The Data of You: Regulating Private Industry's Collection of Biometric Information

Hannah Zimmerman[*]

I. INTRODUCTION

If you use your fingerprint to unlock your mobile phone, you are not alone. The number of phones with embedded fingerprint sensors is projected to grow from 499 million in 2015 to 1.6 billion in 2020.[1] By 2019, fifty percent of smartphones are expected to integrate an embedded fingerprint sensor.[2] And fingerprints are just the beginning—automated facial recognition, hand gesture recognition, iris scanners, hand-vein scanners, and heart rhythm monitors are all vying to be "the next big thing."[3]

Many consumers view fingerprint identification as a secure way to protect the sensitive information they keep on their mobile devices.[4] To alleviate security concerns, phone companies assure consumers that their fingerprint data is not transmitted from their phones and is processed separate from the operating system.[5] However, the security risks from

---

* Associate Attorney, Forbes Law Group, LLC. I extend my sincerest thanks to Professor Mike Kautsch for his invaluable insight and suggestions. I would like to thank Professor Andrew Torrance and the Kansas Law Review Staff and Board for their thoughtful review of this Comment. I would also like to thank my friends and family for their unwavering support and patience throughout this process. Finally, I would like to thank my biggest supporter, Eric, for his constant love and encouragement as I pursue my passion in privacy law.

1. Jamie Fox, *Fingerprint Sensor Market Growth Continues Upward Trajectory*, *IHS Says*, IHS MARKIT (Jan. 25, 2016), https://technology.ihs.com/571358/fingerprint-sensor-market-growth-continues-upward-trajectory-ihs-says.

2. Jess Bolluyt, *Smartphone Fingerprint Scanners: Are They Secure?*, CHEATSHEET.COM (June 1, 2016), http://www.cheatsheet.com/gear-style/smartphone-fingerprint-scanners-are-they-secure.html/?a=viewall.

3. Samuel Gibbs, *2015: The Year the Fingerprint Sensor Stopped Being a Gimmick*, THE GUARDIAN (Dec. 27, 2015), https://www.theguardian.com/technology/2015/dec/27/2015-fingerprint-sensor-smartphone-security-biometrics-data.

4. Ken Yeung, *Paypal Survey Finds Smartphone Owners Comfortable with Fingerprint Security Despite Scares*, TNW (Oct. 9, 2013), http://thenextweb.com/insider/2013/10/09/paypal-survey-finds-smartphone-owners-comfortable-with-fingerprint-security-despite-scares/.

5. Joseph Steinberg, *Why You Should Not Use the New Smartphone Fingerprint Readers*, FORBES (Mar. 5, 2015, 4:00 PM), http://www.forbes.com/sites/josephsteinberg/2015/03/05/why-you-should-not-use-the-new-smartphone-fingerprint-readers/#103eaca41aa8.

fingerprint identification are growing with its rise in popularity. Data breaches are growing more common,[6] and during a major breach at the U.S. Office of Personnel Management in 2014, the fingerprint data of 5.6 million people was stolen.[7] Lifted fingerprints[8] or molds of users' fingerprints can fool fingerprint readers.[9] Some smartphones do not properly encrypt your fingerprint data and others do not have properly protected fingerprint sensors.[10] As the breach at the U.S. Office of Personnel Management demonstrates, when biometric information is collected and stored in a database, there is always the possibility of that information being stolen and subsequently used. As one commentator has noted: "It's easy to replace a swiped credit card, but good luck changing the patterns on your iris."[11]

Despite the popularity of biometrics and the unique issues they pose, there is no generally applicable federal law that regulates the private sector's collection and use of biometric information in the United States. Only three states have enacted statutes governing biometric information privacy.[12] The current lack of regulation is surprising given that biometric information is permanent and unique to each individual and thus creates a concern for identity theft. Additionally, consumers do not have any control over the collection of their biometric information or knowledge of what is collected and by whom.

This Comment will argue that a federal law governing biometric data privacy is necessary because biometric characteristics are increasing in popularity as a form of identification, are permanent and cannot be changed like other forms of identification, and the few state laws

---

6. *See* Joseph Cox, *Are Data Breaches Becoming More Common?*, MOTHERBOARD (July 28, 2016, 11:58 AM), https://motherboard.vice.com/en_us/article/data-breaches-vigilante-pw (describing an archive of hacks showing that "data breaches have become more frequent over the past few years").

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

8. Russell Brandom, *Your Phone's Biggest Vulnerability Is Your Fingerprint*, THE VERGE (May 2, 2016, 8:00 AM), http://www.theverge.com/2016/5/2/11540962/iphone-samsung-fingerprint-duplicate-hack-security.

9. Chandrasekhar Bhagavatula et al., *Biometric Authentication on iPhone and Android: Usability, Perceptions, and Influences on Adoption*, (Feb. 8, 2015) (unpublished, presented at Usable Security Conference 2015), http://wp.internetsociety.org/ndss/wp-content/uploads/sites/25/2017/09/01_3_3.pdf.

