BIOMETRIC CRISIS: LEGAL CHALLENGES TO BIOMETRIC IDENTIFICATION INITIATIVES

MICHAEL ODDEN*

* J.D., University of Wisconsin Law School, 2022; B.A., with distinction, Marquette University, 2019.

INTRODUCTION

Biometric data is the most unique and unalterable information a person possesses.[1] According to the National Institute of Science and Technology, biometrics are "the measurement of physiological characteristics like - but not limited to - fingerprints, iris patterns, or facial features that can be used to identify an individual."[2] Beyond these physiological identifiers, biometric data includes behavioral identifiers such as the unique way an individual walks, talks, or performs gestures.[3] Because of biometric data's unchangeable connection to a person's very identity, this data is the most personal information that someone holds. Unfortunately, despite this information's importance, there is a general lack of privacy laws in the United States and in other countries that would protect individuals' biometric information from potential abuse.[4] In the United States, there is no federal biometric privacy legislation, creating a climate that allows for large-scale personal rights violations.[5] However, several states, most prominently Illinois, have emerged as leaders for enacting legislation that addresses privacy concerns and provides protections for citizens' biometric data. Illinois, in enacting the Biometric Information Privacy Act (BIPA), has demonstrated how legislation can proactively protect biometric data, while also providing a right to legal recourse should an individual's privacy be violated.[6] Individuals' biometric data is at risk globally, and these issues are only growing in importance as the field of biometric data is emerging and playing an increasingly prominent role in everyday life.

Large-scale government initiatives centered around the utilization of biometric data are being undertaken in numerous nations around the world.[7] In India, the government has implemented the most ambitious

---

1 *See* Claire Gartland, *Biometrics Are a Grave Threat to Privacy*, N.Y. TIMES (July 5, 2016), https://www.nytimes.com/roomfordebate/2016/07/05/biometrics-and-banking/biometrics-are-a-grave-threat-to privacy#:~:text=The%20reason%20to%20use%20biometrics,security%20threats%20for%20the%20victims [https://perma.cc/AM4A-7CVU].

2 *Biometrics*, NAT'L INST. OF STANDARDS & TECH. (July 11, 2018), https://www.nist.gov/programs-projects/biometrics [https://perma.cc/52TG-8ATV].

3 Alexander S. Gillis, Peter Loshin & Michael Cobb, *Definition: Biometrics*, TECHTARGET: SEARCH SEC., https://searchsecurity.techtarget.com/definition/biometrics (last updated July 2021) [https://perma.cc/3DBX-2CRB].

4 Gartland, *supra* note 1; *Biometrics FAQs*, CTR. FOR GLOB. DEV., https://www.cgdev.org/page/biometrics-faqs [https://perma.cc/RAE9-E5GJ].

5 *See* Gartland, *supra* note 1.

6 Biometric Information Privacy Act, 740 ILL. COMP. STAT. 14/15 to 14/20 (2008).

7 CTR. FOR GLOB. DEV., *supra* note 4.

program of its kind, Aadhaar, which has the express goal of creating a unique legal identification for all 1.2 billion residents.[8] A program of this scope relies on biometric information in the form of fingerprints and iris scans in order to create a person's identification.[9] The Aadhaar is seeking to accomplish an important goal, one that has been recognized by the United Nations under its "Legal Identity Agenda."[10] While an initiative such as Aadhaar may bring about improvements in streamlining government services, it may also create avenues for crucial biometric data to be misused and violated. Likewise, Kenya has received attention for its program, the National Integrated Identity System (NIIMS), which has been likened to Aadhar.[11] NIIMS sets forth the equally ambitious plan to create a national population registry of all citizens and foreigners in the nation using biometric data.[12] Just as the legitimacy and potential dangers of Aadhaar have been explored, NIIMS, too, has been criticized for its capacity to overreach into the lives of those registered in its database.[13] For these reasons, India and Kenya must remain cautious in the development and implementation of Aadhaar and NIIMS, respectively, and seek to take a more proactive approach in designing guardrails to the program that, from their inception, would protect the privacy of peoples' biometric information.

This Comment will examine the emerging legal challenges to biometric data requirements and will assess the United States' regulations, and then proceed to provide a new viewpoint for how to evaluate the ways that nations are implementing biometric data-driven initiatives. In Part I, this Comment will explore what biometric information is, and how it is being collected and used in the United States, India, and Kenya. In Parts

---

[8] Alan Gelb & Julia Clark, *Building a Biometric National ID: Lessons for Developing Countries from India's Universal ID Program*, CTR. FOR GLOB. DEV. (Oct. 15, 2012), https://www.cgdev.org/publication/building-biometric-national-id-lessons-developing-countries-india%E2%80%99s-universal-id-program [https://perma.cc/S7UR-QQ66].

[9] *Id.*

[10] *See* U.N. Stat. Div., U.N. Legal Identity Agenda, https://unstats.un.org/legal-identity-agenda/#:~:text=SDG%20Goal%2016.9%3A%20By%202030,a%20civil%20authority%2C%20by%20age [https://perma.cc/PEU3-C24F].

[11] Anita Babu, *Aadhaar's Kenyan cousin, Huduma Namba, faces constitutional test in court*, WK. MAG. (Sept. 24, 2019), https://www.theweek.in/news/world/2019/09/24/aadhaar-kenyan-cousin-huduma-namba-faces-constitutional-test-court.html [https://perma.cc/B6TM-MMB3].

[12] *Background*, HUDUMA NAMBA https://www.hudumanamba.go.ke/background/ [https://perma.cc/N7LJ-QH5V].

[13] *See* Mustafa Mahmoud, *Stopping the Digital ID Register in Kenya – A Stand Against Discrimination*, NAMATI (Apr. 25, 2019), https://namati.org/news-stories/stopping-the-digital-id-register-in-kenya-a-stand-against-discrimination/ [https://perma.cc/L6NU-G8E4].

II and III, this Comment will assess the constitutional challenges to the biometric identification programs of India and Kenya and compare the outcomes and implications of the judicial decisions for these nations. Part IV will address emerging threats to biometric data privacy in the United States and introduce potential measures to counteract threats by private and government entities. Part V concludes the Comment by evaluating the implications of the legal challenges to the requirements of biometric data.

I. BACKGROUND

A. THE STATUS OF BIOMETRIC DATA PROTECTION LAWS AND CHALLENGES IN THE UNITED STATES

In the United States, there is a regulatory void at the federal level that has shifted issues regarding violations of personal biometric data to the state level.[14] Currently, at the state level, there is little agreement as to what level of protection, if any, should exist for biometric data.[15] In part, this void of protection is perpetuated by the fact that legal texts are largely written as provisions relating to personal data protection and privacy in a broad sense, and this is often poorly adapted to biometric data.[16] Because states have been slow to enact laws that address issues regarding biometric data protection, it becomes necessary to assess model states which have been proactive on this issue. Currently, six states have passed their own biometric data statutes or expanded existing data privacy laws to include biometric identifiers.[17] Illinois leads the way.[18] By analyzing Illinois' laws, one can see how the federal government can respond to pressing issues

---

[14] Laura K. Donohue, *Technological Leap, Statutory Gap, and Constitutional Abyss: Remote Biometric Identification Comes of Age,* 97 MINN. L. REV. 407, 416 (2012).

