Journal of Law and Policy

Volume 26 | Issue 2 Article 7

5-7-2018

Biometric Data Collection in an Unprotected World: Exploring the Need for Federal Legislation Protecting Biometric Data

Carra Pope

BIOMETRIC DATA COLLECTION IN AN UNPROTECTED WORLD: EXPLORING THE NEED FOR FEDERAL LEGISLATION PROTECTING BIOMETRIC DATA

*Carra Pope**

Currently, there are no federal statutes which protect or regulate the collection of biometric information. Because biometric identifiers cannot be changed if compromised, it is increasingly crucial that this data be protected by law. This note examines the barriers to federal legislation which would protect and regulate biometric data, as well as the steps that should be taken to enact federal biometric legislation in the future.

INTRODUCTION

In 2017, the United States experienced one of the largest data breaches to date when the Equifax credit reporting service was hacked, exposing the names, driver's license numbers, Social Security numbers, and other sensitive personal information of over 145 million Americans.[1] As a result, many people are now concerned that hackers may have gained access to personal identifiers.[2] In order to avoid similar breaches in the future, lessons must be drawn from the Equifax breach about the ways our personal identifying information has traditionally been left vulnerable to

---

*J.D. Candidate at Brooklyn Law School, 2019. I would like to express my sincerest gratitude to Professor Susan Herman for her encouragement and support in pursuing biometric research. I would also like to thank the members of the *Journal of Law and Policy* for their editorial assistance.

[1] Ron Lieber, *How to Protect Yourself After the Equifax Credit Breach*, N.Y. TIMES, https://www.nytimes.com/interactive/2017/your-money/equifax-data-breach-credit.html (last updated Oct. 16, 2017).

[2] *See id.*

breaches, and how the government can best work to protect this sensitive data in the future.

Biometric identifiers are one of the most unprotected areas of our personal identity and could be susceptible to large-scale breaches in the future.[3] Currently, there are no federal statutes protecting or regulating the collection or commercial use of biometric identifiers, and only limited state protections.[4] These are "digital or analog representation[s] of physical attributes that can be used to uniquely identify [each of] us."[5] Biometric identifiers include a variety of personal attributes, such as "fingerprints, voice, or [walking] gait."[6] In fact, one wide-reaching confidential biometric data breach has already occurred.[7] In 2015, a breach of the Office of Personnel Management resulted in the theft of approximately 5.6 million fingerprints.[8] This hack alarmed those on Capitol Hill who suspected that China had orchestrated the data breach in an attempt to build a database of American identities; however, Congress took no action to ensure a breach of this size would not happen again.[9]

---

[3] *See* Chiara A. Sottile, *As Biometric Scanning Use Grows, So Does Security Risk*, NBC NEWS (July 24, 2016), https://www.nbcnews.com/mach/mach/biometric-scanning-use-grows-so-do-security-risks-ncna593161.

[4] *See* Ted Claypoole & Cameron Stoll, *Developing Laws Address Flourishing Commercial Use of Biometric Information*, BUS. LAW TODAY, AM. BAR ASS'N. (May 2016), https://www.americanbar.org/publications/blt/2016/05/08_claypoole.html.

[5] *New NIST Biometric Data Standard Adds DNA, Footmarks and Enhanced Fingerprint Descriptions*, NAT'L INST. OF STANDARDS AND TECH. (Dec. 6, 2011), https://www.nist.gov/news-events/news/2011/12/new-nist-biometric-data-standard-adds-dna-footmarks-and-enhanced [hereinafter *NIST Biometric Data Standard Adds DNA*].

[6] *Biometrics*, ELEC. FRONTIER FOUND., https://www.eff.org/ja/issues/biometrics (last visited May 1, 2018) [hereinafter *Biometrics*, ELEC. FRONTIER FOUND.].

[7] Julianne Pepitone, *OPM Hack: 5.6 Million Fingerprints (Not 1.1 Million) Were Stolen*, NBC NEWS (Sept. 23, 2015), https://www.nbcnews.com/tech/security/opm-5-6-million-fingerprints-not-1-1-million-were-n432281.

[8] *Id.* Many of those targeted by the breach were federal employees. *See id.*

[9] *See* Andrea Peterson, *OPM Says 5.6 Million Fingerprints Stolen in Cyberattack, Five Times as Many as Previously Thought*, WASH. POST (Sept. 23, 2015), https://www.washingtonpost.com/news/the-switch/wp/2015/09/23/opm-now-says-more-than-five-million-fingerprints-compromised-in-

This Note argues that without comprehensive federal legislation regulating and protecting the biometric data of all Americans, citizens remain at risk of having their personal identifiers stolen and exploited.[10] Experts have warned that hackers can use this biometric data for leverage, leaving those affected by a breach dealing with the fallout for years.[11] Moreover, this Note argues that the lack of public knowledge on the issue of biometric data collection has allowed technology companies, such as Facebook, to create a climate favorable to their use of customers' biometric data, largely without their knowledge or consent.[12] The United States government's "wait and see" approach to technology and the law[13] is effectively forcing the American public to wait until a disastrous data breach occurs for the law to change. Rather than drafting responsive legislation in the aftermath of a crisis, the federal government must take proactive steps to prevent data breaches. Accordingly, the federal government must pass legislation which protects biometric data privacy and ensures that companies secure this data, rather than use it for their own profit.

---

breaches/?utm_term=.6db4e37930da. A Chinese national was later arrested in 2017 for selling the malware which caused the OPM breach. *See* Aruna Viswanatha & Robert McMillan, *Chinese National Charged with Providing Hackers with Malware Linked to OPM Breach*, WALL ST. J. (Aug. 24, 2017), https://www.wsj.com/articles/chinese-national-charged-with-providing-hackers-with-malware-linked-to-opm-breach-1503626027.

[10] Those with security sensitive positions are especially at risk. *See* Pepitone, *supra* note 7.

[11] Experts have also warned that as technology evolves, hackers will have more methods of exploiting biometric data. *Biometrics*, ELEC. FRONTIER FOUND., *supra* note 6.

[12] *See, e.g.*, April Glaser, *Facebook Is Using an "NRA Approach" to Defend Its Creepy Facial Recognition Programs*, SLATE (Aug. 4, 2017), http://www.slate.com/blogs/future_tense/2017/08/04/facebook_is_fighting_biometric_facial_recognition_privacy_laws.html [hereinafter Glaser, *Facebook Is Using an "NRA Approach"*] (explaining how Facebook has collected the facial data of millions of its users and is now the biggest lobbying force against biometric data privacy laws).

[13] *See* Lawrence Lessig, *The Path of Cyberlaw*, 104 YALE L.J. 1743, 1744 (1995) (discussing that with the Internet, it is best to let technology develop before the laws regulating it: "let the experience catch up with the technology, a way to give the ordinary language a chance to evolve, and a way to encourage new languages where the old gives out.").

Part I of this Note discusses what biometric data gathering entails, how this data is collected by private companies and the government, and why the average person should be wary of its collection. Part II explores biometric gathering programs outside the United States, and the potential for similar programs to be implemented within the country. Part III examines the effectiveness of state statutes in Illinois, Texas, and Washington that protect biometric data privacy. Part IV analyzes the limited case law regarding biometric data privacy. Finally, Part V scrutinizes proposed federal legislation to protect and regulate biometric data privacy and proposes several methods which could bring that legislation to the forefront of national discourse.

I. WHAT IS BIOMETRIC DATA AND HOW IS IT COLLECTED?

Many people do not know what biometric data is, much less how it is collected. It is important to understand what biometric data entails, and who is collecting and keeping this sensitive data. As biometric technology becomes more commonplace, it is increasingly important to understand how this data collection affects our everyday activities.

A. What is Biometric Data?

Given the highly sensitive nature of biometric data, and the consequences of its dissemination and theft, it is necessary to understand the ways in which it is being collected. Biometric data is unlike other sensitive personal information in that it is collected by both public and private actors.[14] Currently, the biometric data of citizens and non-citizens is collected by the government[15] and

---

[14] Credit information is held by three major reporting agencies: Equifax, TransUnion, and Experian; whereas biometric information is collected and held by a variety of actors, including the government, private companies, and other third parties. *See generally Credit Reports and Scores*, USA.GOV, https://www.usa.gov/credit-reports (last updated March 18, 2018).

[15] *See generally Fingerprints and Other Biometrics*, FBI, https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/ (last visited May 1, 2018) (explaining the FBI's biometric data gathering program); *see also Biometrics*, U.S. DEP'T OF HOMELAND SEC. (Feb. 6, 2017),

private companies,[16] including third parties such as biometric aggregator Daon.[17] This sensitive data is defined by its non-shareability.[18] The term "biometric data" encompasses a multitude of unique personal identifiers,[19] which can include a person's fingerprints,[20] DNA samples,[21] iris or retinal scans,[22] voice recordings,[23] walking gait,[24] typing pattern of the fingers,[25] 3D facial

---

https://www.dhs.gov/biometrics [hereinafter *Biometrics*, U.S. DEP'T OF HOMELAND SEC.] (discussing how the department uses biometric data to stop terrorism and other criminal activity).

[16] *See Face Recognition*, ELEC. FRONTIER FOUND., https://www.eff.org/sls/tech/biometrics/faq#faq-How-do-private-companies-use-biometrics? (last visited May 1, 2018) (discussing how private companies use biometric data they have collected from their users).