10. Kevin Downey, *Fingerprint Sensors: Are They Really Secure?*, KOMANDO.COM (Feb. 15, 2016), http://www.komando.com/happening-now/347464/fingerprint-sensors-are-they-really-secure/all.

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

12. *See infra* notes 88–90 and accompanying text.

implemented are inconsistent and have created uncertainty for businesses regarding compliance. Part II will explain the background of biometric technology, outline the current framework of U.S. federal and state laws related to biometric information collection, and summarize current privacy developments between the United States and the European Union. Part III will argue that a federal law that explicitly delegates enforcement power to the Federal Trade Commission will provide consistent protection for consumers and will ensure continued transatlantic commerce between the United States and the European Union. The Fair Credit Reporting Act will serve as a template for a federal biometric information privacy law. Finally, Part IV will conclude that the current privacy protections in place are insufficient and that a federal biometric information privacy statute will provide sufficient protection of consumers' biometric information.

II. BACKGROUND

The private industry's collection and use of biometric information is largely unregulated in the United States.[13] The mass collection of biometric information has expanded rapidly in the past decade, but the law has not kept up.[14] The United States has yet to pass privacy legislation that adequately protects consumers, who have little to no control over what biometric information companies collect, how they collect it, or how it is stored and used after collection.[15] This Section provides an overview of the basics of biometric technology and the current legal landscape of biometric privacy protections in the United States

A. Biometric Information: The Technology

According to a market research report by Application, Technology, Function, & Geography, "the biometrics market is expected to reach $32.73 billion by 2022."[16] Another market research report predicts the mobile biometrics market to grow at an even faster rate, reaching $49.33

13. Anne T. McKenna, *Pass Parallel Privacy Standards or Privacy Perishes*, 65 RUTGERS L. REV. 1041, 1080–81 (2013).

14. *See Biometric Security Poses Huge Privacy Risks*, *supra* note 11 ("Current law is not even remotely prepared to handle these [biometric technology] developments. The legal status of most types of biometric data is unclear.").

15. *See* McKenna, *supra* note 13, at 1081.

16. *Biometric System Market by Authentication Type (Single-Factor: (Fingerprint, IRIS, Palm Print, Face, Vein, Signature, Voice), Multi-Factor), Component (Hardware and Software), Function (Contact and Non-Contact), Application, and Region - Global Forecast to 2022*, MARKETSANDMARKETS (Nov. 2016), http://www.marketsandmarkets.com/Market-Reports/next-generation-biometric-technologies-market-697.html.

billion by 2022.[17] To understand how biometric technology has become so popular in the private industry, it is helpful to understand what biometrics are, how they work, and the benefits they provide to consumers and businesses.

To put it simply, biometrics are biological measurements.[18] The term "biometrics" refers to one or more distinguishing biological characteristic of an individual.[19] A biometric characteristic is a measureable physiological or behavioral trait that may be used to identify an individual.[20] Thus, biometric characteristics can be broken down further into two categories: physiological characteristics and behavioral characteristics.[21] Physiological characteristics are those that concern the body's composition and measurements.[22] Examples include hand geometry, fingerprints, DNA, and face, retina, iris, or ear features.[23] Behavioral characteristics concern a person's behavior.[24] Behavioral characteristics are measurable patterns such as typing rhythm, gait, and voice, which can be used to continuously identify an individual.[25]

The term "biometrics" is also used to describe a system.[26] A biometric system is the process of recognizing an individual based on a measurable physiological or behavioral characteristic.[27] Biometric systems consist of three basic components: first, a device that captures the biometric characteristic; second, "software to convert the [] scanned biometric data into a standardized digital format and to compare [relevant] match points;" and third, "[a] database to securely store biometric data for comparison."[28]

---

17. *Mobile Biometrics Market Worth 49.33 Billion USD by 2022*, MARKETSANDMARKETS, http://www.marketsandmarkets.com/PressReleases/mobile-biometric.asp (last visited Jan. 18, 2018).

18. *See Definition: Biometrics*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/biometrics (last visited Jan. 18, 2018) (defining biometrics as "the measurement and analysis of unique physical or behavioral characteristics (such as fingerprint or voice patterns) especially as a means of verifying personal identity").

19. *See* Margaret Rouse, *Definition: Biometric Verification*, SEARCHSECURITY.COM, http://searchsecurity.techtarget.com/definition/biometric-verification (last updated May 2008).

20. *FAQ – Biometrics*, 360 BIOMETRICS, http://www.360biometrics.com/faq/biometrics.php (last visited Jan. 18, 2018).

21. Margaret Rouse, *Definition: Biometrics*, SEARCHSECURITY [hereinafter Rouse, *Biometrics*], http://searchsecurity.techtarget.com/definition/biometrics (last updated Nov. 2015).

22. *Id.*

23. *FAQ – Biometrics*, *supra* note 20.