[15] *See id. See also* Carra Pope, *Biometric Data Collection in an Unprotected World: Exploring the Need for Federal Legislation Protecting Biometric Data*, 26 J.L. & POL'Y 769, 769 (2018) (describing the lack of federal regulation protecting collection of biometric information and proposing a solution); *and* Kelly A. Wong, *The Face-ID Revolution: The Balance Between Pro-Market and Pro-Consumer Biometric Privacy Regulation*, 20 J. HIGH TECH. L. 229, 230–31 (2020) (addressing the need for a uniform federal regulation concerning biometric data and proposing a blueprint).

[16] *Biometric Data and Data Protection Regulations*, THALES (Jun. 16, 2021) https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/biometric-data [https://perma.cc/46D5-WB26].

[17] Natalie A. Prescott, *The Anatomy of Biometric Laws: What U.S. Companies Need to Know in 2020*, NAT'L L. REV. (Jan. 15, 2020), https://www.natlawreview.com/article/anatomy-biometric-laws-what-us-companies-need-to-know-2020 [https://perma.cc/8DRV-CJZ9].

[18] *Id.*

involving biometric data that are becoming increasingly unavoidable around the world.

Any discussion of notable biometric data protection laws in the United States must begin with Illinois and its Biometric Information Privacy Act (BIPA).[19] BIPA is the oldest and most powerful biometric data protection law in place in the United States.[20] The law states that no private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person or customer's biometric identifier or biometric information unless it informs the subject that their biometric information is being collected, stored, or used along with the purpose and length of use.[21] In addition to this requirement to inform, the private entity must also receive a written release by the person to whom the biometric information belongs.[22]

What is perhaps most notable about BIPA is that the law provides individuals with a right of action against an offending party for violations enumerated under BIPA.[23] The statute sets forth the damages that an aggrieved party is entitled to after BIPA violations.[24] Relief from the statute varies based on the violation, and ranges from a court injunction to damages of at least $1000.[25] Additionally, the statute permits an aggrieved party to receive attorney's fees.[26]

BIPA states that "[biometrics] are unlike other unique identifiers that are used to access finances or other sensitive information."[27] Unlike social security numbers, which can be changed once compromised, biometrics are unique to the individual, and once they are compromised, the individual has no way to change them.[28] BIPA's power and reach has been challenged, and a recent pivotal case centered on BIPA illustrates what kinds of challenges to biometric data requirements are occurring in the United States, and what similarities and differences they have to challenges occurring in other parts of the world.[29]

---

[19] Biometric Information Privacy Act, 740 ILL. COMP. STAT. 14/1 (2008).

[20] *See* Prescott, *supra* note 17.

[21] Biometric Information Privacy Act, 740 ILL. COMP. STAT. 14/15 (2008).

[22] *Id.*

[23] *See id.* § 20.

[24] *Id.*

[25] *Id.*

[26] *Id.*

[27] *Id.* § 5.

[28] *Id.*

[29] Rosenbach v. Six Flags Ent. Corp., 2019 IL 123186.

A pivotal challenge to the application and extent of the Illinois BIPA law came from the Illinois Supreme Court case *Rosenbach v. Six Flags Entertainment Corporation*.[30] The case addressed the central issue of whether someone qualifies as an "aggrieved" person.[31] The case then answers whether an "aggrieved person" may seek damages and injunctive relief under BIPA even if he or she has not articulated an actual injury beyond the violation of his or her rights under the statute.[32] This issue arose because Six Flags Great America theme park had used a fingerprinting process to issue repeat-entry passes to the park.[33] The system would scan passholders' fingerprints, collect, and record this biometric data, and then use it to quickly verify customers' identities upon subsequent visits to the theme park.[34] The rationale for the system was that it would make entry to the park faster and more seamless, maximize the time passholders are in the park, and eliminate lost revenue due to fraud or park entry from using someone else's pass.[35] While the fingerprinting system would generally ensure that the entry process was more efficient, the plaintiff in the case alleged that he had not been informed of the specific purpose or term for which his fingerprints had been collected.[36] The lack of consent and disclosure regarding the plaintiff's biometric data violated the BIPA protections to personal information and therefore provided the plaintiff a private cause of action.[37]

The Illinois Supreme Court held that when a private entity collected the plaintiff's biometric data without his consent, this violation constituted an invasion, impairment, or denial of the plaintiff's statutory rights.[38] Of significance, the court held that beyond the violation, no such consequences need to be pleaded or proved; the violation in itself is sufficient to support the individual's statutory cause of action.[39] This decision showcases the power of BIPA, and its ability to curtail private entities' collection and use of individuals' biometric data. While the implementation of biometric data-driven services may improve the

---

30 *Id.*
31 *Id.* ¶ 1.
32 *Id.*
33 *Id.* ¶¶ 4, 10.
34 *Id.* ¶ 4.
35 *Id.*
36 *Id.* ¶ 8.
37 *Id.* ¶¶ 33, 34, 40.
38 *Id.* ¶ 33.
39 *Id.* ¶ 40.

efficiency of entry and overall experience for a theme park attendee, this case acknowledges that at a much larger scale, there are significant personal costs to having one's biometric data collected, stored, and used under unspecified terms.[40]

B. LEGAL CHALLENGES TO INDIA'S BIOMETRIC DATA-DRIVEN INITIATIVE, AADHAAR

At the forefront of controversies involving the collection of biometric data is India's Aadhaar program. Initiated in 2009, Aadhaar is a twelve-digit number issued by the Unique Identification Authority of India (UIDAI).[41] UIDAI mandated that all Indians submit personal information, including biometrics, to receive an Aadhaar number from the government.[42] This number is used as a type of identification and corresponds to an individual's biometric and demographic data.[43] The data submitted must include ten fingerprints, two iris scans, and a facial photograph.[44] Largely replacing the role of traditional paper identification documents, this information would then be required to prove one's identity to receive government services.[45] This digital identification aims to provide citizens with better access to government aid and services, particularly those who live in more rural regions, where it could be much more difficult and time-consuming to receive legitimate government paperwork such as a birth certificate.[46]

In the immediate aftermath of Aadhaar, critics feared that Aadhaar would give the government unprecedented insight and control into the lives of all Indians.[47] Millions of the poorest Indians were denied their crucial food rations when distribution sources could not read fingerprints

---

[40] *Id.* ¶ 34.

[41] *About your Aadhaar*, UNIQUE IDENTIFICATION AUTH. OF INDIA, https://uidai.gov.in/my-aadhaar/about-your-aadhaar.html [https://perma.cc/XL99-R38R].

[42] *Id.*

[43] *Id.*

[44] *Id.*

[45] *See Usage of Aadhaar*, UNIQUE IDENTIFICATION AUTH. OF INDIA, https://uidai.gov.in/my-aadhaar/about-your-aadhaar/usage-of-aadhaar.html [https://perma.cc/27LQ-YTAK].