[17] *See About Daon*, DAON, https://www.daon.com/company/about-daon (last visited May 1, 2018); *see also* Martin Anderson, *DNA-based Advertising Redefines Commercial Ad-Targeting*, THE STACK (Sept. 16, 2015), https://thestack.com/security/2015/09/16/ancestry-com-dna-advertising/ (explaining how the ancestry.com DNA matching program uses its participants' DNA in conjunction with third parties to target advertising based on their DNA).

[18] Andrea Chang & Samantha Masunaga, *Apple Says iPhone X's FaceID Can't be Easily Spoofed. But Your Face Isn't Exactly Private*, L.A. TIMES (Sept. 12, 2017), http://www.latimes.com/business/technology/la-fi-tn-apple-iphone-face-id-20170913-story.html.

[19] *See NIST Biometric Data Standard Adds DNA*, *supra* note 5.

[20] *See id.*

[21] *See id.*

[22] *See id.*; Dario Betancourt, *Difference Between Retina and Iris Biometric Identification*, BIOMETRIC NEWS PORTAL (Oct. 5, 2017), https://www.biometricnewsportal.com/retina_biometrics.asp.

[23] *See* Tim De Chant, *The Boring and Exciting World of Biometrics*, PBS (June 18, 2013), http://www.pbs.org/wgbh/nova/next/tech/biometrics-and-the-future-of-identification/.

[24] *See id.*

[25] *See Biometrics: Who's Watching You*, ELEC. FRONTIER FOUND. (Sept. 14, 2003), https://www.eff.org/wp/biometrics-whos-watching-you.

scans,[26] and other forms of hand geometry data.[27] Unlike other, changeable forms of identification, such as driver's licenses or passports, biometric identifying information cannot be changed to safeguard your identity or other assets which use your biometrics to secure. For example, the fingerprints of a German Defense Minister were stolen from high resolution images of herself online.[28] Some experts have cautioned that stealing a person's fingerprints is as easy for a hacker as stealing a password.[29] Since this data cannot be changed once it is compromised, the security risks associated with a biometric hack are great. As such, it is important that the government take prompt action to protect this data.

B. How the United States Government Gathers Biometric Data

The federal government has been carrying out biometric data-collecting initiatives for longer than most citizens might realize;[30] for example, the FBI began its national fingerprint collection

---

[26] *See* Bryson Masse, *What's the Worst That Could Happen With Huge Databases of Facial Biometric Data?*, GIZMODO (September 11, 2017, 9:51 AM), http://gizmodo.com/what-s-the-worst-that-could-happen-with-huge-databases-1802696698.

[27] Stephen Mayhew, *Explainer: Hand Geometry Recognition*, BIOMETRICUPDATE.COM (June 22, 2012), https://www.biometricupdate.com/201206/explainer-hand-geometry-recognition.

[28] Alex Hern, *Hacker Fakes German Minister's Fingerprints Using Photos of Her Hands*, GUARDIAN (Dec. 30 2014), https://www.theguardian.com/technology/2014/dec/30/hacker-fakes-german-ministers-fingerprints-using-photos-of-her-hands. This incident led to many experts suggesting that biometrics only be used as a second factor of authentication, rather than as a standalone method of security. *Id.*

[29] Kaveh Waddell, *When Fingerprints Are as Easy to Steal as Passwords*, THE ATLANTIC (March 24, 2017), https://www.theatlantic.com/technology/archive/2017/03/new-biometrics/520695/.

[30] *Fingerprints and Other Biometrics*, *supra* note 15 (explaining that the FBI has been a leader in biometrics, starting the first national biometric data program (fingerprinting) in 1924); *see also Biometrics and Security*, CTR. FOR STRATEGIC & INT'L STUDIES, https://www.csis.org/programs/strategic-technologies-program/cybersecurity/other-projects-cybersecurity/biometrics-and (last visited May 1, 2018) ("Governments have been collecting biometric data for decades.").

program in 1924.[31] The FBI founded the Biometric Center of Excellence in 2007, which works to strengthen and drive the nation's biometrics programs.[32] Additionally, the FBI has developed the Next Generation Identification (NGI) program, which it claims is the "world's largest and most efficient electronic repository of biometric and criminal history information."[33] The FBI is not the only government agency collecting biometric data;[34] the Departments of Justice, Homeland Security, Defense, State, and other agencies work together to send biometric information to the Office of Biometric Identity Management (OBIM).[35] In addition to these federal agencies, state, local, and tribal law enforcement also collect and share biometric data with the OBIM.[36]

The attacks of September 11, 2001 motivated much of this interagency cooperation, as well as the push for a national biometric data program, and these efforts are specifically aimed at fighting terrorism.[37] The OBIM claims that the use of biometric data in

---

[31] *Fingerprints and Other Biometrics*, *supra* note 15.

[32] *See About the Biometric Center of Excellence*, FBI, https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/biometric-center-of-excellence/about-the-biometric-center-of-excellence (last visited May 1, 2018).

[33] *See Next Generation Identification (NGI)*, FED BUREAU OF INVESTIGATION, https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/ngi (last visited May 1, 2018); *see also Fingerprints and Other Biometrics*, *supra* note 15 (discussing the FBI's Next Generation Identification program).

[34] *See Biometrics*, U.S. DEP'T OF HOMELAND SEC., *supra* note 15 (explaining that biometric data is collected by multiple government agencies).

[35] *See id.*

[36] *See generally* NATIONAL PROTECTION AND PROGRAMS DIRECTORATE, OFFICE OF BIOMETRIC IDENTITY MANAGEMENT, U.S. DEP'T OF HOMELAND SEC. OFFICE OF BIOMETRIC IDENTITY MANAGEMENT MULTI-YEAR INVESTMENT AND MANAGEMENT PLAN ii (June 11, 2015), https://www.dhs.gov/sites/default/files/publications/National%20Protection%20and%20Programs%20Directorate%20%28NPPD%29%20-%20Office%20of%20Biometric%20Identity%20Management%20Multi-Year%20Investment%20and%20Management%20Plan.pdf (explaining how "state, local, and tribal law enforcement" agencies coordinate biometric data collection with OBIM).

[37] DEFENSE SCI. BD., U.S. DEP'T OF DEF., REPORT OF THE DEFENSE SCIENCE BOARD TASK FORCE ON DEFENSE BIOMETRICS 3 (2007), https://fas.org/irp/agency/dod/dsb/biometrics.pdf (discussing how biometric data

national security makes "travel simple, easy and convenient for legitimate visitors, but virtually impossible for those who wish to do harm or violate U.S. laws."[38] One of the first major changes to national biometric strategy came in 2003, when the Department of Homeland Security (DHS) created the US-VISIT program.[39] The US-VISIT program was created to more accurately keep records of all persons entering and exiting the country by collecting visitors' biometric data, including digital fingerprints and photographs, at border crossings and airport terminals.[40] As part of the expansive US-VISIT program, all U.S. visa applicants are required to submit their biometric data to the U.S. Citizenship and Immigration Service (USCIS) before their applications will be processed.[41] DHS checks that data against terrorist and other watch lists to verify the individual's identity.[42] The US-VISIT program has also been used to authorize the collection of biometric data from migrants entering

---

use has changed since 9/11, as well as the need for interagency cooperation to prevent future terrorist attacks).

[38] *Office of Biometric Identity Management Identification Services*, U.S. DEP'T OF HOMELAND SEC. (Feb. 10, 2016), https://www.dhs.gov/obim-biometric-identification-services.

[39] *See generally* U.S. DEP'T OF HOMELAND SEC., FACT SHEET 1 (2007), http://www.fosterglobal.com/govt_websites/USVisitDHSFactSheet12-2007.pdf (explaining how US-VISIT was started in 2003 and identifying the programs that would be implemented under its authority).

[40] *See id.* Additionally, in 2018 the government announced it would be expanding the biometric program at airports to include all the country's biggest and busiest airports. *See* U.S. CUSTOMS AND BORDER PROTECTION (CBP), U.S. DEP'T OF HOMELAND SEC., COMPREHENSIVE BIOMETRIC ENTRY/EXIT PLAN FISCAL YEAR 2016 REPORT TO CONGRESS i (2016), https://www.dhs.gov/sites/default/files/publications/Customs%20and%20Border%20Protection%20-%20Comprehensive%20Biometric%20Entry%20and%20Exit%20Plan.pdf.

[41] U.S. DEP'T OF HOMELAND SEC., FACT SHEET, *supra* note 39, at 1–2.

[42] *See id.* at 3; *see also Testimony of Deputy Assistant Secretary for Policy Kathleen Kraninger, Screening Coordination, and Director Robert A. Mocny, US-VISIT, National Protection and Programs Directorate, Before the House Appropriations Committee, Subcommittee on Homeland Security, "Biometric Identification"*, U.S. DEP'T OF HOMELAND SEC. (March 19, 2009), https://www.dhs.gov/news/2009/03/19/testimony-biometric-identification [hereinafter *US-Visit Testimony*] (discussing the ways US-VISIT verifies an individual's identity when entering and exiting the country).

illegally by the sea near Puerto Rico and other US territories.[43] DHS claims US-VISIT has improved with border control security significantly because it allows law enforcement to verify a person's identity before allowing them into the country, creating more efficient travel both at border crossings and in airports.[44]

The government claims that many of the improvements in immigration and border security are due to Immigration and Customs Enforcement's (ICE) Secure Communities initiative.[45] The goal of the Secure Communities initiative is to improve interoperability between state and local law enforcement and federal biometric databases.[46] This interoperability allows local law enforcement to send the biometrics of those detained by the FBI and DHS, who can check their biometrics against an immigration database.[47] If a person's biometrics are identified in the immigration system as unlawful or otherwise removable, ICE can choose to take enforcement action.[48] ICE claims that this initiative led to the removal of over 363,400 criminal aliens from the U.S. between 2008 and 2014 and the program's reactivation in 2017.[49]

This interagency cooperation has also led to the creation of the Automated Biometric Identification System (IDENT), which is maintained by OBIM.[50] Statistics about IDENT's data collection

---

[43] U.S. DEP'T OF HOMELAND SEC., FACT SHEET, *supra* note 39, at 3.