24. Rouse, *Biometrics*, *supra* note 21.

25. *Id.*

26. Salil Prabhakar et al., *Biometric Recognition: Security and Privacy Concerns*, IEEE SECURITY & PRIVACY, Mar.–Apr. 2003, at 33, 33, http://biometrics.cse.msu.edu/Publications/GeneralBiometrics/PrabhakarPankantiJain_BiometricSecurityPrivacy_SPM03.pdf.

27. *Id.* For the purpose of this Comment, "biometrics" will be discussed as the utilization of physiological or behavioral characteristics for identification.

28. Rouse, *Biometrics*, *supra* note 21.

The biometric information in the database is compiled as measurements, which are used to create an algorithm or a "template" of an individual's specific biometric characteristic, such as their fingerprint or their facial features.[29] Once an individual's characteristic is in a database, it is compared to new records.[30] Biometric authentication can then be used to either verify an individual's identity, or to identify an unknown person.[31] If the new records match the database record, then that individual's identity is confirmed:

> For example, when someone shows up at a security checkpoint claiming to be "John Doe," that person's biometrics are checked against the system which contains the biometrics of "John Doe," and the system verifies that the person is in fact that particular "John Doe." Alternatively, an unknown person's biometrics can be checked against a database to determine who that person is, such as matching a fingerprint found at a crime scene to the FBI's database.[32]

Both the government and the private industry collect vast amounts of personal data, including biometric data. Biometric data is unlike any other personal data collected about individuals; biometric characteristics are personal to each individual, permanent, and indispensable.[33] While there is a need for regulation of the collection of personal data in general, the focus of this Comment is on biometric data because of its unique nature. Similarly, while the government was an early adopter of biometric technology and continues to collect vast amounts of biometric data on individuals today, the private industry's collection and use of biometric data is almost entirely unregulated.[34]

The private industry has created an environment in which data collection is a prevalent business practice and data is used for a wide variety of purposes.[35] Its use of biometric identification quickly expanded

---

29. Carmen Aguado, Comment, *Facebook or Face Bank?*, 32 LOY. L.A. ENT. L. REV. 187, 193 (2012).

30. Rouse, *Biometrics*, *supra* note 21.

31. Erin M. Sales, Note, *The "Biometric Revolution": An Erosion of the Fifth Amendment Privilege to be Free from Self-Incrimination*, 69 U. MIAMI L. REV. 193, 213–14 (2014).

32. *Id.* at 214.

33. Natasha Kohne et al., *Unique Biometric Data Creates Unique Privacy Concerns*, N.Y.L.J. (Feb. 22, 2016), https://www.law.com/newyorklawjournal/almID/1202749996053/.

34. The government's collection of personal information is bound by the constraints of the Fourth Amendment, the Omnibus Crime Control and Safe Streets Act, the Electronic Communications Privacy Act of 1986, the Pen/Trap Statute, and the Stored Communications Act, among others. For a discussion of these governmental restraints, *see* McKenna, *supra* note 13, at 1046–50.

35. Gregory James Evans, Comment, *Regulating Data Practices: How State Laws Can Shore Up the FTC's Authority to Regulate Data Breaches, Privacy, and More*, 67 ADMIN. L. REV. 187, 195 (2015).

in recent years partially because of advancements in technology, but largely because of the advantages of biometric identification.[36] Traditional methods of identification include passwords, personal identification numbers (PIN), driver's licenses, passports, and, increasingly, social security numbers.[37] While these methods have been used for years, they have unavoidable disadvantages. For example, a password or PIN can be forgotten, a person may discover and use someone else's social security number, and a driver's license or passport can be lost or forged.[38] Alternatively, biometric identification is difficult to duplicate, cannot be lost, and does not depend on an individual to remember it because it is based on his or her "intrinsic characteristics."[39] Biometric characteristics are inherent and provide completely unique data sets that result in accurate data generation and verification.[40] It is, in fact, these intrinsic characteristics that appeal so strongly to innovators.

The advantages that biometrics provide have led to new innovations in identification technology. For example, researchers have been able to identify individuals by measuring their brainwave patterns using an electroencephalogram (EEG) headset.[41] Researchers at Binghamton University measured fifty individuals' EEG responses to certain stimuli, like food and celebrities.[42] The brain reactions were so unique that each "brainprint" was used to identify individuals with 100% accuracy.[43] In the future, brainwave patterns could be used in security systems to verify an individual's identity.[44]

---

36. *See* Scott M. Bernat, *Biometrics: Enhancing Security in the Public and Private Sectors*, ASIA PACIFIC SECURITY MAG. (Aug. 8, 2012), http://www.asiapacificsecuritymagazine.com/biometrics-enhancing-security-in-the-public-and-private-sectors/.

37. McKenna, *supra* note 13, at 1066. *See also* Elizabeth M. Walker, Note, *Biometric Boom: How the Private Sector Commodifies Human Characteristics*, 25 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 831, 842 (2015) ("Today, the Social Security number is considered the most valuable piece of information to a criminal because it is a 'skeleton key' for all accounts.").