[46] *See Features of Aadhaar*, UNIQUE IDENTIFICATION AUTH. OF INDIA, https://uidai.gov.in/my-aadhaar/about-your-aadhaar/features-of-aadhaar.html [https://perma.cc/TLJ6-UGKX]. *See also* Gelb & Clark, *supra* note 8 (describing the possibility of the technology helping poor residents lacking birth certificates).

[47] Vindu Goel, *'Big Brother' in India Requires Fingerprint Scans for Food, Phones and Finances*, N.Y. TIMES (Apr. 7, 2018), https://www.nytimes.com/2018/04/07/technology/india-id-aadhaar.html [https://perma.cc/RK86-43LB].

from the hands of longtime manual workers.[48] Also, the unreliability of India's cellphone networks prevented some from connecting to the servers necessary to authorize their government services.[49] As a result of the poor execution of the program, at least 25 Indians are known to have died of starvation after Aadhaar-related verification problems prevented them from receiving their food rations.[50] Some local governments, including the local government of the nation's capital city, New Delhi, stopped using the Aadhaar system for its food programs.[51] Questions arose as to whether these issues stemming from the implementation of the Aadhaar program were merely growing pains or indications of deeper flaws within the system.[52]

In the landmark 2018 case, *Puttaswamy v. India*, the nation's Supreme Court ruled on challenges encapsulating these biometric ID concerns and the constitutionality of the Aadhaar Act.[53] The decision was delivered after 38 days of hearings on over 30 challenges.[54] The Supreme Court held that Aadhaar was constitutional, but some individual sections of the 2016 Aadhaar Act were unconstitutional.[55] In *Puttaswamy v. India*, the Supreme Court approved the use of Aadhaar for public matters such as the distribution of food rations, other government benefits, and the collection of income taxes.[56] The Supreme Court, however, did strike down Prime Minister Narendra Modi's attempts to require the digital ID for private purposes, like opening a bank account.[57] The Supreme Court also dismissed a provision in the 2016 Aadhaar Act that had given private companies like banks and cellphone companies access to individuals'

---

48 Vindu Goel, *India's Top Court Limits Sweep of Biometric ID Program*, N.Y. TIMES (Sept. 26, 2018), https://www.nytimes.com/2018/09/26/technology/india-id-aadhaar-supreme-court.html [https://perma.cc/HQ2M-ULR3].

49 *Id.*

50 *Id.*

51 *Id.*

52 Jyoti Panday, *Can India's Biometric Identity Program Aadhaar Be Fixed?*, ELEC. FRONTIER FOUND. (Feb. 27, 2018), https://www.eff.org/deeplinks/2018/02/can-indias-aadhaar-biometric-identity-program-be-fixed [https://perma.cc/UKD8-CGB6].

53 Puttaswamy v. Union of India, (2018) 494 SCR 3 (India).

54 Goel, *supra* note 48.

55 *Constitutionality of Aadhaar Act*, SUP. CT. OBSERVER, https://www.scobserver.in/court-case/constitutionality-of-aadhaar-act [https://perma.cc/4ACK-M88L]; *See* Manveena Suri, *Aadhaar: Supreme Court Upholds Controversial Biometric Database*, CNN (Sept. 26, 2018), https://www.cnn.com/2018/09/26/asia/india-aadhaar-ruling-intl/index.html [https://perma.cc/PV6X-8B7V].

56 Goel, *supra* note 48.

57 *Id.*

personal biometric data information in order to verify customer identities.[58] The Court also established protections with the intention that these new protections would prevent the government and other entities with access from misusing data in the name of national security.[59]

While the Indian Supreme Court's judgment limited the scope of the Aadhaar Act, the Indian government accepted the decision as a success.[60] Prime Minister Modi's Bharatiya Janata Party and the Indian National Congress both claimed the ruling was a "victory."[61] Speaking on the result of the case, Modi's Finance Minister, Arun Jaitley, claimed that the Court had recognized taxpayers' savings under the program, which he estimated at $12 billion a year.[62] These savings were said to be a result of Aadhaar's effectiveness in reducing abuse and fraud committed by fake or duplicative recipients of government benefits.[63] It is worth noting, however, that these figures are contested.[64]

Opposing the Indian government in litigation, Shyam Divan, a veteran litigator before the Supreme Court of India, asserted in an interview that the court had "contained" the government's efforts to use Aadhaar to build a surveillance state.[65] Divan's arguments likely influenced the dissenting Justice D.Y. Chandrachud, who concluded that the Aadhaar Act, as a whole, was unconstitutional.[66] The majority opinion recognized and addressed some of these constitutional concerns, particularly the security lapses that were felt by those who most heavily relied on government programs.[67] Despite the Court's recognition of these more controversial aspects of the program, the majority held that it trusted the government to resolve these problems as the Aadhaar program continued to develop.[68] The Indian government celebrated this decision as

---

58 *Id.*

59 *Id.*

60 *See id*.

61 *Id.*

62 *Id.*

63 *Id.*

64 Jean Drèze & Reetika Khera, *Aadhaar's $11-bn question: The numbers being touted by govt have no solid basis*, ECON. TIMES (Feb. 8, 2018), https://economictimes.indiatimes.com/news/economy/policy/aadhaars-11-bn-question-the-numbers-being-touted-by-govt-have-no-solid-basis/articleshow/62830705.cms [https://perma.cc/XXT8-EVQC].

65 Goel, *supra* note 48.

66 *Id.*

67 *Id.*

68 *Id.*

a success, as it received validation and approval from the nation's highest court to continue its development and implementation of Aadhaar.[69]

C. LEGAL CHALLENGES ARISING FROM A SIMILAR BIOMETRIC IDENTIFICATION INITIATIVE IN KENYA

In Kenya, the nation's High Court had suspended an initiative likened to the Aadhaar program, known as NIIMS, due to a lack of laws in place to uphold the security of the data collected.[70] The Kenyan government planned to assign each citizen a "Huduma Namba," or "service number," to serve as a unique identification number that would be required to enroll in school, get healthcare and housing, register to vote, get married, obtain a driver's license, open a bank account, and more.[71] The government of Kenya has already collected face and fingerprint scans of approximately forty million Kenyans.[72] This system is similar to the Aadhaar initiative in India because of its ambition in collecting the biometric data of all citizens with the defined goals of streamlining services and making services more available to the poor and those in rural communities.

After its suspension, this biometric ID plan drew more attention, faced more constitutional scrutiny, and has been challenged further in Kenyan courts by civil rights organizations claiming that the program disenfranchises members of minority groups who may not be able to get an ID card.[73] In an effort to push back against the breadth of powers NIIMS wields and the alleged lack of transparency in its implementation, the Nubian Rights Forum filed a case with the High Court of Kenya, Constitutional Human Rights Division.[74] The Kenya Human Rights Commission and Kenya National Commission on Human Rights each

---

[69] *See id.*

[70] Abdi Latif Dahir & Carlos Mureithi, *Kenya's High Court Delays National Biometric ID Program*, N.Y. TIMES (Jan. 31, 2020), https://www.nytimes.com/2020/01/31/world/africa/kenya-biometric-ID-registry.html [https://perma.cc/57ER-XZMN].