[44] *See id.* at 2–3*; see also* Jeff John Roberts, *Homeland Security Plans to Expand Fingerprint and Eye Scanning at Borders*, FORTUNE (Sept. 12, 2016), http://fortune.com/2016/09/12/border-security-biometrics/.

[45] *See generally Secure Communities: Overview*, U.S. IMMIGRATION AND CUSTOMS ENF'T, https://www.ice.gov/secure-communities (last updated March 20, 2018) (discussing how the Secure Communities program has been successful); *see also US-Visit Testimony*, *supra* note 42 (explaining how ICE has increased their performance since the implementation of the Secure Communities initiative).

[46] Memorandum of Agreement Between U.S. Department. of Homeland Security. Immigration and Customs Enforcement and State Identification Bureau (available at https://www.ice.gov/doclib/foia/secure_communities/securecommunitiesmoatemplate.pdf) (last visited May 1, 2018).

[47] *Secure Communities: Overview*, *supra* note 45.

[48] *Id.*

[49] *Id.* Since the Trump administration reactivated the initiative, over 43,000 "convicted criminal aliens" were deported in 2017 alone. *Id.*

[50] *See Biometrics*, U.S. DEP'T OF HOMELAND SEC., *supra* note 15.

reveal just how commonplace government biometric data has become.[51] IDENT currently holds more than 200 million biometric identities and processes more than 300,000 biometric transactions per day.[52] A large portion of these transactions come from state and local law enforcement, which submit roughly 50,000 biometric samples per day across the country.[53] These very large figures demonstrate just how largescale our national biometric programs have become.

The federal government has recently deployed several pilot programs for biometric data collection at airports for travelers leaving the U.S.[54] Using facial recognition technology, the new exit programs check a traveler's live facial scans against their passport photo to ensure they match.[55] If a traveler is determined to be a U.S. citizen, they are to be removed from the exit screening and their photo is to be removed from the file.[56] However, the government does not disclose how long facial data might stay in the government's possession.[57] Since there is no regulation of this type of data, there is no guarantee that the government will destroy the biometric data in a timely manner, or at all.

The federal government was not the only government actor that increased its biometric data gathering after 9/11; similarly, New York City created what is now known as the Domain Awareness System.[58] The Domain Awareness System is a counterterrorism program developed to "facilitate the observation of pre-operational

---

[51] *See generally id.*

[52] *Id.*

[53] *US-Visit Testimony*, *supra* note 42.

[54] *See CBP Deploys Biometric Exit Technology to Chicago O'Hare International Airport*, U.S. CUSTOMS AND BORDER PROTECTION (July 11, 2017), https://www.cbp.gov/newsroom/national-media-release/cbp-deploys-biometric-exit-technology-chicago-o-hare-international.

[55] *Id.*

[56] *Id.*

[57] *See generally id.* (explaining that U.S. citizen's facial data will be removed from government databases "after a short period of time").

[58] Chris Francescani, *NYPD Expands Surveillance Net to Fight Crime as Well as Criminals*, REUTERS (June 21, 2013, 11:24 AM), https://www.reuters.com/article/usa-ny-surveillance/nypd-expands-surveillance-net-to-fight-crime-as-well-as-terrorism-idUSL2N0EV0D220130621.

activity by terrorist organizations or their agents."[59] As part of the program, the NYPD utilizes more than 6,000 cameras citywide through a network funded in part by the Department of Homeland Security.[60] Although the program does not use facial recognition software, it can collect biometric data, such as an individual's walking gait, in furtherance of the stated purpose to control pedestrian traffic.[61] Even though the government cites many national security-related reasons for the collection of biometric data, there remain many significant privacy risks for those who wish to safeguard this highly sensitive data.

It is crucial to note that "[l]aw enforcement use of biometrics poses special problems."[62] While the government's collection of biometric data may seem to only affect travelers, visiting non-citizens, or those being processed into the criminal justice system, many Americans who have committed no crime have had their biometric information collected by the FBI's NGI program.[63] Additionally, there is evidence to suggest that the NGI system has disproportionately collected the biometric information of African Americans and Latinos.[64] This is worrisome because it means that the facial recognition technology used by the FBI may be more likely to misidentify African Americans and Latinos than other groups of people.[65]

Nevertheless, a new exemption to the NGI program leaves most of those who may be misidentified or wish to otherwise challenge

---

[59] NYPD, PUBLIC SECURITY PRIVACY GUIDELINES 2 (2009), http://www.nyc.gov/html/nypd/downloads/pdf/crime_prevention/public_security_privacy_guidelines.pdf.

[60] Francescani, *supra* note 58.

[61] *See* NYPD, *supra* note 59, at 1–3.

[62] *Biometrics and Security*, *supra* note 30 (arguing that without regulation of biometric data programs is "underdeveloped" and as a result the US government has blurred the line between foreign and domestic law enforcement).

[63] Letter from 18 Million Rising et al. to Ms. Erika Lee Brown, U.S. Department of Justice (May 27, 2016) (available at https://assets.documentcloud.org/documents/2849880/Letter-urges-Justice-Department-to-grant-public.pdf) [hereinafter Letter to DOJ].

[64] *Id.*

[65] *Id.* (explaining that young people are also more at risk of being misidentified).

their data's inclusion in the program without any recourse.[66] In August 2017, the program became exempt from the Privacy Act of 1974.[67] Citing national security reasons, the FBI will no longer have to disclose whether an individual's biometrics are included in the NGI database, no longer need consent to share an individual's biometric data with other agencies, and no longer need consent to amend an individual's profile within the program.[68] Many privacy groups have argued that this exemption will render the Privacy Act meaningless, leaving citizens without any way to know if their biometric profiles are full of errors, and without judicial redress if they discover this to be the case.[69] This is a troublesome development for those who would like to challenge the presence of their biometrics in the NGI database, or their misidentification through the program.[70]

Some law-abiding citizens have been mistakenly identified as terrorism suspects through government biometric identification programs.[71] Brandon Mayfield, an attorney and Army veteran from Oregon, was mistakenly identified as a suspect in the aftermath of the 2004 Madrid bombings, in which 191 people were killed and about 2,000 were injured.[72] After an FBI supercomputer incorrectly matched Mayfield's fingerprints with those found on a bag at the

---

[66] *See* Madelyn Bacon, *FBI's Next Generation Identification System Exempt from Privacy Act*, TECH TARGET (Aug. 11, 2017), http://searchsecurity.techtarget.com/news/450424332/FBIs-Next-Generation-Identification-system-exempt-from-Privacy-Act; Ellen Nakashima, *FBI Wants to Exempt its Huge Fingerprint and Photo Database from Privacy Protections*, WASH. POST (June 1, 2016), https://www.washingtonpost.com/world/national-security/fbi-wants-to-exempt-its-huge-fingerprint-and-photo-database-from-privacy-protections/2016/05/31/6c1cda04-244b-11e6-8690-f14ca9de2972_story.html?utm_term=.cc04afdbcc86.

[67] Bacon, *supra* note 66.

[68] *Id.*

[69] *See* Letter to DOJ, *supra* note 63.

[70] *See id.*

[71] *See, e.g.*, Harry Schuster & Terry Frieden, *Lawyer Wrongly Arrested in Bombings: 'We lived in 1984'*, CNN (Nov. 30, 2006), http://www.cnn.com/2006/LAW/11/29/mayfield.suit/index.html.

[72] *FBI Apologizes to Lawyer Held in Madrid Bombings*, NBC NEWS (May 25, 2004), http://www.nbcnews.com/id/5053007/ns/us_news-security/t/fbi-apologizes-lawyer-held-madrid-bombings/#.Wg9sQkxFxD8.

scene of the bombings, multiple FBI analysts then erroneously confirmed the match (despite the fact that fifteen other fingerprints were matched in the system).[73] As a result, Mayfield's property, as well as his family's, was seized from his residence by the government, and he was placed in jail for over two weeks.[74] Even after it was determined the FBI had made a mistake in identifying Mayfield as a suspect, he was held as a material witness to the bombing, and his movements were tracked by the government.[75] The FBI eventually issued an apology to Mayfield,[76] but his story is a cautionary tale demonstrating how the government's unregulated[77] use of biometric data can have disastrous consequences for mistakenly-identified individuals. Without legislation protecting biometric identities, there is nothing stopping future cases like that of Brandon Mayfield's.

C. How Private Companies Gather Biometric Data

Private companies have been collecting biometric data for many years, frequently by monitoring peoples' interactions with their smartphones.[78] Whether a phone uses the increasingly ubiquitous

---

[73] *Id. See also* Press Release, FBI National Press Office, Statement on Brandon Mayfield Case (May 24, 2004) (available at https://archives.fbi.gov/archives/news/pressrel/press-releases/statement-on-brandon-mayfield-case).

[74] *See FBI Apologizes to Lawyer Held in Madrid Bombings*, *supra* note 72.

[75] *See id.* (explaining that the FBI's claim that Mayfield's attendance at a local mosque served as additional evidence to support his arrest, even after the Spanish authorities had determined another man's fingerprints were on the bag).