38. McKenna, *supra* note 13, at 1066.

39. *Id.*

40. *Advantages of Biometrics*, SUPERPAGES.COM, https://www.superpages.com/em/advantages-of-biometrics/ (last visited Jan. 18, 2018).

41. Maria V. Ruiz-Blondet et al., *CEREBRE: A Novel Method for Very High Accuracy Event-Related Potential Biometric Identification*, IEEE TRANSACTIONS ON INFO. FORENSICS AND SECURITY, July 2016, at 1618–19, http://ieeexplore.ieee.org/ielx7/10206/7447855/07435286.pdf?tp=&arnumber=7435286&isnumber=7447855.

42. *Id.* at 1619.

43. *See id.* at 1618. ("Results indicate that there are multiple configurations of data collected . . . that all allow 100% identification accuracy in a pool of 50 users.").

44. *Researchers Can Identify You by Your Brain Waves with 100 Percent Accuracy*, SCIENCEDAILY (Apr. 18, 2016), https://www.sciencedaily.com/releases/2016/04/160418120608.htm.

The private industry can, and does, "surreptitiously gather, collect, store, and sell vast amounts of intimate, personal data."[45] While the fundamental technology behind the devices we use has not changed in recent years, the scope of the collection of our information has become more complex and pervasive.[46] The current privacy framework in the United States does not give individuals the power to protect their privacy by controlling the personal data gathered, collected, stored, and sold by the private industry.[47] This is increasingly problematic, because the "private industry tracks 24/7 our physical location, online travels, friends, activities, likes and dislikes, preferences (including religious and sexual), personal status (married, divorced, or single), and financial status. Such tracking is accomplished in myriad ways and, more increasingly, it is done using individuals' biometric identifiers."[48] The next section will provide an overview of the legal framework surrounding biometric information privacy in the U.S.

B. Collecting and Using Biometric Data: The Legal Landscape

Thanks to the Internet and advancements in technology, the number of individuals and businesses connected worldwide is constantly increasing.[49] As such, it is important to understand the legal landscape of biometric privacy law both in the United States and internationally. While there are no federal statutes that directly regulate the collection and use of biometric information in the private sector, some states have enacted biometric information privacy laws. Federal laws provide sector-specific protections that may overlap with collection of biometric information. Additionally, some businesses are constrained by the Privacy Shield, which is an agreement between the United States and the EU regarding additional protections that businesses must have in place to protect data privacy if they want to engage in business with the EU.

1. Federal Laws and Regulations

Though the United States is a world leader in data-driven business, current federal statutes do not comprehensively regulate the collection of

45. McKenna, *supra* note 13, at 1042.

46. Evans, *supra* note 35, at 195–96.

47. McKenna, *supra* note 13, at 1042.

48. *Id.* at 1043.

49. As of January 2018, there were roughly 3.8 billion Internet users in the world. *Internet Users*, INTERNET LIVE STATS, http://www.internetlivestats.com/internet-users/ (last visited Jan. 18, 2018).

personal data via the Internet.[50] Nor do they protect consumers from the collection of biometric data, despite requests from industry leaders for guidelines to protect individuals from the collection of their biometric data without their consent.[51] There is no generally applicable federal law regulating the private industry's collection, storage, use, purchasing and selling of biometric information.[52] Instead, federal privacy law in the United States is a patchwork of statutes that do not sufficiently protect individuals' biometric information privacy or give businesses a uniform law to follow.[53]

Instead of one general statute regulating biometric data, or even data privacy generally, much of the current privacy legislation in the United States regulates specific areas—which means that very little legislation exists that specifically regulates data privacy.[54] Unless a federal law regulating a certain industry provides restrictions on the collection and use of personal information, such as financial institutions, credit reporting agencies, and health care providers,[55] consumers have very little protection absent additional protections provided under state law. As a result, the United States has developed a sectoral approach,[56] where data privacy

---

50. *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, THE WHITE HOUSE (Feb. 23, 2012), https://obamawhitehouse.archives.gov/sites/default/files/privacy-final.pdf.

51. Aguado, *supra* note 29, at 223.

52. Nancy J. King & V.T. Raja, *What Do They Really Know About Me in the Cloud? A Comparative Law Perspective on Protecting Privacy and Security of Sensitive Consumer Data*, 50 AM. BUS. L.J. 413, 443 (2013).

53. *See* Erin Corken, *The Changing Expectation of Privacy: Keeping Up with the Millennial Generation and Looking Toward the Future*, 42 N. KY. L. REV. 287, 294 (2015) ("Over the years in the U.S. . . . a sectoral approach to privacy regulation has developed.").