[71] *Id. See also* Daniel Cullen, *High Court of Kenya suspends implementation of biometric ID system*, OXFORD HUM. RTS. HUB, (Mar. 16, 2020), https://ohrh.law.ox.ac.uk/high-court-of-kenya-suspends-implementation-of-biometric-id-system/ [https://perma.cc/23KE-C2ZZ] (explaining the court's judgment halting the Huduma Namba system); HUDUMA NAMBA, *supra* note 12 (describing the system).

[72] Dahir & Mureithi, *supra* note 70.

[73] Nubian Rts. F. v. Att'y-Gen. (2019) 56, 58 & 59 K.L.R. 3 (Kenya); Cullen, *supra* note 71.

[74] *Nubian Rts. F.*, 56, 58 & 59 K.L.R.

filed petitions as well.[75] These petitions were consolidated, and additional interested parties and NGOs joined the civil action.[76] The challenges raised included: the non-transparency and noncompetitive manner in which the NIIMS contract was awarded, the use of a miscellaneous amendments bill to pass substantive amendments, the lack of public participation in the process, concerns over data privacy and protection, the right to information, and the risk that the system could further entrench discrimination of marginalized groups.[77]

The High Court of Kenya later reversed the suspension of NIIMS and ruled that the government, with conditions, could proceed with its mass data collection initiative for the NIIMS system.[78] However, the Court ruled to prevent government authorities from making registration to the NIIMS program mandatory, collecting DNA and GPS data, setting a deadline for enrollment, and sharing data between agencies or to third parties.[79]

The High Court of Kenya noted an objection raised by Petitioners stating that the process establishing NIIMS could be flawed due to inadequate public participation, but did not find this concern to warrant suspension.[80] However, the Court did take issue with substantive amendments to the act introduced through a Miscellaneous Amendments Bill; these bills are expected to contain only minor, non-controversial amendments.[81] The amendments introduced in this fashion were significant, as they included the following: the creation of the NIIMS system, a new definition of biometrics, and the collection of GPS coordinates from each person during registration.[82] This decision by the High Court of Kenya has drawn attention for both allowing the program to proceed and for its efforts in pushing back against elements of the program that could have long and drastic negative consequences for the people of Kenya.[83]

---

[75] *Id.*

[76] *Id.*

[77] OPEN SOC'Y JUST. INITIATIVE, Kenya's National Integrated Identity Management System 3 (Sept. 2019), https://www.justiceinitiative.org/uploads/8f3b665c-93b9-4118-ad68-25ef390170c3/briefing-kenya-nims-20190923.pdf [https://perma.cc/R5KM-UMF3]; Mahmoud, *supra* note 13.

[78] *Nubian Rts. F.*, 56, 58 & 59 K.L.R. at para. 107.

[79] *Id.*

[80] *Id.* at para. 98.

[81] OPEN SOC'Y JUST. INITIATIVE, *supra* note 77.

[82] *Id.*

[83] Cullen, *supra* note 71.

II. THE FRAMEWORK FOR LEGITIMIZING AADHAAR

A. FOUNDATION OF LEGAL CHALLENGES IN INDIA AND THEIR APPLICATIONS TO BIOMETRIC DATA ISSUES

The Supreme Court of India, in upholding the constitutionality of the Aadhaar Act, relied partly on a 2017 judgment that reaffirmed the right to privacy as a fundamental right in Indian jurisprudence.[84] The judgment also established a proportionality test to determine whether violations of the right to privacy have occurred and whether the violations may have been necessary.[85] Since this decision, the Supreme Court's analysis has been used as an important precedent in many cases to emphasize that privacy is, in fact, a fundamental right and to clarify the scope of privacy that a person is owed.[86] In applying the proportionality test, Indian courts must consider the following: "(i) The action must be sanctioned by law; (ii) The proposed action must be necessary in a democratic society for a legitimate aim; (iii) The extent of such interference must be proportionate to the need for such interference; (iv) There must be procedural guarantees against abuse of such interference."[87] When the Supreme Court of India upheld the constitutionality of the Aadhaar Act and greater Aadhaar program, the majority opinion relied on the fulfillment of the proportionality test established in *Puttaswamy*.[88] The court reasoned that the Aadhaar program did not violate citizens' right of privacy because minimal biometric data was collected in the enrollment process and the authentication process was not exposed to the internet.[89] The Supreme Court of India upheld the Aadhaar Act, but barred several provisions governing disclosure of personal information and the use of the Aadhaar network by private corporations.[90]

By applying the proportionality test, the majority opinion drew limits and applied a rationale that warranted restraining private entities from utilizing the Aadhaar network and its connection to citizens'

---

[84] Puttaswamy v. Union of India (*Puttaswamy I*), (2017) 10 SCC 1, 142–43.

[85] *Id*. at 252.

[86] Sangh Rakshita & Nidhi Singh, *The Puttaswamy Effect*, CTR. FOR COMMC'N GOVERNANCE NAT'L L. UNIV. DELHI (Jan. 22, 2020), https://ccgnludelhi.wordpress.com/2020/01/22/the-right-to-privacy-the-puttaswamy-effect/ [https://perma.cc/E62R-AQPZ].

[87] *Puttaswamy I*, 10 SCC at 252.

[88] Rakshita & Singh, *supra* note 86.

[89] Puttaswamy v. Union of India, (2019) 1 SCC 1 (*Puttaswamy II*); *See also* Rakshita & Singh, *supra* note 86.

[90] Rakshita & Singh, *supra* note 86.

identifications for their private purposes.[91] However, because biometric-based information plays an increasingly large role in government functions and day-to-day life,[92] it is valuable for all parties involved to have a defined framework that may be implemented to resolve issues of alleged privacy violations. The *Puttaswamy* framework presents an opportunity for the court to use its discretion; the proportionality prong is largely determined on a case-by-case basis as to whether there was a legitimate rationale for the encroachment on a persons' privacy.[93] Because the third prong is discretionary, courts must be careful to apply this rule consistently, or it may create confusion amongst other jurisdictions in future applications.[94] As a whole, the *Puttaswamy* framework is helpful even beyond India's jurisdiction. Because nearly every country's governing bodies are learning to grapple with biometric data issues, it is valuable for courts to have a method of determining what may be considered a violation, and what rationales are proportional to the threat to privacy rights.

The Supreme Court of India's reasoning from *Puttaswamy* continues to be viewed as precedent in subsequent privacy-related cases in courts across India.[95] The decisions from these cases affirm the court's holding that privacy is a fundamental right.[96] The 2019 case *Kumar v. Central Bureau of Investigation* is an important application of the proportionality framework because of how the Bombay High Court dealt with balancing the competing interests of public safety and the right to privacy.[97] Section 5(2) of the Indian Telegraph Act 1885 permits the interception of telephone communications in the case of a public emergency or where there is a public safety requirement.[98] The court

---

[91] *Puttaswamy II*, 1 SCC at 404.

