241] If the public fears the monitoring and storing of their views, they will engage in self-censorship and be less likely to express a "contrarian or controversial view point."[242]

Additionally, private actors may take advantage of such a system. For example, one wealthy neighborhood in India requires all labor and domestic workers to have an Aadhaar card.[243] The residents felt it was a cheaper and more reliable way of controlling surveillance of the neighborhood, rather than a police verification process.[244] However, allowing private actors to take on a police role could lead to discrimination, isolation, and profiling of minority groups.

The implementation of a national ID system in the United States would have grave consequences to personal privacy rights. The Aadhaar system should serve as a lesson to the United States about how a purportedly "pro-poor, pro-development," and "anti-corruption" mechanism can result in mass surveillance, mandatory enrollment, and dangerous hacking.[245] To maintain a liberal democratic society that values and upholds privacy rights, the United States

---

238 SURVEILLANCE, PRIVACY, AND SECURITY: CITIZENS' PERSPECTIVES 217 (Michael Friedewald et al. eds., 2017).

239 *See* Charlotte Ahlin, *The Meaning of 'Orwellian' Is More Complicated than You Think — and It's Extremely Relevant to Modern Politics*, BUSTLE (May 24, 2018), https://www.bustle.com/p/the-meaning-of-orwellian-is-more-complicated-than-you-think-its-extremely-relevant-to-modern-politics-9118383 (describing modern understandings of the term "Orwellian" as being associated with totalitarian governments, constant surveillance, and limits to personal freedom). *See generally* GEORGE ORWELL, 1984 (1949).

240 *See* Ahlin, *supra* note 239; *see also* ORWELL, *supra* note 239, at 4 (describing government surveillance of citizens via television).

241 *See* Bhandari & Sane, *supra* note 162, at 10.

242 *Id*.

243 Kalyani Menon Sen, *Aadhaar: Wrong Number, or Big Brother Calling?*, 11 SOCIO-LEGAL REV. 85, 105 (2015).

244 *Id.*

245 Shah, *supra* note 122, at 28; *see also* Shetty, *supra* note 237.

should avoid proposing such a system, no matter how beneficial and convenient it may seem.

CONCLUSION

In 2018, the Indian Supreme Court considered several petitions submitted in prior years addressing the mandatory use of Aadhaar and the overarching matter of citizens' right to privacy.[246] In the 2018 *Puttaswamy II* judgment, the Court declared Aadhaar to be constitutional and ruled that Aadhaar can be a mandatory requirement for government services.[247] However, the mandatory linkage of Aadhaar numbers to bank accounts and other private services is unconstitutional.[248] If the Indian Supreme Court had stricken down the Aadhaar Act as an unconstitutional violation of privacy rights, the Act might have been amended and re-implemented with greater privacy protections. By the Court permitting the mandatory linkage of Aadhaar to government services, the program will become the most essential and pervasive identity proof in India—the one number that connects citizens and residents to all governmental agencies.[249] While Aadhaar may create a more efficient distribution of services, it also exposes a vast number of Indians to cybercrime and potential privacy violations.[250]

However, considering that most Indians have already registered for Aadhaar,[251] the government may continue to incentivize Aadhaar linkages by creating persuasive and innovative ways to encourage the voluntary linkage of Aadhaar identities to private schemes. Even if this is the case, universal Aadhaar participation would not be the grimmest outcome (considering the benefits that

---

246 Rajagopal, *supra* note 184; *India's Top Court*, *supra* note 136; *Like It or Not, Aadhaar Will Be the Basis of Your Life in 2018*, ECON. TIMES, https://economictimes.indiatimes.com/news/politics-and-nation/like-it-or-not-aadhaar-will-be-the-basis-of-your-life-in-2018/articleshow/62303979.cms (last updated Dec. 30, 2017) [hereinafter *Aadhaar Will be the Basis of Your Life*].

247 *Puttaswamy II*, Writ Petition (Civil) No. 494 of 2012 1, 90–92 (Sup. Ct. India Sept. 26, 2018); *India's Top Court*, *supra* note 136.

248 *Puttaswamy II*, Write Petition (Civil) No. 494 of 2012 at 90–92; *India's Top Court*, *supra* note 136.

249 *Aadhaar Will Be the Basis of Your Life*, *supra* note 246.

250 *Id.*

251 Kumar, *supra* note 128.

Aadhaar does provide),[252] as long as there are efficient and reliable privacy measures to protect identity information and prevent mass surveillance by the Indian government.

The Indian Supreme Court's analysis of the right to privacy in the Indian Constitution is one step toward the implementation of more specific and enforceable privacy laws in India. Having a flexible and resilient interpretation of the Indian Constitution will allow future generations to address the concerns of a system such as Aadhaar. As rapid technological growth may render obsolete many present notions of privacy and security, laws must be able to evolve with the necessities and concerns of the time.

The Aadhaar system is fast becoming mandatory for government services in India for citizens and noncitizen residents alike. Community and government leaders can and should demand effective data privacy legislation to prevent the Orwellian[253] outcome of mass surveillance, data collection, and state intrusion. As more and more citizens become conditioned to accepting state intrusion into their lives, they run the risk of normalizing government data collection for possibly unconstitutional purposes.[254] Therefore, effective legislative solutions should include third-party oversight, judicial review, and transparent disclosures of information distribution.

These core elements of privacy will—at minimum—remove incentives to impose even more personally invasive methods of data collection and monitoring. This visceral loss of privacy weakens autonomy, leads to greater self-censorship, and increases risks for identity theft, profiling, and discrimination.[255] Losing privacy protections implicates cores values enshrined in the Constitutions of India and the United States. Hopefully, the United States will gain insight from the Aadhaar decisions in India and, if the United States does decide to implement a similar system, it should do so with privacy protections in mind.

---

[252] *See generally* McKenna, *supra* note 118, at 729–32 (describing how Aadhaar empowers the poorest segments of Indian society).

[253] *See* Ahlin, *supra* note 239.

[254] *See* SURVEILLANCE, PRIVACY, AND SECURITY: CITIZENS' PERSPECTIVES, *supra* note 238, at 217.

[255] Bhandari & Sane, *supra* note 162, at 9–12.