54. An example of these regulated areas are "consumer protection, records management in federal agencies, telecommunications, electronic communication, healthcare, banking and financial institutions, education, audio visual material rental, sale and subscription, electronic government services, children, and drivers that typically concern provisions regarding personal information and the safeguarding of it." *Id.*

55. King & Raja, *supra* note 52, at 443–44 (citing Gramm-Leach-Bliley Act of 1999, Pub. L. No. 106-102, 113 Stat. 1338 (codified at 15 U.S.C. §§ 6801–6809 (2012)); Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, § 1173, 110 Stat. 1936, 2024–25 (codified as amended at 42 U.S.C. § 1320d-2 (2012)); Fair Credit Reporting Act of 1970, Pub. L. No. 91-508, 84 Stat. 1114 (codified at 15 U.S.C. §§ 1681–1681x (2012))).

56. One example of this sectoral approach is the Cable Communications Policy Act (CCPA). 47 U.S.C. § 551 (2012). This statute applies to cable operators and service providers and is intended to protect cable subscribers' privacy. Cable operators and service providers are required to notify subscribers of the type of personal information that is collected and its uses, gain the written consent of subscribers before collecting information that could personally identify them, and allow subscribers to access their personal data. *Id.* § 551(a)(1). The CCPA gives consumers power over their data by ensuring transparency and allowing consumers to have knowledge about their personal data and what is done with it. Consumers can prohibit or limit the disclosure of their names and addresses, and decline to consent to the disclosure of their personally identifiable information. *Id.* § 551(c)(1).

protection is limited to specific types of information in limited circumstances.[57] Various federal statutes regulate data collected from federal agency records,[58] state motor vehicle records,[59] video rental records,[60] medical records,[61] bank records,[62] consumer reporting agency records,[63] and ISP records.[64] There are very few federal statutes that regulate Internet use and electronic communications. Statutes that do regulate personal information collected via the Internet or electronic communications, such as the Children's Online Privacy Protection Act[65] or the Electronic Communications Privacy Act,[66] do not regulate the collection of biometric information. The only direct regulation of biometric information collected by private entities is a requirement in the Health Insurance Portability and Accountability Act's regulations.[67] Specifically, "[b]iometric identifiers, including finger and voice prints" must be removed from protected health information to ensure it is not "individually identifiable health information."[68]

Notably missing from these statutes is a federal statute regulating Internet websites, data brokers, or the collection of biometric information by businesses. The only biometric-related relief offered to consumers, albeit indirectly, is a possible conviction for aggravated identity theft for using their biometric information.[69] There is no statute that directly protects consumers from the collection and use of their biometric information. That being said, such a statute is certainly possible. Some of

---

Additionally, the CCPA provides a private cause of action for consumers to recover from violations of the statute. *Id.* § 551(f).

57. Joshua J. McIntyre, Comment, *Balancing Expectations of Online Privacy: Why Internet Protocol (IP) Addresses Should Be Protected as Personally Identifiable Information*, 60 DEPAUL L. REV. 895, 902 (2011).

58. 5 U.S.C. § 552a (2012).

59. 18 U.S.C. §§ 2721–2725 (2012).

60. 18 U.S.C. § 2710 (2012).

61. 42 U.S.C. § 1320d-6 (2012).

62. 15 U.S.C. §§ 6801–6809 (2012).

63. 15 U.S.C. § 1681 (2012).

64. 18 U.S.C. §§ 2510–2522, 2701–2712, 3121–3127 (2012).

65. The Children's Online Privacy Protection Act regulates websites' collection and use of children's personal information by requiring parental consent. 15 U.S.C. §§ 6501–6506 (2012).

66. The Electronic Communications Privacy Act is comprised of three acts: (1) the Wiretap Act, which regulates the interception of communications; (2) the Stored Communications Act, which regulates communications in storage and ISP subscriber records; and (3) the Pen Register Act, which regulates the use of pen register and trap and trace devices. 18 U.S.C. §§ 2510–2522, 2701–2711, 3121–3127.

67. 45 C.F.R. § 164.514 (2016).

68. *Id.* § 164.514(b)(2)(i)(P).

69. *See* 18 U.S.C.S. § 1028(d)(7)(B) (2011). *See generally* 18 U.S.C.S. § 1028A (Supp. 2017) (defining aggravated identity theft).

the same privacy concerns surrounding biometric characteristics were the impetus behind the creation of a statute that regulates genetic information.

The Genetic Information Nondiscrimination Act (GINA) was enacted in 2008 to protect individuals from discrimination based on their genetic information.[70] GINA prohibits employers from discriminating against individuals because of their genetic information with regards to health insurance and employment.[71] A large part of the drive behind the enactment of GINA was the "fears of misuse of genetic information[,]" which parallels the growing fear of the misuse of biometric information.[72] Supporters of GINA believed that scientific advancement in genetics could create a new way to discriminate against individuals.[73] Despite the fact that genes are "facially neutral markers," Congress found that some genetic conditions are associated with certain racial groups, ethnic groups, or genders and thus could be used to discriminate against or stigmatize specific groups of people.[74] Congress also found that federal law governing genetic discrimination was "incomplete in both the scope and depth of its protections."[75] While some states had enacted their own laws prohibiting genetic discrimination, Congress found that the state laws varied on "approach, application, and level of protection" and were not only confusing but also did not protect the public from discrimination.[76] These same concerns underlie the collection of biometric data.