[92] *See* Alexandro Pando, *Beyond Security: Biometrics Integration Into Everyday Life*, FORBES (Aug. 4, 2017), https://www.forbes.com/sites/forbestechcouncil/2017/08/04/beyond-security-biometrics-integration-into-everyday-life/?sh=12f472b6431f [https://perma.cc/NCE2-MLGG].

[93] *Puttaswamy II*, 1 SCC at 63.

[94] Ankush Rai, *Proportionality in Application – An Analysis of the "Least Restrictive Measure,"* INDIAN CONST. L. & PHIL. (May 8, 2020), https://indconlawphil.wordpress.com/tag/proportionality/#:~:text=Puttaswamy%20vs%20Union%20of%20India,and%20liberty%20under%20Article%2021.&text=In%20all%20these%20three%20cases,the%20four%2Dpronged%20proportionality%20test [https://perma.cc/GFL4-NAPR].

[95] *See* Kumar v. Cent. Bureau of Investigation, AIR 2019 Bom 2367 (India); Cent. Pub. Info. Officer v. Subhash Chandra Agarwal, (2019) 2010 SCC 10044 (India); Shine v. India, AIR 2018 SC 194 (India).

[96] *See Kumar*, AIR 2019 Bom 2367; *Agarwal*, (2019) 2010 SCC 10044; *Shine*, AIR 2018 SC 4898.

[97] *Kumar*, AIR 2019 Bom 2367.

[98] Indian Telegraph Act, 1885, § 5.

clarified that unless a public emergency has occurred or public safety interests demand it, the authorities have no jurisdiction to exercise the powers under Section 5(2).[99] The court defined public emergency as the "prevailing of a sudden condition or state of affairs affecting the people at large and calling for immediate action."[100] In its decision, the Bombay High Court applied the proportionality test laid out in the *Puttaswamy* decision, and held that the interception order failed the proportionality test and could not be justified by the interests of public safety.[101] This decision is important because it reflects a greater trend in personal information issues where privacy is at odds with purported public safety interests. Courts and legislative bodies must respect the set boundaries surrounding privacy and ensure that proper tests, such as the proportionality test, are applied so that individual rights to privacy are not lost entirely to government-driven efforts.

B. CRITICISM OF AADHAAR AND THE INDIAN GOVERNMENT'S RESPONSE

Indian courts have ruled on the Aadhaar program's constitutionality, and the Indian government has throughout voiced its belief and support for the initiative, but many critics of Aadhaar are deeply opposed to its implementation.[102] Despite promises from the government that the Aadhaar program's development would be safe and secure,[103] there remains room for debate whether the program will live up to its vast and ambitious plans, or whether it will depart from its ideals and take shape in a much more dangerously invasive form. The program's critics argue that the personal impact of the program may prove detrimental, particularly in instances where the database is abused.[104] Holding every citizen's most important personal information, the Aadhaar database would surely be an appealing target for cyber-crime. If this database was

---

[99] *Kumar*, AIR 2019 Bom 2367, at para. 6.

[100] *Id.* at para. 4.

[101] *Id.* at para. 19.

[102] Rahul Bhatia, *Critics of Aadhaar project say they have been harassed, put under surveillance*, REUTERS (Feb. 12, 2018), https://www.reuters.com/article/india-aadhaar-breach/critics-of-aadhaar-project-say-they-have-been-harassed-put-under-surveillance-idINKBN1FX0FU [https://perma.cc/Z2KV-Q8N6].

[103] *See id.*

[104] Mardav Jain, *The Aadhaar Card: Cybersecurity Issues with India's Biometric Experiment*, UNIV. OF WASH. (May 9, 2019), https://jsis.washington.edu/news/the-aadhaar-card-cybersecurity-issues-with-indias-biometric-experiment/ [https://perma.cc/GCC5-AYMX].

breached, it is plausible that government services could be breached and shut down. This is a complex issue as there is no uniform consensus as to how the Indian government should go about designing a program with its significantly vast goals, while also offering adequate protection. However, indications that the Indian government is making efforts to shut down and silence entities that challenge or at least question the scope and power of the program are troubling and reveal a deeper complexity in the Aadhaar program.[105]

In some instances, researchers and journalists who identified concerns or loopholes in the Aadhaar program have said that they have been targeted by government agencies, and have been served with criminal complaints for their critical work.[106] In one case, the Unique Identification Authority of India (UIDAI), the government body responsible for the Aadhaar, filed a criminal case against the *Tribune* newspaper based on a story it published, which stated that access to a citizen's Aadhaar card's database could be bought for 500 rupees, or the U.S. equivalent of $7.82.[107] This case created a strong response from media associations that criticized the actions of UIDAI and characterized the case as harassment toward those telling a story that would be of great public interest.[108] Despite this, UIDAI's response refused to characterize its criminal complaints as retributive, or against free press, but rather as a necessary response to a false narrative.[109] The head of India's telecom regulatory body said that there was an "orchestrated campaign" against Aadhaar because it was against the interests of those who thrive in the shadow economy, and those who were abusing subsidy systems less protected in a pre-Aadhaar time.[110] The Indian government has consistently responded that pushback to the program largely stemmed from those who profited from abusing welfare systems or other social services that were not well protected before Aadhaar.[111]

This argument should not be accepted without skepticism. For the head of the telecom regulatory body to dismiss valid criticism of the program by merely dismissing it as coming from scammers, he is creating a dangerous environment where no criticism to the program may be

---

[105] *See* Bhatia, *supra* note 102.
[106] *Id.*
[107] *Id.*
[108] *Id.*
[109] *Id.*
[110] *Id.*
[111] *Id.*

considered or heard at all. There appears to be a disconnect between those working toward implementing Aadhaar and the public citizens who are vulnerable as their biometric information is collected from them, sometimes against their will. Tension exists between UIDAI and critics of the program; this conflict demonstrates just how complex the development of this new system is and the disagreements and obstacles that exist preventing any sort of consensus regarding how Aadhaar should be implemented.

III. HOW THE HIGH COURT OF KENYA HALTED THE GOVERNMENT'S INITIATIVE

A. HIGH COURT RULING AND RESPONDING CRITICISM TO THE NIIMS PROGRAM OF KENYA

Following the initial phase of registration for NIIMS, there was immediate pushback to the government's initiative which manifested in a court case challenging the program's constitutionality and its requirements of personal biometric data.[112] The petitions of three civil rights groups were consolidated and brought to the High Court of Kenya challenging the legality of the NIIMS platform.[113] The High Court of Kenya identified three substantive issues requiring judgment and sought to draw a balance between the parties' interests.[114] The High Court in its decision recognized that, in order to reach its stated goals, the NIIMS system would require more than two biometric characteristics be entered; this affirmed the government's argument that NIIMS would not be able to function as it was designed if it were limited to an inadequate pool of data.[115] The Court also held, however, that this approval only applies to the collection of more traditionally collected biometric data like fingerprints, iris and face scans, and not a person's DNA or GPS coordinates.[116] The Court reasoned that those two methods of identification were overly intrusive and unnecessary and therefore violate Article 31 of the Constitution.[117] The High Court drawing a line here is of interest because it makes a value judgment as to

---

[112] Nubian Rts. F. v. Att'y-Gen. (2019) 56, 58 & 59 K.L.R. 3 (H.C.K.) (Kenya).
[113] *Id.* at para. 5.
[114] *Id.* at para. 537.
[115] *Id.* at para. 783.
[116] *Id.* at para. 784.
[117] *Id.*

which forms of data are exceedingly personal, and which forms of data may be collected and stored permanently by the government.[118] Following the decision, the Kenyan government may still pursue its goal of building a "single source of truth" on Kenyans' identities, but there still remains information which is untouchable under the NIIMS system.[119] While this explanation may have settled this issue in court in the short-term, there is still an argument that a person's fingerprints or face scans are as private and valuable as their DNA or GPS location and should therefore receive the same level of protection.