[76] *Id.*

[77] *See generally* Carlton Purvis, *Report: Biometric Data Being Collected with 'Little to No Standards, Oversight, or Transparency'*, ELEC. FRONTIER FOUND. (May 23, 2012), https://www.eff.org/ja/mention/report-biometric-data-being-collected-little-no-standards-oversight-or-transparency.

[78] April Glaser, *Biometrics are Coming, Along with Serious Security Concerns*, WIRED (March 9, 2016), https://www.wired.com/2016/03/biometrics-coming-along-serious-security-concerns/; *see also Company Overview of Daon, Inc.*, BLOOMBERG, https://www.bloomberg.com/research/stocks/private/snapshot.asp?privcapId=7827847 (last visited May 1, 2018); *About Daon*, *supra* note 17 (Daon is the one of the world's largest private holders of biometric information, holding over 100 million unique identities, and has been in operation in the United States since 2002). *See, e.g.*, Jeff Chiu, *App Scans Faces of Bar-Goers to Estimate Age, Man-to-Woman Mix of Crowd for Would-be Patrons*,

fingerprint to unlock,[79] iris scans,[80] or an advanced technology like the new iPhone X and Samsung Pass 3D facial screening,[81] each one records a user's biometric data and stores that information on the phone.[82] Knowing that people might be wary about the storage of their fingerprints, Apple has claimed that biometrics are never stored on their servers or in iCloud, and are only stored directly on the user's device.[83] However, with the release of the iPhone X, Apple broke its promise to users and began sharing facial data with third-party applications through the phone's new "TrueDepth" camera.[84] Because there are currently no federal laws regulating the use of biometrics by private companies, those who are outraged by this practice are left with little to no legal recourse.

However, phone companies are not the only private actors collecting our biometric data. Amusement parks such as Disney World gather the biometric data of park-goers to ensure there is no

---

ELEC. FRONTIER FOUND. (May 31, 2012), https://www.eff.org/ja/mention/app-scans-faces-bar-goers-estimate-age-man-woman-mix-crowd-would-be-patrons (showing that in 2012 apps were already using facial recognition technology).

[79] *See, e.g.*, Vindu Goel, *That Fingerprint Sensor on Your Phone is Not as Safe as You Think*, N.Y. TIMES (April 10, 2017), https://www.nytimes.com/2017/04/10/technology/fingerprint-security-smartphones-apple-google-samsung.html.

[80] *Samsung Pass*, SAMSUNG, http://www.samsung.com/global/galaxy/apps/samsung-pass/ (last visited May 1, 2018) (describing the different security features of the Samsung Pass program, available on new Samsung smartphones, which includes facial recognition technology and iris scanning).

[81] *See* Clare Garvie, *Facial Recognition is Here. The iPhone X is Just the Beginning*, GUARDIAN (Sept. 13, 2017), https://www.theguardian.com/commentisfree/2017/sep/13/facial-recognition-iphone-x-privacy; *see also Samsung Pass*, *supra* note 80.

[82] *See About Touch ID Advanced Security Technology*, APPLE (Sept. 11, 2017), https://support.apple.com/en-us/HT204587.

[83] *Id.*

[84] Geoffrey A. Fowler, *Apple is Sharing Your Face with Apps. That's a New Privacy Worry*, WASH. POST (Nov. 30, 2017), https://www.washingtonpost.com/news/the-switch/wp/2017/11/30/apple-is-sharing-your-face-with-apps-thats-a-new-privacy-worry/?utm_term=.7eb596ecc715 (explaining that Apple has received little attention for sharing users' facial data with apps since the release of the newest iPhone model).

ticket fraud within their parks.[85] Newer video games, such as EA's NBK 2K series and FIFA soccer games, collect users' biometric data through GameFace, a 3D facial scanning technology which creates personal profiles for game players.[86] Fitbit and other fitness tracking wearable devices collect biometric data as well.[87] Even the NFL Players Association recently agreed to a deal which allows players to sell biometric data collected through wearables.[88] These instances are concerning because most users are unaware that their biometrics are being collected and stored without any form of legal protection.

Another increasingly popular way our biometric data is being collected is through ancestry background services that use DNA, such as 23andMe and Ancestry.[89] The 23andMe company has amassed the DNA of over 2 million individuals.[90] However, the personal data collected by 23and Me is not appropriately safeguarded against hacking.[91] In one instance, a hacker claimed that he had gotten access to the 23andMe application program

---

[85] *My Disney Experience—Frequently Asked Questions*, DISNEY, https://disneyworld.disney.go.com/faq/my-disney-experience/my-magic-plus-privacy/ (last visited May 1, 2018).

[86] *See Put on Your Game Face*, ELEC. ARTS GAMES, https://www.easports.com/nba-live/companion-app (last visited May 1, 2018) (explaining that EA Gameface technology allows the user to scan his or her facial geometry via a smartphone camera. These scans can be used across the current EA gaming catalog).

[87] *See generally* Cavan Canavan, *The Future of Biometric Marketing*, TECHCRUNCH (Dec. 21, 2014), https://techcrunch.com/2014/12/21/the-future-of-biometric-marketing/ (discussing how wearable devices, such as Fitbit and other fitness trackers, which collect biometric data, will be increasingly popular in the future).

[88] *See* Rhett Jones, *NFL Players Strike a Deal to Sell Their Biometric* Data, GIZMODO (April 24, 2017, 11:45 PM), https://gizmodo.com/nfl-players-strike-a-deal-to-sell-their-biometric-data-1794616994.

[89] *See* Ron Dichter, *Biometrics: Are We Going Too Far?*, FORBES (June 5, 2017, 9:00 AM), https://www.forbes.com/sites/forbesfinancecouncil/2017/06/05/biometrics-are-we-going-too-far/#7fe5de5d1b8d.

[90] *See id.*

[91] Kristen V. Brown, *What DNA Testing Companies' Terrifying Privacy Policies Actually Mean*, GIZMODO (Oct. 18, 2017, 10:10 AM), https://gizmodo.com/what-dna-testing-companies-terrifying-privacy-policies-1819158337.

interface (API) and created a program that could "restrict access to your [web]site based on traits including sex, ancestry, disease susceptibility, and arbitrary characteristics associated with single-nucleotide polymorphisms (SNPs) in a person's genotype."[92] Furthermore, some privacy advocates are concerned by 23andMe's openness about selling its participants' personal health data to third parties.[93]

More recently, many people have raised concerns about 23andMe and Ancestry.com's ability to share biometric information with law enforcement.[94] One man was wrongfully held for six hours and his blood drawn by police after a false match of his DNA (provided by Ancestry) connected him to a 1996 murder.[95] Although these companies have been open about the fact that they share users' information with police and sell their data to third parties, some privacy advocates have doubts about whether customers would be upset if they were more fully aware of the use of their personal data.[96] Since biometric data is unprotected by federal law, many people who might want to challenge these business practices are left without a remedy.

Facebook has gathered a large amount of its users' biometric data through its facial recognition technology, widely considered to be the most remarkable collection of biometric information by a

---

[92] Bio-IT World Staff, *23andMe Shuts Down App that Uses Genetic Information to Screen Access*, CAMBRIDGE HEALTHTECH INST. (July 22, 2015), http://www.bio-itworld.com/2015/7/22/23andme-shuts-down-app-uses-genetic-information-screen-access.html.

[93] *See* Matthew Herper, *Surprise! With $60 Million Genentech Deal, 23andMe Has a Business Plan*, FORBES (Jan. 6, 2015, 9:58 AM), https://www.forbes.com/sites/matthewherper/2015/01/06/surprise-with-60-million-genentech-deal-23andme-has-a-business-plan/.

[94] *See* Fiza Pirani, *Can Police Legally Obtain Your DNA from 23andMe, Ancestry?*, ATLANTA JOURNAL-CONSTITUTION, http://www.ajc.com/news/national/can-police-legally-obtain-your-dna-from-23andme-ancestry/8eZ24WN7VisoQiHAFbcmjP/ (last updated May 11, 2018). 23andMe claims it keeps a record of police requests for personal data in its Transparency Report, see 23ANDME, TRANSPARENCY REPORT (2017), https://www.23andme.com/transparency-report/.

[95] Pirani, *supra* note 94.

[96] *See* Herper, *supra* note 93.

private company.[97] Facebook claims that it has a "practically infinite" amount of facial data from its 2 billion users to help train the facial recognition technology.[98] One of the inventors of facial recognition technology believes that Facebook's database could allow its system to "recognize the entire population of earth."[99] Facebook uses this facial data to research artificial intelligence with the goal to improve targeted advertising to its users.[100] More alarmingly, Facebook has made no promises to its users regarding the future uses of this facial data.[101] This massive data-collection program, and its inherent potential for abuse and for-profit exploitation, is the driving force behind litigation against Facebook under state statutes protecting biometric data.[102] Since Facebook is such a large company, only a piece of federal legislation regulating this kind of biometric data collection could deter their facial data gathering program.

II. BIOMETRIC DATA GATHERING PROGRAMS AROUND THE WORLD

Many countries have started to adopt biometrics programs of their own.[103] In Argentina, Germany, Italy, and many other countries around the world, biometric identifiers are used to create a national identification system.[104] It is increasingly important to understand the ways biometrics are used by other countries, since any biometric programs successfully implemented internationally

---

[97] *See* Jared Bennett, *Saving Face: Facebook Wants Access Without Limits*, CTR. FOR PUB. INTEGRITY (July 31, 2017), https://www.publicintegrity.org/2017/07/31/21027/saving-face-facebook-wants-access-without-limits.