Under Title II of GINA, employers are prohibited from using genetic information for the purpose of hiring or firing, offering promotions, determining salary, or employment privileges.[77] Essentially, it is illegal "for your employer to use family health history and genetic test results in

---

70. Genetic Information Nondiscrimination Act of 2008, Pub. L. No. 110-223, 122 Stat. 881 (codified as amended in scattered sections of Titles 29 and 42 of the United States Code). *See* Jessica L. Roberts, *The Genetic Information Nondiscrimination Act as an Antidiscrimination Law*, 86 NOTRE DAME L. REV. 597, 599 (2011) ("Ultimately, [Congress] drafted GINA as civil rights legislation, intended to outlaw a burgeoning form of discrimination. Specifically, GINA prohibits discrimination on the basis of genetic information . . . .").

71. *Genetic Information*, U.S. DEP'T HEALTH & HUM. SERVS., http://www.hhs.gov/hipaa/for-professionals/special-topics/genetic-information/index.html (last visited Jan. 20, 2018) ("Title I of GINA prohibits discrimination based on genetic information in health coverage. Title II of GINA prohibits discrimination based on genetic information in employment.").

72. LEX K. LARSON, LARSON ON EMPLOYMENT DISCRIMINATION § 172.02[2][a] (Matthew Bender ed., 2d ed. 2017).

73. Jessica L. Roberts, *Preempting Discrimination: Lessons from the Genetic Information Nondiscrimination Act*, 63 VAND. L. REV. 439, 443 (2010).

74. 42 U.S.C. 2000ff note (GINA § 2(3)) (2012).

75. *Id.* (GINA § 2(5)).

76. *Id.*

77. 42 U.S.C. 2000ff-1(a).

making decisions about your employment."[78] Additionally, employers cannot compel or purchase genetic information of an employee or an employee's family member except in a few limited circumstances.[79] Any genetic information that is possessed by an employer must be treated as a confidential employee medical record.[80] GINA also provides a private cause of action for employees for a violation dependent upon what other antidiscrimination statute covers the employee.[81]

GINA provides protection from employment-related discrimination based on genetics, but it does not provide protection for related biometric information. "Genetics" refers to the genetic makeup of an individual.[82] GINA defines genetic information as information about an individual's genetic tests, a family member's genetic tests, or "the manifestation of a disease or disorder" in a family member.[83] Information about the sex or age of an individual is specifically excluded from the definition.[84] Genetic information relates to biometric information in the sense that both can be characterized as "informatization of the body."[85] However, genetics generally involve DNA, while biometrics involve a broad scope of information ranging from fingerprints and facial recognition to hand geometry and iris recognition.[86] GINA does not protect biometric information outside the scope of genetic testing and genetic diseases or disorders. Additionally, GINA only protects consumers from discrimination in employment. Consumers generally remain unprotected from the collection of their biometric information by private industries.[87]

As GINA has shown, there is potential for federal statutes that protect

---

78. *GINA & Employment*, GENETIC INFORMATION NONDISCRIMINATION ACT, http://www.ginahelp.org/ (last visited Jan. 27, 2018).

79. 42 U.S.C. § 2000ff-1(b).

80. *Id.* § 2000ff-5(a).

81. The applicable remedies and procedures depend on whether the employee is covered by Title VII of the Civil Rights Act of 1964, the Government Employee Rights Act of 1991, the Congressional Accountability Act of 1995, chapter 5 of title 3 of the United States Code, or section 717 of the Civil Rights Act of 1964. *See generally* 42 U.S.C. § 2000ff-6(a)–(e) (remedies and enforcement for GINA violations).

82. *Definition: Genetics*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/genetics (last visited Jan. 18, 2018).

83. 42 U.S.C. § 2000ff(4)(A)(i)–(iii).

84. *Id.* § 2000ff(4)(C).

85. Irma van der Ploeg, *Genetics, Biometrics, and the Informatization of the Body*, ANN IST SUPER SANITA 2007, at 44, 44, http://www.iss.it/binary/publ/cont/STAMPA%20ANN_07_07%20VD%20Proeg.1180428381.pdf (describing "informatization of the body" as "a relatively new phenomenon in which the human body appears to be redefined as an entity made of information").

86. *See Types of Biometrics*, BIOMETRIC INST., https://www.biometricsinstitute.org/types-of-biometrics (last visited Jan. 18, 2018).

87. Roberts, *supra* note 73, at 454–57.

biometric information. Because none are currently in place, state law provides the most protection to individuals.