Next, the High Court recognized the need for a database for storage purposes, to which the collected biometric data can be compared.[120] The Court explained that there is utility in having both a local copy of the information, like an ID card, and a separate system for use by the national government.[121] The High Court determined that the biometric data collected in the NIIMS registry is necessary to NIIMS' stated purpose, and that the system can only provide trustworthy identification if a person's specific information is stored in the greater database.[122] The Court held that NIIMS is not superfluous and that it is necessary to meet the goals of the government's biometric identification initiative.[123] This judgment may not be sufficient to settle critics, however, who contend that NIIMS intrudes too far into the lives of Kenyan citizens, and that the NIIMS system is not developed to properly protect citizens from discrimination and violations of their right to equality.[124]

Lastly, the High Court ruled on whether there was a violation of the right to equality and non-discrimination.[125] The issue here arose between the government and the suing civil rights groups, which demanded that NIIMS, as it is developed and implemented, properly protect citizens from discrimination.[126] Kenya is home to nearly 50 million people with a population that encompasses dozens of different ethnic

---

[118] *Id.*
[119] *Id.* at para. 785.
[120] *Id.* at para. 783.
[121] *Id.* at para. 787.
[122] *Id.*
[123] *Id.* at para. 784.
[124] *See* Mahmoud, *supra* note 13.
[125] *Nubian Rts. F.*, 56, 58 & 59 K.L.R. at para. 982.
[126] *Id.*

groups.[127] During the initial registration phase for NIIMS, which collected the biometric information of roughly 40 million people, many minorities failed to register through the registration drives.[128] This was in large part because members of Kenya's minority groups, such as the Nubians, already face discrimination when applying for the documents required to get the national identity cards or birth certificates required to register into the NIIMS system.[129] Therefore, already disadvantaged groups in Kenyan society are at risk of becoming even further disadvantaged in society as registration under NIIMS increasingly becomes a requisite to most facets of daily life.

The High Court cited the nation's Constitution, specifically Article 27, which guarantees the right to equality, non-discrimination, and equal benefit of the law.[130] The Court drew attention to the fact that the law being challenged, which established NIIMS, applies to "information of all Kenyan citizens and registered foreigners resident in Kenya."[131] Article 27 does not make differentiations between nationals or foreigners, and therefore everyone, including members of ethnic minorities, is allowed to register under NIIMS.[132] The Court shifted its focus to recognize that the real issue in this challenge was that the persons from marginalized areas are subjected to discriminatory and onerous processes to establish their Kenyan nationality and obtain their identification cards.[133] However, the Court ultimately sided with the government, stating that the petitioners had not properly established a violation of the right to equality and non-discrimination because the law did not establish or require that a person undergoes a vetting process, just that they present themselves with an identification document in order to be registered under NIIMS.[134]

The High Court of Kenya ruled that the government may proceed with its plan to implement NIIMS and assign all citizens an ID number, but that the process must be done under a comprehensive regulatory

---

[127] Morgan Winsor, *Digital IDs that civil rights groups say bar minorities are lawful in this country*, ABC NEWS (Jan. 31, 2020), https://abcnews.go.com/International/kenya-rule-digital-ids-civil-rights-groups-disenfranchize/story?id=68635887 [https://perma.cc/YKD4-CTMH].

[128] *Id.*

[129] *Id.*

[130] CONSTITUTION art. 27 (2010) (Kenya).

[131] *See Nubian Rts. F.*, 56, 58 & 59 K.L.R. at para. 990.

[132] CONSTITUTION art. 27 (2010) (Kenya).

[133] *Nubian Rts. F.*, 56, 58 & 59 K.L.R. at para. 991.

[134] *Id.* at para. 992.

framework in place with regards to data and the treatment of minorities.[135] In the Court's words, "[such] a framework will need to regulate the manner in which those without access to identity documents or with poor biometrics will be enrolled in NIIMS."[136] In conclusion, the Court stated that it recognizes the possibility for marginalized groups' exclusion, but that this possibility is not in itself a sufficient reason to find NIIMS as a whole to be unconstitutional.[137]

A lingering issue remains following the decision from the High Court of Kenya. The Court affirmed the concerns of the suing civil rights groups and acknowledged that NIIMS may potentially exacerbate discriminatory practices aimed toward ethnic minorities, yet it gave little to no instruction as to how the government may go about implementing the necessary components to promote equality and freedom from discrimination which had previously been lacking in the first iteration of NIIMS.[138] The civil rights groups which put pressure on the government may have some degree of influence on the direction of NIIMS development, but the responsibility ultimately falls upon the Kenyan government to ensure that this point of emphasis is not forgotten or ignored. As such, moving forward, it will be critical for human rights groups, such as the Nubian Rights Forum, to continue pressuring the Kenyan government to improve the system. This ideal system will be able to reach the heights of the program's ambitions without bringing such a high potential cost to the safety and freedom of ethnic groups that are already at-risk of suffering on the fringes of society. The Court provided the government a clear mandate to include the necessary provisions to ensure that the most at-risk groups in the nation's population would be adequately protected,[139] but it is unclear whether the government will take affirmative measures to correct and adjust the challenging registration requirements of the NIIMS system to be more readily inclusive.

---

[135] Tony Bitzionis, *Kenya's National Biometric ID Program Delayed by High Court*, FIND BIOMETRICS (Feb. 3, 2020), https://findbiometrics.com/biometrics-news-kenyas-national-biometric-id-program-delayed-high-court-020301/ [https://perma.cc/58XC-G7ZU].

[136] *Nubian Rts. F.*, 56, 58 & 59 K.L.R. at para. 1012.

[137] *Id.*

[138] *Id.* at para. 1012.

[139] *Id.*

B. COMPARING THE CONSTITUTIONAL CHALLENGES OF THE BIOMETRIC PROGRAMS AND THEIR OUTCOMES

The right to privacy is a fundamental right that has been enshrined in many constitutions around the world and has been recognized in international human rights law.[140] The right to privacy is multifaceted and enables other rights. One of these is the protection of individuals' data.[141] Since 1988, the United Nations Human Rights Committee has recognized the need for data protection laws to safeguard this essential right.[142] The development and implementation of both the Aadhaar and NIIMS systems in many ways challenge most people's conception of this right. It is a contentious matter as to whether these programs intrude too far into individuals' personal lives, despite the promises delivered by government bodies. The unique identification number will be required in order to participate in nearly every aspect of ordinary life.[143] Education, health care, housing, voting, marriage, bank accounts, and more will be tied to the unique number and if one cannot collect the necessary documents or travel to the proper offices in order to obtain an ID, life becomes perilously uncertain.