[98] *See id.*

[99] *Id.*

[100] *Id.*

[101] In 2013, Facebook's Chief Privacy Officer, when asked for assurances the facial data would never be used for other purposes, responded, "absolutely not." *Id.*

[102] *See generally* In re Facebook Biometric Info. Privacy Litig., 185 F. Supp. 3d 1155 (N.D. Cal. 2016).

[103] *Mandatory National IDs and Biometric Databases*, ELEC. FRONTIER FOUND, https://www.eff.org/issues/national-ids (last visited May 1, 2018).

[104] *Id.*

could result in similar programs being enacted within the United States.

A. India's Aadhaar Program

Aadhaar, a national biometric data collection program in India, is the largest of its kind in the world.[105] More than one billion people have had their biometric identifiers cataloged as part of the program, including fingerprints, photographs, and iris scans.[106] Participation in the Aadhaar program is essentially compulsory;[107] one must be enrolled in order to receive government benefits like pensions and food subsidies.[108] Recently, the country announced that Aadhaar identification must be linked to citizens' bank accounts in order to prevent money laundering.[109] Though some claim that the policy reduces government waste and fraud,[110] others have argued that the Aadhaar program presents significant privacy issues.[111]

In fact, the Aadhaar program has already shown that it has significant security vulnerabilities.[112] A recent report released by the Centre for Internet and Society, India, claimed that over 130 million

---

[105] *See* Namrata Kolachalam, *The Privacy Battle Over the World's Largest Biometric Database*, THE ATLANTIC (Sept. 5, 2017), https://www.theatlantic.com/technology/archive/2017/09/aadhaar-worlds-largest-biometric-database/538845/.

[106] *See id.*

[107] *See id.*

[108] *See* Vidhi Doshi, *No ID, No Benefits: Thousands Could Lose Lifeline Under India's Biometric Scheme*, GUARDIAN (March 21, 2017), https://www.theguardian.com/global-development/2017/mar/21/no-id-no-benefits-thousands-could-lose-lifeline-india-biometric-scheme-aadhaar-card.

[109] *RBI Clears Aadhaar Air, Says Linking Mandatory for Bank Accounts Under Laundering Rules*, ECONOMIC TIMES, www.economictimes.indiatimes.com/articleshow/61162307.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst (last updated Oct. 22, 2017) (explaining the new government ruling on compliance with the Aadhaar program, as well as who is exempt from the requirement).

[110] *See* Kolachalam, *supra* note 105.

[111] *See id.*; Doshi, *supra* note 108.

[112] *See* Dell Cameron, *130 Million at Risk of Fraud After Massive Leak of Indian Biometric Data System*, GIZMODO (May 13, 2017, 12:27 PM), https://gizmodo.com/130-million-at-risk-of-fraud-after-massive-leak-of-indi-1794856154 (explaining a reported breach of the Aadhaar program).

Indians might be at risk of having their Aadhaar data stolen due to a massive leak of biometric and other personal data online.[113] However, the Indian government denies this report and claims that no biometric data has been breached.[114] Regardless of whether or not the data was hacked, the report should serve as a cautionary tale to governments of the risks of seeking to implement a largescale, national biometric identity program. Like the United States, India could benefit from formal legal protections for biometric identifiers, specifically because their national identification program is based on this data.

B. Other International Biometric Data Programs

The use of biometric data is increasingly common in the developing world.[115] One of the largest programs, ID4Africa, aims to collect biometric data in order to create a centralized legal identification system for people across all African nations.[116] The use of biometric data in the developing world has been effective, specifically in preventing fraud and ensuring government benefits.[117] South Africa, for example, uses biometric data to control

---

[113] AMBER SINHA & SRINIVAS KODALI, CTR. FOR INTERNET AND SOC'Y., INDIA, INFORMATION SECURITY PRACTICES OF AADHAAR (OR LACK THEREOF): A DOCUMENTATION OF PUBLIC AVAILABILITY OF AADHAAR NUMBERS WITH SENSITIVE PERSONAL FINANCIAL INFORMATION 3, https://drive.google.com/file/d/0BwsvF1X5umK4LVBmYW14UzJDdk0/view (last visited May 1, 2018).

[114] Rohith BR, *UIDAI Chief: No Breach of Data in Aadhaar Theft Case*, THE TIMES OF INDIA (Aug. 4, 2017, 12:37 AM), https://timesofindia.indiatimes.com/india/uidai-chief-no-breach-of-data-in-aadhaar-theft-case/articleshow/59906305.cms.

[115] *See Biometrics*, CTR. FOR GLOBAL DEV., https://www.cgdev.org/topics/technology/biometrics (last visited May 1, 2018).

[116] *See About the ID4Africa Movement*, ID4AFRICA, http://www.id4africa.com/
about/ (last visited May 1, 2018).

[117] *See* Xavier Giné et al., *Use of Biometric Technology in Developing Countries*, WORLD BANK RES. COMM. ET AL., http://siteresources.worldbank.org/DEC/Resources/Policy_paper-biometrics.pdf (last visited May 1, 2018).

its pension payments.[118] In Ghana, Biometric Voter Registration Kits were used to register 14 million voters in 40 days.[119] Afghanistan and Pakistan used iris and retinal scans to ensure reparation payments to refugees reentering the countries.[120] The Philippines, Spain, South Africa, and many other countries use biometric systems for national identification, similar to India's Aadhaar program.[121] Biometric identification of infants has even been used to keep track of which babies have been vaccinated in developing countries.[122] Most recently, the United Nations has used biometric identification for displaced Rohingya Muslim refugees fleeing Myanmar.[123] In November 2017, the UN completed phase one of this project, which created biometric identities for over half a million refugees, mostly women and children.[124] Although these initiatives seem to offer many benefits to developing countries, there are significant privacy issues which outweigh the positive aspects of such programs. Most notably, many of the countries using these biometric schemes have no legal framework for addressing an abuse of power within these systems, nor do they have any legal protections for citizens in the case of a breach of biometric data.[125]

---

[118] Alan Gelb, *Biometrics, Identity, and Development*, CTR. FOR GLOBAL DEV. (Oct. 14, 2010), https://www.cgdev.org/blog/biometrics-identity-and-development.

[119] *Ghana Voter Registration*, HSB IDENT., http://www.hsb.nl/our-solutions/elections/ghana-voter-registration/ (last visited May 1, 2018). These voter registration kits collect digital photos and fingerprints of voters. *Id.*

[120] Gelb, *supra* note 118.

[121] *See* Xavier Giné et al., *supra* note 117.

[122] Martin LaMonica, *Fingerprinting Infants Helps Track Vaccinations in Developing Countries*, MIT TECH. REV. (Sept. 4, 2014), https://www.technologyreview.com/s/530481/fingerprinting-infants-helps-track-vaccinations-in-developing-countries/.

[123] Chris Burt, *Biometric ID Program for Displaced Rohingya Completes First Phase*, BIOMETRIC UPDATE (Nov. 14, 2017), http://www.biometricupdate.com/201711/biometric-id-program-for-displaced-rohingya-completes-first-phase.

[124] *Id.* This biometric program was largely put in place to ensure no ISIS members were migrating into Malaysia, at the encouragement of the Malaysian government. *See id.*

[125] *Mandatory National IDs and Biometric Databases*, *supra* note 103.

One of the major issues for many developing countries who might want to deploy biometric data programs is the cost of buying the cameras and equipment needed to successfully launch a program.[126] This is largely the result of the lack of biometric programs designed specifically for developing countries, where the internet might not be reliable or even readily available for uploading the data.[127] Additionally, many privacy experts have warned that implementing biometric identification programs too quickly will violate at-risk citizens' civil liberties, as so few of these countries have data protection laws.[128] Finally, one of the largest barriers to these biometric data programs is lack of public trust, as seen with India's Aadhaar program.[129] The use of biometrics internationally should be of concern to us all, since any programs enacted abroad could lead to similar programs being enacted within the United States, unless some form of protection and regulation for this data is put in place.

III. STATES WITH BIOMETRIC DATA PRIVACY LAWS

Over the last decade, many states around the country have started to take biometric privacy into their own hands.[130] The push

---

[126] *See* Xavier Giné et al., *supra* note 117.

[127] *See* Daniel M.L. Storisteanu et al., *Can Biometrics Beat the Developing World's Challenges?*, BIOMETRIC TECH. TODAY, Nov./Dec. 2016, at 6. However, companies have started to work on solutions to this problem, such as rugged and portable laptops equipped with fingerprint scanners and digital cameras. *See, e.g.*, *Biometric Registration Kits*, HBS IDENT., http://www.hsb.nl/our-products/biometric-registration-kits/ (last visited March 1, 2018).

[128] *See* Gelb, *supra* note 118. "Only 10 countries on the [African] continent have some form of data protection law[s]". Kevin P. Donovan & Carly Nyst, *Privacy for the Other 5 Billion*, SLATE (May 17, 2013 11:51 AM), http://www.slate.com/articles/technology/future_tense/2013/05/aadhaar_and_other_developing_world_biometrics_programs_must_protect_users.html.

[129] *See* Probir Roy, *We Need a Trust Model for Aadhaar*, LIVEMINT (Aug. 21, 2017), http://www.livemint.com/Opinion/SJFc62Qio7g5UmNDHzEPxH/We-need-a-trust-model-for-Aadhaar.html; *see also* Usha Ramanathan, *Aadhaar, Rights and the State*, INDIAN EXPRESS (Oct. 8, 2015), http://indianexpress.com/article/opinion/columns/aadhaar-rights-and-the-state/.