2. State Biometric Privacy Law

A handful of states have enacted state statutes governing biometric data collection. Connecticut, Iowa, Nebraska, North Carolina, Oregon, Wisconsin, and Wyoming have regulated the collection of biometric information by defining "personal information" in data security breach notification laws to include types of biometric data.[88] Illinois and Texas have implemented even further regulation of biometric data collection by creating statutes focusing solely on biometric data privacy.[89] Washington recently followed suit, and on May 16, 2017, House Bill 1493 was signed into law, which broadly regulates the collection, retention, and use of "biometric identifiers."[90] These comprehensive statutes provide consumers more protection because they recognize that biometric information is inherent, distinct from other types of personal information, and potential harms are not limited to data security breaches.[91] However, as discussed below, these statutes are ambiguous, conflicting, and pose significant challenges to businesses.

Illinois enacted the Biometric Information Privacy Act (BIPA) in 2008, limiting private industry's collection and use of biometric information.[92] Under BIPA, private entities are required to notify

88. Daveante Jones, Comment, *Protecting Biometric Information in Arkansas*, 69 ARK. L. REV. 117, 132 (2016) (internal quotation marks omitted) (quoting Phil Ross, *Biometrics: A Developing Regulatory Landscape for a New Era of Technology*, GENOMICS L. REP. (2014), http://www.genomicslawreport.com/index.php/2014/05/21/biometrics-a-developing-regulatory-landscape-for-a-new-era-of-technology/).

89. *Jones*, *supra* note 88, at 132.

90. Justin Kay & Brendan McHugh, *The Next Steps for Biometrics Legislation Across the US*, LAW 360 (May 25, 2017, 11:55 AM), https://www.law360.com/articles/928056/the-next-steps-for-biometrics-legislation-across-the-us.

91. Jones, *supra* note 88, at 131.

92. Biometric Information Privacy Act, SB 2400, 95th Gen. Assemb. (Ill. 2008). BIPA was enacted in reaction to the bankruptcy of Pay By Touch, a biometrics firm that supplied fingerprint scanners to Illinois retailers. When the company considered selling its database of information collected from the fingerprint scanners, the Illinois chapter of the American Civil Liberties Union drafted BIPA. *See* Scott Holland, *Class Action: Local L.A. Tan Franchisee Must Pay for Storing Client Fingerprints, Despite Similar Suit vs National Brand*, COOK COUNTYRECORD (Apr. 12, 2016), http://cookcountyrecord.com/stories/510714536-class-action-local-l-a-tan-franchisee-must-pay-for-storing-client-fingerprints-despite-similar-suit-vs-national-brand; Shubha, *Failure Story: What Happened to Pay By Touch?*, LET'S TALK PAYMENTS (Apr. 20, 2015), https://letstalkpayments.com/failure-story-what-happened-to-pay-by-touch/; Dune Lawrence, *Do You Own Your Own Fingerprints?*, BLOOMBERG BUSINESSWEEK (July 7, 2016, 6:00 AM), https://www.bloomberg.com/news/articles/2016-07-07/do-you-own-your-own-fingerprints.

individuals that their biometric information is being collected, obtain informed consent before collecting it, and destroy the information within a certain timeframe.[93] BIPA also prohibits private entities from profiting from a consumer's biometric information and requires publicly-available written policies concerning biometric data retention and destruction.[94]

In 2009, Texas enacted a statute governing biometric information, the "Capture or Use of Biometric Identifier" (CUBI).[95] Under CUBI, private entities cannot collect biometric information before giving notice and obtaining an individual's consent.[96] The statute also includes time limitations for storing and destroying biometric information.[97]

CUBI and BIPA have some similarities, but a large number of differences. Under both CUBI and BIPA, private entities can disclose an individual's biometric information to a third party[98] only if (1) the individual consents; (2) the disclosure completes a financial transaction the individual requested or authorized; (3) the disclosure is required by law; or (4) the disclosure is made in response to a warrant or subpoena.[99]

BIPA creates a private right of action against private entities that do not follow requirements for the collection and use of biometric information.[100] A prevailing party may recover $1,000 in damages per negligent violation and $5,000 per intentional or reckless violation.[101] No private right of action exists under CUBI. Instead, the statute permits the Texas Attorney General to bring a civil action and provides a penalty cap of $25,000 per violation.[102] The statutes' definitions of "biometric identifier" also differ. BIPA defines a "biometric identifier" as a "retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry" and lists materials specifically excluded from the definition.[103] Notably,

---

93. 740 ILL. COMP. STAT. ANN. 14/15 § 15 (West 2010).

94. *Id.* § 15(a), (c); *see also* A. Marcello Antonucci & John P. Morgan, *The Future Is in Our Hands: Biometric Identification as Authentication*, LAW PRACTICE TODAY (Jan. 14, 2016), http://www.lawpracticetoday.org/article/the-future-is-in-our-hands-biometric-identification-as-authentication/.