The legal challenges to both Aadhaar and NIIMS, and the responses they received, offer an opportunity to compare the two systems. They are similar in that both the Supreme Court of India and the High Court of Kenya recognize that the mass collection of citizens' biometric data is constitutional while it is fulfilling the overarching goals established by the government.[144] The Courts' decisions, however, indicate that there must be some limits in place as the biometric identification programs

---

[140] Thomas Fisher, *Affidavit of Dr. Thomas Fisher of Privacy International*, PRIVACY INT'L (Apr. 11, 2019), https://privacyinternational.org/sites/default/files/2019-05/Kenya%20affidavit%20website%20version.pdf [https://perma.cc/T9C2-37K2].

[141] Hum. Rts. Comm., Gen. Comment No. 16: Art. 17 (Rt. to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, ¶ 10, U.N. Doc. HRI/GEN/1/Rev.9 (Apr. 8, 1988) [hereinafter The Right to Respect]. *See* Frank La Rue (Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression), *Rep. of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, ¶ 58, U.N. Doc. A/HRC/17/27 (May 16, 2011); U.N. High Comm'r for Hum. Rts., *The Right to Privacy in the Digital Age*, ¶ 6, U.N. Doc. A/HRC/39/29 (Aug. 2018).

[142] The Right to Respect, *supra* note 141, ¶ 10.

[143] Abdu Latif Dahir, *Kenya's New Digital IDs May Exclude Millions of Minorities*, N.Y. TIMES (Jan. 28, 2020) https://www.nytimes.com/2020/01/28/world/africa/kenya-biometric-id.html [https://perma.cc/U9CM-E3KM].

[144] Puttaswamy v. Union of India, (2018) 494 SCR 3. *See* Nubian Rts. F. v. Att'y-Gen., 56, 58 & 59 K.L.R. 2, 171 (H.C.K.) (Kenya).

presented in their initial forms do raise serious concerns. How deeply these programs intrude into citizens' personal lives and how peoples' lives may change when their most personal information is compiled onto a single ID card and database remain significant questions.

The Supreme Court of India did not halt Aadhaar, nor did it prescribe a solution to the myriad ways the biometric ID systems threaten disadvantaged groups in Indian society. For both India and Kenya to develop and implement their national biometric data systems, it will be critical to build on the groundwork laid out by the High Court of Kenya, which acknowledges that biometric ID initiatives can present certain dangers and challenges that may not be present for all groups of people. Civil rights groups must continue to advocate for marginalized groups who may struggle to integrate into a rapidly digitizing society. Just as India and Kenya grapple with issues regarding personal data and increasingly challenged privacy, the United States, too, has the opportunity to determine its path forward, particularly as federal agencies expand their usage of biometric data.

IV. THE UNITED STATES GOVERNMENT'S RESPONSE TO BIOMETRIC DATA CONCERNS

A. EMERGING THREATS FROM THE U.S. DEPARTMENT OF HOMELAND SECURITY

While the United States has not enacted federal legislation governing the collection and use of biometric data, the Department of Homeland Security (DHS) and its Office of Biometric Identity Management (OBIM) collect and use individuals' biometric data for a range of purposes, similar to the Aadhaar and NIIMS projects of India and Kenya, respectively.[145] Naturally, concerns arise as to whether proper safeguards are in place and whether the capabilities of DHS will be within defined limits.[146] At DHS, biometric data is used to detect and prevent illegal entry into the United States, to grant and administer proper immigration benefits, to vet and provide credentials, to facilitate legitimate

---

[145] *Biometrics*, DEP'T OF HOMELAND SEC., (June 9, 2021), https://www.dhs.gov/biometrics [https://perma.cc/2RQP-SY3C]; *see* Gartland, *supra* note 1.

[146] *See* Matthew Guariglia, *Tell the Department of Homeland Security: Stop Collecting DNA and other Biometrics*, ELEC. FRONTIER FOUND. (Sept. 29, 2020), https://www.eff.org/deeplinks/2020/09/tell-department-homeland-security-stop-collecting-dna-and-other-biometrics [https://perma.cc/GD4P-WAGD].

travel and trade, to enforce federal laws, and to enable verification for visa applications to the United States.[147] These procedures are set to expand under a new proposal that would extend the capabilities of DHS to collect and store biometric data for its database; this development could have dire consequences for immigrants and U.S. citizen sponsors alike.[148] The United States does not yet have laws in place or court precedent available to challenge DHS' procedures, and violations of countless citizens' right to privacy of their biometric data will likely ensue.

On September 1, 2020, DHS announced its intentions to drastically expand U.S. Citizenship and Immigration Services' (USCIS) collection of the biometric data of both non-citizens and U.S. citizens.[149] The proposal would permit USCIS to require U.S. citizens and children to submit to biometric data collection so that the agency could create detailed biological profiles of individuals involved in the immigration system by gathering data from facial scans, voice prints, and even DNA samples.[150] This proposed rule by DHS presents a concerning development in issues of biometric data infringements in the United States.[151] While the United States has not moved toward a biometric-based identification system such as those found in India and Kenya, federal agencies like DHS are utilizing individuals' biometric data for their own purposes with largely unclear terms, goals, and limitations.[152] DHS asserts that its Automated Biometric Identification System (IDENT) holds as many as 260 million unique identities and processes more than 350,000 biometric transactions per day.[153] This data is not held by DHS alone; DHS shares this critical biometric information with the Department of Defense along with the Department of Justice.[154] The information sharing across different federal agencies for different purposes highlights the similarities this type of data network shares with a fully-fledged biometric data-based identification system like Aadhaar or NIIMS. This proposal by DHS would significantly extend its reach without sufficient oversight by any legislative body and

---

147 DEP'T OF HOMELAND SEC., *supra* note 145.

148 *See DHS, USCIS to Modernize, Define the Collection of Biometrics*, DEP'T OF HOMELAND SEC., (Sept. 1, 2020), https://www.dhs.gov/news/2020/09/01/dhs-uscis-modernize-define-collection-biometrics [https://perma.cc/73FC-9CX5].

149 *Id.*

150 *See* Guariglia, *supra* note 146.

151 *See id.*

152 *See id.*; discussion *infra* Sections I-B, I-C.

153 DEP'T OF HOMELAND SEC., *supra* note 145.

154 *Id.*

could drastically overreach into the most fundamental private data of anyone involved in the immigration process.