[130] *See* Michael McGivney et al., *Illinois's Biometric Information Privacy Act Spurs Similar Legislation Around the Country*, JDSUPRA, LLC (Nov. 27,

for more statutes protecting biometric information began in 2008, when Illinois passed the first state law regulating biometric data.[131] After Illinois first brought biometric privacy to the national discourse, many other states began to consider their own statutes.[132] Although many states have taken this initiative, the federal government has not yet passed any biometrics laws.

A. Illinois BIPA Statute

In October 2008, Illinois became the first state to pass a comprehensive biometric data privacy statute, when it adopted the Illinois Biometric Information Privacy Act (BIPA).[133] Under BIPA, businesses and other organizations are prohibited from purchasing, capturing, or obtaining personal "biometric information," unless the business first:

> (1) informs the subject . . . in writing that a biometric identifier is being collected;
> (2) informs the subject . . . in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and
> (3) receives a written release executed by the subject.[134]

The BIPA statute has been referred to by many as the "archetype example of a biometric privacy law."[135] However, some have argued

---

2017), https://www.jdsupra.com/legalnews/illinois-s-biometric-information-12299/.

[131] Justin Kay & Brendan McHugh, *The Next Steps for Biometrics Legislation Across the US*, LAW360 (May 25, 2017), https://www.law360.com/articles/928056/the-next-steps-for-biometrics-legislation-across-the-us; *see* Biometric Information Privacy Act (BIPA), 740 ILCS 14/1–99 (2008).

[132] Kay & McHugh, *supra* note 131.

[133] *See id.*; BIPA, 740 ILCS 14/1–99 (2008).

[134] BIPA, 740 ILCS 14/15; Jeffrey Neuburger, *Wow! Illinois Biometric Privacy Suits Proliferate*, NAT'L LAW REV. (Sept. 27, 2017), https://www.natlawreview.com/article/wow-illinois-biometric-privacy-suits-proliferate.

[135] Jane Bambauer & James E. Rogers, *Biometric Privacy Laws: How a Little-Known Illinois Law Made Facebook Illegal*, PROGRAM ON ECON. AND

that because BIPA was passed almost ten years ago, it has become outdated with current technology.[136]

BIPA has been the basis for most litigation concerning biometric data privacy thus far, with 2017 being the first major year of case law.[137] Notably, BIPA has given Illinois residents a means by which they may pursue technology giants like Facebook over the unconsented collection of their biometric information.[138] Facebook, in turn, has hired an Illinois-based lobbying firm to work on amending state laws to be more favorable to technology companies who use people's likenesses.[139] Although BIPA is not perfect, it is arguably the best existing statute for consumers who wish to legally challenge unconsented biometric collection.

B. Texas Capture or Use of Biometric Identifier Statute

Shortly after Illinois passed BIPA, Texas became the second state to pass a law protecting citizens' biometric data in 2009.[140] The Texas statute is very similar to the Illinois BIPA statute; however, it does not allow for a private right of action.[141] Like BIPA, the law

---

PRIVACY (June 28, 2017), https://pep.gmu.edu/wp-content/uploads/sites/28/2017/06/Biometric-Privacy-Laws-FINAL_really_6.20-.pdf.

[136] *See id.* at 6, 13.

[137] *See* Carley Daye Andrews et al., *Litigation Under Illinois Biometric Information Privacy Act Highlights Biometric Data Risks*, K&L GATES (Nov. 7, 2017), http://www.klgates.com/litigation-under-illinois-biometric-information-privacy-act-highlights-biometric-data-risks-11-07-2017/; Amy Korte, *Ill. Employers Flooded with Class-Action Lawsuits Stemming from Biometric Privacy Law*, ILL. POLICY (Oct. 17, 2017), https://www.illinoispolicy.org/illinois-employers-flooded-with-class-action-lawsuits-stemming-from-biometric-privacy-law/; *see also* Meg Graham, *Illinois Biometric Lawsuits May Help Define Rules for Facebook, Google*, CHI. TRIBUNE (Jan. 7, 2017 9:00 AM), http://www.chicagotribune.com/bluesky/originals/ct-biometric-illinois-privacy-whats-next-bsi-20170113-story.html.

[138] *See* In re Facebook Biometric Info. Privacy Litig., 185 F. Supp. 3d, 1155, 1158 (N.D. Cal. 2016).

[139] *See* Bennett, *supra* note 97.

[140] *See* Kay & McHugh, *supra* note 131.

[141] Jeffrey Neuburger, *A Host of Biometric Privacy/Facial Recognition Bills Currently Circulating in State Legislatures*, PROSKAUER ROSE LLP (Feb. 23, 2017), https://newmedialaw.proskauer.com/2017/02/23/1445/; *see* TEX. PROB. CODE. ANN. § 503.001.

requires notice and consent before a company can collect users' biometric data; unlike BIPA, this does not have to include a written release.[142] However, the Texas statute is not significantly weaker than BIPA.[143] One illustration of this is the time period that each law allows for companies holding biometric data: Illinois' BIPA allows a three-year window, while Texas requires the information be destroyed within one year of its collection.[144] Additionally, although there is no private right of action, the Attorney General of Texas has the authority to recover $25,000 from companies that violate the statute.[145]

C. Washington

In 2017, Washington became the third and most recent state to enact a biometric privacy statute.[146] The Washington statue is aimed specifically at companies that collect and market biometric data without users' knowledge.[147] Washington's biometric privacy law, however, was the subject of major pushback from technology companies like Google and Facebook.[148] Again, Facebook hired in-state lobbyists to aggressively work to stop the bill in its tracks;[149]

---

[142] Michael McGivney et al., *supra* note 130; *see* TEX. PROB. CODE. ANN. § 503.001 (West 2017).

[143] *See generally* Michael McGivney et al., *supra* note 130.

[144] *Id.*

[145] TEX. PROB. CODE. ANN. § 503.001(d).; *see also* Mark Melodia et al., *Legal Risks and Rules of the Move to Biometrics*, N.Y. LAW JOURNAL, (March 2, 2015), https://www.technologylawdispatch.com/wp-content/uploads/sites/26/2016/02/Legal-NYLJ-Article-Risks-and-Rules-of-the-Move-to-Biometrics.pdf.

[146] *See* Paul Shukovsky, *Washington Biometric Privacy Law Lacks Teeth of Illinois Cousin*, BLOOMBERG LAW: PRIVACY AND DATA SEC. (July 18, 2017), https://www.bna.com/washington-biometric-privacy-n73014461920/.

[147] Ben Byer, *Washington's New Biometric Privacy Law: What Businesses Need to Know*, DAVIS WRIGHT TREMAINE LLP (July 24, 2017), http://www.dwt.com/Washingtons-New-Biometric-Privacy-Law-What-Businesses-Need-to-Know-07-24-2017/; *see* WASH REV. CODE § 40.26.020 (2017).

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

[149] Bennett, *supra* note 97.

the result was a significantly watered-down version of the Illinois statute.[150] Notably, this statute does not include digital photographs or voice audio recordings in the definition of "biometric identifier,"[151] meaning that programs like Facebook's facial tagging feature fall outside the scope of the law.[152] Similar to the Texas statute, Washington's Attorney General is the only person in the state with the authority to enforce the statute.[153] The statute also prevents private lawsuits from being filed against companies violating the law.[154] Many have argued this exception for facial data, in combination with the bar against litigation, makes the Washington law much more tech-business friendly than those biometric laws passed in Texas and Illinois.[155] The Washington biometric law serves as an example of what can happen when technology companies are willing to invest large amounts of time and money to prevent an unfavorable statute.

D. Other States with Proposed Legislation

As technology companies have become increasingly aware of the value of biometric data, they have begun to lobby in states considering biometric privacy statutes.[156] This has not altogether deterred other states from considering biometric protection legislation, but rather has blocked or weakened new bills being

---

[150] *See id.*

[151] *See* WASH REV. CODE § 40.26.020 (7)(b). Many sources define biometric data to include facial data gathered from digital photographs, as well as audio recording data. *See* Byer, *supra* note 147; *see, e.g.*, *Face Recognition*, *supra* note 16 (discussing how facial data from photographs can be used by private companies).

[152] Bennett, *supra* note 97.

[153] Byer, *supra* note 147 (noting the statute is enforced through the state Consumer Protection Act).

[154] *Id.*

[155] *Id.*; *see also* Justin Lee, *Washington's New Biometrics Law Softer on Privacy Protections than Illinois BIPA*, BIOMETRICUPDATE.COM (July 24, 2017), http://www.biometricupdate.com/201707/washingtons-new-biometrics-law-softer-on-privacy-protections-than-illinois-bipa.

[156] *See, e.g.*, Mehrotra, *supra* note 148.; *see also* Glaser, *Facebook Is Using an "NRA Approach"*, *supra* note 12.

proposed.[157] In 2015, the California legislature considered a bill that would have required businesses that collect biometrics to protect the data from misuse.[158] Although the bill passed the California state assembly, the state senate never brought the bill to a vote.[159]

In 2017, eight states[160] attempted to pass legislation protecting consumer biometric data; however, Washington was the only state that succeeded in doing so.[161] In Montana, an intellectual property attorney helped draft a biometric protection bill that was later blocked by the lobbying efforts of Facebook and Verizon.[162] The Montana bill faced particular pushback because it would have required very specific notice and consent requirements from businesses wishing to collect biometric information from their customers.[163] On the other end of the spectrum, Connecticut proposed biometric legislation that would only apply to "facial recognition [technology] used for marketing purposes," showing just how narrow newer biometric legislation may be.[164] Alaska and New Hampshire proposed bills that would have protected and

---

[157] *See* Bennett, *supra* note 97.

[158] Personal Data, AB 83, 2015-16 Reg. Sess. (Ca. 2015); Mehrotra, *supra* note 148.

[159] *Id.* Although it is unclear why the bill was never given a hearing on the state senate floor, it can be inferred from the amount spent on lobbying by tech companies that the industry pushback played a large role.

[160] *See* Bennett, *supra* note 97 (noting that Washington, Alaska, Montana, New Hampshire, Connecticut, and New York have all proposed some form of comprehensive biometric protection legislation, while Arizona and Missouri attempted to pass more narrow legislation aimed just at protecting students); *see also* Brian Nearing, *NY AG Calls for Safeguards on Biometric Data*, GOV'T TECH. (Nov. 3, 2017), http://www.govtech.com/security/NY-AG-Calls-for-Safeguards-on-Biometric-Data.html.

[161] Bennett, *supra* note 97.

[162] *Id; see also* Montana Biometric Information Privacy Act, HB 518, Reg. Sess. 2017 (Mt. 2017).

[163] *See* Mehrotra, *supra* note 148.

[164] H.B. 5522, 2017 Gen. Assemb., Reg. Sess. (Conn. 2017); *see also* Aaron K. Tantleff, *States Continue to Fill Gaps in Privacy Legislation: Illinois Biometric Law Gains Traction and Serves as Model for Other States,* FOLEY & LARDNER LLP (April 17, 2017), https://www.foley.com/states-continue-to-fill-gaps-in-privacy-legislation-illinois-biometric-law-gains-traction-and-serves-as-model-for-other-states/.

regulated biometric information, while allowing for a private right of action like BIPA; both failed.[165]

In November 2017, then-New York Attorney General Eric Schneiderman proposed the "Stop Hacks and Improve Electronic Data Security" ("SHIELD") Act, which would apply to all businesses and companies that collect biometric data from their employees.[166] The SHIELD Act would require that businesses "adopt 'reasonable' administrative, technical, and physical safeguards for sensitive data, and report breaches" of this data.[167] Additionally, the SHIELD Act would allow for penalties and potential legal action against companies who fail to safeguard this data, while offering legal liability protection for those companies that can demonstrate very strong preventative action taken to secure such data.[168] One of the more interesting aspects of the SHIELD Act is that it carves out a more "flexible" standard for small businesses without compromising data protection from bigger technology companies.[169] However, it remains unclear whether or not the SHIELD Act will become law in New York.[170]

IV. BIOMETRIC PRIVACY CASE LAW UNDER STATE STATUTES

2017 was the first year with a significant amount of cases involving biometric data privacy; more than thirty class action suits were filed in the second half of the year.[171] Most of these suits center around employers' use of employees' biometric data without their

---

[165] *See id.*; Mehrotra, *supra* note 148; *See* H.B. 523, 2017 N.H. H.R., Reg. Sess. (N.H. 2017); H.B. 72, 30th Legislature, Reg. Session (Alaska 2017).

[166] S. S6933A, 2017–2018 Reg Sess. (N.Y. 2017); Nearing, *supra* note 160.

[167] Nearing, *supra* note 160.

[168] *Id.*

[169] Kenneth K. Dort & Katherine E. Armstrong, *A.G. Schneiderman Announces SHIELD Act to Protect New Yorkers*, LEXOLOGY (Nov. 15, 2017), https://www.lexology.com/library/detail.aspx?g=7569b15d-93d5-4c80-8894-ab75f98f6861.

[170] The bill has been at the committee stage since November 2017. *See Senate Bull S6933A*, *Current Bill Status*, N.Y. STATE SENATE (Nov 1, 2017), https://www.nysenate.gov/legislation/bills/2017/s6933.

[171] Andrews et al., *supra* note 137.

knowledge or consent.[172] Many of these employees filed suits under BIPA against employers for the misuse of biometric identifiers in employee timekeeping.[173] These cases include some of America's larger employers, such as American Airlines and Hyatt Hotels.[174] These cases represent the first real wave of biometric lawsuits that have the potential to create a day-to-day impact on millions of Americans, creating a fundamental shift in the way employers treat such sensitive data.[175]

One of the more consequential suits arising from biometric privacy statutes is *In re: Facebook Biometric Information Privacy Litigation*, a class action filed under BIPA and currently being heard in the Northern District of California.[176] The case began as three separate claims in 2015, which were consolidated into one class action later that year.[177] The plaintiffs claimed they never received meaningful consent from Facebook before having their photos

---

[172] *See* Diana Novak Jones, *Employers Face Surge of Suits Under Ill. Biometrics Law*, LAW360 (Oct. 30, 2017), https://www.law360.com/articles/979243/employers-face-surge-of-suits-under-ill-biometrics-law; *see also* Lauraann Wood, *Media Co. Hit with Suit Over Scanning Workers' Fingerprints*, LAW360 (Dec. 1, 2017), https://www.law360.com/articles/989947/media-co-hit-with-suit-over-scanning-workers-fingerprints (explaining that over a dozen employment-related cases have been filed since June 2017).

[173] *See* RJ Vogt, *Bob Evans Latest to Face Suit Over Ill. Biometric Law*, LAW360 (Oct. 31, 2017), https://www.law360.com/articles/979967/bob-evans-latest-to-face-suit-over-ill-biometrics-law; *see also* Hannah Meisel, *Hotel Co. Wants Biometric Class Action Moved to Fed. Court*, LAW360 (Nov. 9, 2017), https://www.law360.com/articles/984083/hotel-co-wants-biometric-class-action-moved-to-fed-court.

[174] *See* Hannah Meisel, *United Airlines Latest to be Sued Under Ill. Biometrics Law*, LAW360 (Nov. 8 2017), https://www.law360.com/articles/983384/united-airlines-latest-to-be-sued-under-ill-biometrics-law; *see also* Rick Archer, *Hyatt Hit with Class Action Over Employee Fingerprinting*, LAW360 (Oct. 31, 2017), https://www.law360.com/articles/980166/hyatt-hit-with-class-action-over-employee-fingerprinting.

[175] *See* sources cited *supra* note 174.

[176] In re Facebook Biometric Info. Privacy Litig., No. 15-cv-03747-JD, 2017 U.S. Dist. LEXIS 139051 (N.D. Cal. Aug. 29, 2017); In re Facebook Biometric Info. Privacy Litig., 185 F. Supp. 3d 1155 (N.D. Cal. 2016); *see also* Cara Bayles, *Facebook Biometric Data Row May Hinge on "Right to Say No,"* LAW360 (Nov. 30, 2017), https://www.law360.com/articles/989879.

[177] Bayles, *supra* note 176.

included in the website's facial tagging feature.[178] Facebook claimed that the plaintiffs lacked standing because the BIPA statute did not apply to the facial tagging program.[179] However, in a November 2017 hearing, a federal judge said the case concerned "the most personal aspects of your life: your face, your fingers, who you are to the world."[180] Moving forward, the case will turn on Facebook users' "right to say no," which BIPA created for citizens of Illinois.[181] In April 2018, a federal judge granted class certification to the plaintiffs.[182] In May 2018, Facebook's motion for summary judgement was denied, and the trial was set to move forward in July 2018.[183] If Facebook loses the case, they could be forced to pay a fine of $1000 to $5000 per occurrence of a person's photo being used without permission.[184]

V. PROPOSING FEDERAL LEGISLATION

As states continue to push for more biometric data protection, a patchwork of privacy laws is taking shape.[185] Given that most technology companies operate around the country, federal legislation is an appropriate solution to biometric privacy concerns. By passing comprehensive legislation which protects biometric data from being sold without the consumer's permission and creates standards of security for this data, consumers and businesses alike will benefit. By providing businesses with a clear framework for

---

[178] *In re Facebook*, 185 F. Supp. 3d at 1159.

[179] *See id.*

[180] Joel Rosenblatt, *Facebook Judge Frowns on Bid to Toss Biometric Face Print Suit*, BLOOMBERG TECH. (Nov. 30, 2017), https://www.bloomberg.com/news/articles/2017-11-30/facebook-judge-frowns-on-bid-to-toss-biometric-face-print-suit.

[181] *Id.*; *see generally* BIPA, 740 ILCS 14/1–99 (2008).

[182] In re Facebook Biometric Info. Privacy Litig., No. 3:15-cv-03747-JD, 2018 U.S. Dist. LEXIS 63930 (N.D. Cal. Apr. 16, 2018); *see also* Rosenblatt, *supra* note 180 (explaining that the hearings thus far dealt with Facebook's first motion to dismiss for lack of standing claiming the Illinois law did not apply to them).

[183] *See* In re Facebook Biometric Info. Privacy Litig., No. 3:15-cv-03747-JD, 2018 U.S. Dist. LEXIS 81044 (N.D. Cal. May 14, 2018).

[184] *Id.*

[185] *See* Michael McGivney et al., *supra* note 130.

how to treat biometric data, they can work to ensure they are complying with the law while still being innovative. Furthermore, giving consumers a clear biometric privacy framework can help people feel more secure in their daily interactions with technology. However, it is important to understand that the road to passing federal biometric legislation will not be easy.