B. U.S. CONGRESSIONAL INTERVENTION TO UPHOLD BIOMETRIC DATA PRIVACY

The DHS-proposed biometric data collection plan is not supported by the United States Congress and should not be implemented. Congress is currently challenging the agency's use of biometric information, and it has not authorized DHS to act as broadly as it seeks to under the grounds of its proposed rule.[155] In a letter challenging the DHS-proposed biometric data submission requirements, Senators Markey, Sanders, Wyden, Warren, and Merkley urged DHS to abandon its plans to drastically expand U.S. Citizenship and Immigration Services' collection of biometric information of both non-citizens and U.S. citizens alike.[156] In the letter to then-acting DHS Secretary Chad Wolf, the Senators expressed their grave concerns that the proposed rule—allowing DHS to collect biometric information as it conducts removal proceedings, processes family-based immigration applications, and reviews immigrants seeking naturalization—would threaten the public's privacy.[157]

The senators reason that the USCIS proposal would dramatically expand the populations subject to "invasive biometric data collection."[158] The new rule would change the policy so that DHS may require any "applicant, petitioner, sponsor, beneficiary, or individual filing to associated with an immigration benefit or request" to appear and have their biometric data collected.[159] This regulation would allow DHS to force both U.S. citizens and non-U.S. citizens to share personal biometric information with the federal government, which may potentially violate

---

[155] Press Release, Ed Markey, U.S. Senate, Senators Markey, Merkley Lead Colleagues on Legislation to Ban Government Use of Facial Recognition, other Biometric Technology (June 15, 2021), https://www.markey.senate.gov/news/press-releases/senators-markey-merkley-lead-colleagues-on-legislation-to-ban-government-use-of-facial-recognition-other-biometric-technology [https://perma.cc/D7CL-CUVW].

[156] Press Release, Ed Markey, U.S. Senate, Markey, Sanders, Wyden, Warren, and Merkley Demand Trump Administration Abandon Plans for Expanded Biometric Data Collection in Immigration System (Oct. 16, 2020), https://www.markey.senate.gov/news/press-releases/markey-sanders-wyden-warren-and-merkley-demand-trump-administration-abandon-plans-for-expanded-biometric-data-collection-in-immigration-system [https://perma.cc/7VB7-S6W4].

[157] *Id.*

[158] *Id.*

[159] *Id.*

constitutionally protected privacy and search and seizure rights.[160] That DHS would force children to share their data is particularly concerning because there had previously been age-based exemptions available for those who were subject to biometric data collection.[161]

The practice of collecting immense amounts of data profiles is not safe for those who have submitted their data. According to a report from the DHS Office of the Inspector General, a data breach involving a facial recognition pilot program at U.S. Customs and Border Protection resulted in the exposure of more than 180,000 traveler images and this resulted in dozens of these images later appearing on the dark web.[162] The Inspector General concluded that DHS "did not adequately safeguard sensitive data on an unencrypted device used during its facial recognition technology pilot" and this casts doubt on DHS' ability to safely collect and store biometric profiles on a further expanded scale.[163] DHS is dangerously moving forward in its plan, without congressional insight or approval, and without guiding principles of privacy or proportionality. Until this shortcoming is acknowledged, these moves forward must continue to be challenged by authorities that may best represent the interests of individuals and their rights to privacy over basic biometric information.

The United States Congress is poised to address issues beyond the proposed plan by DHS and it must succeed in enacting legislation that will prevent widespread violations of biometric information from occurring under the authority of federal agencies. Senators Markey and Merkley, and Representatives Jayapal and Pressley, have introduced legislation that would ban government use of facial recognition and other biometric technology.[164] The Facial Recognition and Biometric Technology Moratorium Act would "[p]lace a prohibition on the use of facial

---

[160] Markey, *supra* note 156; Saira Hussain, Jennifer Lynch & Nathaniel Sobel, *EFF Files Comment Opposing the Department of Homeland Security's Massive Expansion of Biometric Surveillance*, ELEC. FRONTIER FOUND. (Oct. 22, 2020), https://www.eff.org/deeplinks/2020/10/eff-files-comment-opposing-department-homeland-securitys-massive-expansion [https://perma.cc/M2YV-C859].

[161] Markey, *supra* note 156.

[162] OFF. OF THE INSPECTOR GEN., OIG-20-71, REVIEW OF CBP'S MAJOR CYBERSECURITY INCIDENT DURING A 2019 BIOMETRIC PILOT (2020), https://www.oig.dhs.gov/sites/default/files/assets/2020-09/OIG-20-71-Sep20.pdf [https://perma.cc/53R8-DJ73].

[163] *Id.*

[164] Press Release, Ed Markey, U.S. Senate, Senators Markey and Merkley, and Reps. Jayapal, Pressley to Introduce Legislation to ban Government Use of Facial Recognition, Other Biometric Technology (June 25, 2020), https://www.markey.senate.gov/news/press-releases/senators-markey-and-merkley-and-reps-jayapal-pressley-to-introduce-legislation-to-ban-government-use-of-facial-recognition-other-biometric-technology [https://perma.cc/2QKN-RKAR].

recognition and other biometric technologies by federal entities which [could] only be lifted with an act of Congress."[165] This Act would also prohibit the use of information collected via biometric technology that violates the Act in judicial proceedings, and would include a private right of action for individuals whose biometric data is used in violation of the Act.[166] This Act would allow for enforcement by state Attorneys General and would allow states and localities to enact their own laws regarding the use of facial recognition and biometric technologies.[167]

This legal challenge to overreaching biometric technologies represents the type of step that governing bodies in the United States must take if they are to finally address the growing importance of these issues in a rapidly developing field.[168] This proposed legislation from the United States Congress regarding government capabilities to collect and use biometric data on a broad scale[169] conveys a similar message to what was voiced by the High Court of Kenya, particularly in its concern for the extent of violations that may occur when a government agency has broad and virtually unfettered control over citizens' biometric data.[170] Where the challenges in Kenya and in India have, in some part, curtailed the biometric data collection capacities of private entities or given protections to exceedingly personal information such as DNA or GPS data, the United States has the potential to act and take an even greater proactive step in setting clear terms, limits, and modes of recourse for violations of citizens' personal biometric data committed by federal agencies. This action is both crucial and necessary in order to prioritize the population's interests, while also respecting new technological methods and the natural developments of technology.

V. CONCLUSION

At the heart of a person's identity is their biometric information. A person's walk, manner of speech, and facial features are fundamental to who a person is. And while there is great value to this information, it is not easily defined by courts or government bodies around the world. The

---

[165] *Id.*; Facial Recognition and Biometric Technology Moratorium Act of 2020, S. 4084, 116th Cong. (2020).

[166] *Id.*

[167] *Id.*

[168] *See id.*

[169] *Id.*

[170] *See* Nubian Rts. F. v. Att'y-Gen. (2019) 56, 58 & 59 K.L.R. 2 (H.C.K.) (Kenya).

recent developments in organized government initiatives to collect and use biometric data for government programs in the United States, India, and Kenya, demonstrate that one's biometric data is only going to become more prevalent in ordinary aspects of daily life. It is crucial that identification programs driven by biometric data are not designed to operate at the expense of the people who contributed to their creation. The critics' voices must continue to be heard, legal recourse should be made available in instances of violations, and government agencies must provide transparency in the development and implementation of these programs. Only when the dignity attached to a person's most personal information is respected and valued may any biometric data initiative proceed in an ethical way. When these needs are met, national biometric data programs will be better suited to pursue broad ambitions of modernizing and streamlining services beneficial to the people of their respective nations.