A. Problems with Proposing Federal Biometric Data Regulations

As technology companies have become increasingly aware of the risk of lawsuits under biometric privacy statutes, they have begun to aggressively lobby against any laws that might protect or regulate the use of biometric data.[186] Many "privacy advocates say Facebook is uniquely aggressive in opposing all forms of regulation on its technology."[187] Facebook has played a significant part in blocking many state bills which would have regulated the use of biometric data, so it is not a far reach to assume if federal biometric legislation were to be proposed the company would be among the first to aggressively oppose its implementation.[188] Some scholars have even suggested the approach taken by Facebook is similar to the lobbying approach taken by controversial groups like the NRA.[189] This may be why no federal lawmaker has introduced a bill that would comprehensively protect biometric data, even though the Government Accountability Office recommended a federal law protecting this data after the privacy concerns raised by facial recognition technologies.[190] In fact, the federal government has

---

[186] *See* Mehrotra, *supra* note 148.

[187] Bennett, *supra* note 97.

[188] Especially given the large sums of money spent by Facebook already on lobbying the federal government (currently over $8 million). *See* Chris Burt, *Facebook Lobbying Against Facial Recognition Laws*, BIOMETRIC UPDATE (Aug. 1, 2017), http://www.biometricupdate.com/201708/facebook-lobbying-against-facial-recognition-laws.

[189] *See id.*; *see also* Glaser, *Facebook Is Using an "NRA Approach"*, *supra* note 12.

[190] Jared Bennett, *Facebook: Your Face Belongs to Us*, CTR. FOR PUB. INTEGRITY (July 31, 2017), https://www.thedailybeast.com/how-facebook-fights-to-stop-laws-on-facial-recognition.

recently rolled back existing protections of personal data by allowing internet providers to sell users' data without their knowledge or consent.[191]

One of the biggest challenges to drafting federal biometric legislation could be the lack of common definition of the term "biometrics."[192] This has been an issue for many states that have proposed biometric legislation,[193] and presents a major opportunity for technology companies to shape a definition most favorable to their business models.[194] Another concern some experts have voiced is that a piece of federal legislation to protect or regulate biometric data might run afoul of the Constitution.[195] One scholar has even suggested that these laws are content-based discrimination and thus violate the First Amendment.[196] However, the scholar based these claims on the fact that companies do *not* use your biometric data in advertising or marketing[197] which is no longer the case with most private companies that collect biometric data. Furthermore, the first amendment argument against biometric legislation seems to be outweighed by the interest in maintaining privacy of consumers; however, a court is yet to rule on the constitutional issues presented by biometric data collection.

---

[191] Congress voted to roll back FCC privacy rules put in place by the Obama administration. *See* Molly Olmstead, *Congress Votes to Allow Broadband Providers to Your Data Without Your Permission,* SLATE (Mar. 28, 2017), http://www.slate.com/blogs/future_tense/2017/03/28/congress_votes_to_allow_broadband_providers_to_sell_your_data.html.

[192] *See* Byer, *supra* note 147; Rebecca Yergin, *Washington Becomes the Third State with a Biometric Law*, COVINGTON & BURLING LLP (May 31, 1010), https://www.insideprivacy.com/united-states/state-legislatures/washington-becomes-the-third-state-with-a-biometric-law/.

[193] *See* sources cited *supra* note 192.

[194] *See, e.g.*, Byer, *supra* note 147 (arguing that this has allowed industry groups to lobby when biometric bills are introduced to create a more favorable working environment by ensuring bills include only limited biometric points or do not include a private right of action).

[195] Bambauer & Rogers, *supra* note 135, at 10.

[196] *Id.* at 10–11.

[197] *Id.*

B. A Suggested Approach for Future Federal Legislation

As of 2017, 64 percent of Americans had been personally affected by a data breach.[198] In addition, many Americans feel that their personal data has become less secure in the last five years.[199] These two factors are important in considering an approaching for legislation to protect biometric data. Since many Americans already feel their data is less secure, there is likely public support for legislation to protect such sensitive data.[200] Additionally, there are many lawmakers and technology experts who have voiced concern over the lack of regulation of biometric gathering technology.[201]

Moreover, following the Equifax breach, Congress introduced the Consumer Protection Privacy Act of 2017, which requires companies to notify their users of data breaches and misuses of personal information "as expediently as possible."[202] Although this legislation protects biometric identifiers, it does *not* create a consent or notice requirement before a company can collect or use your biometrics.[203] Even more notably, this legislation would only regulate companies which collect biometric data of at least 10,000 Americans per year, a much more narrow application than the

---

[198] Kenneth Olmstead & Aaron Smith, *Americans and Cybersecurity*, PEW RES. CTR. (Jan. 26, 2017), http://www.pewinternet.org/2017/01/26/americans-and-cybersecurity/.

[199] *Id.*

[200] *See id.* Research has shown that Americans have little faith in private companies' ability to protect their sensitive personal data. *Id.*

[201] *See* Bennett, *supra* note 97. One of the inventors of facial recognition technology now says without federal regulation, citizens are left vulnerable since state laws regulating biometrics can be more easily manipulated by commercial interests. *See id.*

[202] Consumer Privacy Protection Act of 2017, H.R. 4081, 115th Cong. § 1 (2017); *see generally* Allison Grande, *Forever 21 Says Unencrypted Payment Card Data Breached*, LAW360 (Nov. 16, 2017), https://www.law360.com/articles/986152/forever-21-says-unencrypted-payment-card-data-breached (discussing the Consumer Protection Privacy Act); Consumer Privacy Protection Act of 2017, H.R. 4081, 115th Congress, (2017).

[203] *See* H.R. 4081 (requiring that covered entities notify any resident of the United States whose sensitive personally identifiable information has been, or is reasonably believed to have been, accessed or acquired following the discovery of a security breach of such information).

Illinois, or even Washington, biometric statutes.[204] Additionally, the legislation has an exception for financial institutions, healthcare providers, and electronic communications providers.[205] By creating such broad exceptions for some businesses, in combination with the very narrow application to certain smaller businesses, this legislation leaves many gaps for citizens who are concerned about their biometric privacy. Privacy advocates can delay their concern, however, since the bill has an extremely small chance of becoming law and has yet to make it out of the committee phase.[206]

While it is promising that some members of Congress have taken the initiative to propose such legislation, more and better changes are needed to our federal privacy laws. The best approach may be for concerned citizens to work with non-profits like the Electronic Frontier Foundation and the American Civil Liberties Union to lobby those Senators and Congressmen who supported the Consumer Protection Privacy Act, encouraging them to adopt a biometric protection bill that more closely resembles the Illinois BIPA statute. Although the BIPA statute was enacted in 2008,[207] it is relatively straightforward and allows for the most accountability for businesses who violate the statute. Furthermore, by lobbying for a federal statute that mirrors BIPA, the legislation would be easier for average citizens to understand than the sixty-one-page Consumer Protection Privacy Act.[208] In order to be an effective piece of biometric privacy legislation, the law should apply to a broad range of businesses, as well as a large array of biometric data gathering methods. Like BIPA, an effective piece of federal legislation would also include a private right of action to hold those companies who frequently violate people's privacy to be held accountable.

---

[204] *See* H.R. 4081, §201(b); Biometric Information Privacy Act (BIPA), 740 ILCS 14/15 (2008); WASH REV. CODE § 40.26.020 (2017).

[205] H.R. 4081, §201(c)

[206] *See H.R. 4081-115th Congress: Consumer Privacy Protection Act of 2017: Prognosis*, GOVTRACK, https://www.govtrack.us/congress/bills/115/hr4081 (last visited May 1, 2018). Some scholars have suggested the bill only has a 2% chance of passing. *See id.*

[207] BIPA, 740 ILCS 14/1–99 (2008).

[208] The Consumer Privacy Protection Act is sixty-one pages in length, whereas BIPA is much shorter and easier to understand, containing only twelve pages. *See* H.R. 4081; BIPA, 740 ILCS 14/1–99.

Moreover, by capitalizing on the lack of public trust of data security, more people could effectively be mobilized to call or write their representatives, encouraging them to adopt comprehensive federal biometric legislation. By average citizens working in unison with privacy-oriented non-profits, there is potential to change, or in some cases spark, the national conversation around biometric data collection.

CONCLUSION

Without legislation protecting our biometric data, it is not a matter of if, but rather when, this highly sensitive data will be breached.[209] As the few states who do have biometric protection laws show, litigants are willing to use these statutes to enforce their privacy and hold private companies accountable. However, passing legislation will not be an easy achievement. Developing effective biometric privacy legislation requires an understanding of the cultural, social and legal contexts of the biometric systems, otherwise failing such impacts diminishes the efficacy of the legislation and can bring serious unintended consequences.[210] On the other hand, technology companies have already demonstrated a real desire to quash any new legislation that would protect or regulate biometric data.

Moreover, to pass federal legislation would take a major public awareness campaign that effectively conveys the dangers of unregulated biometric data collection. There are many privacy and civil liberties orientated organizations who already have the capacity to take on this type of campaign. As biometric programs from private companies become increasingly commonplace, more of these organizations are likely to speak out. Since there is a pre-existing lack of public trust surrounding the security of our personal data online, it most likely would not take too much for this type of campaign to catch on. In the wake of the Equifax data breach, now

---

[209] *See* The Editors, *Biometric Security Poses Huge Privacy Risks*, SCI. AM. (Jan. 1, 2014), https://www.scientificamerican.com/article/biometric-security-poses-huge-privacy-risks/.

[210] *See generally* BIOMETRIC RECOGNITION: CHALLENGES AND OPPORTUNITIES 85–87 (Joseph N. Pato & Lynette I. Millett eds., 2010) (ebook), https://www.nap.edu/read/12720/chapter/6.

is not the time to wait for better protection of our sensitive biometric data. Rather, it is the time for citizens to push their legislators for stringent biometric protections to be codified into law.