95. TEX. BUS. & COM. CODE ANN. § 503.001 (West 2009 & Supp. 2013).

96. *Id.* § 503.001(b).

97. *Id.* § 503.001(c)(3).

98. 740 ILL. COMP. STAT. ANN. 14/15 § 15(d); TEX. BUS. & COM. CODE ANN. § 503.001(c)(1).

99. Jones, *supra* note 88, at 135–36 (quoting 740 ILL. COMP. STAT. ANN. 14/15 § 15(d); TEX. BUS. & COM. CODE ANN. § 503.001(c)(1)).

100. 740 ILL. COMP. STAT. ANN. 14/20 § 20 (West 2010); *see also* Theodore F. Claypoole, *State Forays into the Regulation of Biometric Data*, LAW360 (Nov. 10, 2015, 11:12 AM), http://www.law360.com/articles/724349/state-forays-into-the-regulation-of-biometric-data.

101. 740 ILL. COMP. STAT. ANN. 14/20 § 20(1)–(2).

102. Antonucci & Morgan, *supra* note 94.

103. 740 ILL. COMP. STAT. ANN. 14/10 § 10.

physical descriptions and photographs are excluded from the definition.[104] CUBI defines a "biometric identifier" as a "retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry" but does not provide specific exclusions from the definition.[105]

The plain language of each statute illuminates potential problems posed by multiple statutes offering similar but distinct protections to consumers. First, conflicting definitions of "biometric identifier" creates risk for private entities conducting business primarily through the Internet. It is challenging for businesses to abide by various applicable state laws if they significantly differ. For example, photographs are excluded under BIPA but included under CUBI.[106] This creates ambiguity for businesses that collect information about consumers derived from photographs.

As more states implement biometric information privacy statutes in the future, the difficulty of abiding by each individual definition will increase. For example, California's proposed definition of biometric information would extend to unique biological characteristics and the data generated by measuring them, as opposed to the more limited definitions under BIPA and CUBI.[107] As a result of varying definitions, entities are at a higher risk of noncompliance and face significant penalties if found liable.

Second, entities face varying high statutory penalties and potential class actions for violations under each statute. A consolidated class action lawsuit against Facebook is illustrative of this issue. The lawsuit alleges that Facebook's Tag Suggestion feature violates BIPA because it collects and stores users' facial geometry, a biometric identifier, without their knowledge or consent.[108] Specifically, the plaintiffs argue "that they never authorized Facebook to collect their biometric information when someone 'tagged' them in a photo, which allows the software to memorize their facial features and prompt users to identify them in other images."[109]

---

104. *Id.*

105. TEX. BUS. & COM. CODE ANN. § 503.001 (West 2009 & Supp. 2013).

106. *Id.*; 740 ILL. COMP. STAT. ANN. § 14/10.

107. A proposed amendment to California's privacy statute defines "biometric information" as "data generated by automatic measurements of an individual's biological characteristics that are used . . . to authenticate an individual's identity, such as a fingerprint, voice print, eye retinas or irises, or other unique biological characteristic." Assemb. B. 83, 2015–2016 Reg. Sess. (Cal. Jan. 6, 2015) (proposed amendment to CAL. CIV. CODE § 1798.81.5(d)(3) (West 2009)).

108. Amy Korte, *Future of Privacy: Lawsuit by Illinois Residents Focuses on Facebook Facial-Recognition Technology*, ILL. POL'Y (May 26, 2016), https://www.illinoispolicy.org/the-future-of-privacy-lawsuit-by-illinois-residents-focuses-on-facebook-facial-recognition-technology/.

109. Dawn Rhodes, *California Judge: Illinois Facebook 'Tagging' Lawsuit can Proceed*, CHI. TRIBUNE (May 10, 2016, 3:28 PM), http://www.chicagotribune.com/news/local/breaking/ct-facebook-lawsuit-20160510-story.html.

Because BIPA authorizes penalties ranging from $1,000 to $5,000 per violation, this class action lawsuit could cost Facebook millions in damages if it is ultimately found liable.[110]

While class action lawsuits are not an issue under CUBI, companies are still subject to penalties of up to $25,000 per violation, which can quickly escalate to the millions.[111] Proposed statutes also threaten significant civil penalties. A proposed statute in New York would allow civil penalties for knowing and reckless violations of up to $1,000 per person, up to a maximum of $50 million.[112] The risk of exorbitant penalties and unclear standards will only increase as more states implement biometric privacy statutes. This risk will continue to escalate as more companies enter the biometric technology domain.[113]

3. The EU-U.S. Privacy Shield

The United States does not have stringent federal or state data privacy regulations, but that does not mean that businesses do not have restrictions emanating from other sources. The U.S. Chamber of Commerce has referred to the transatlantic flow of data as "the biggest advancement in trade facilitation since air travel."[114] The European Centre for International Political Economy and the U.S. Chamber of Commerce conducted a trade impact assessment of the General Data Privacy Regulation in 2013.[115] That assessment concluded that "[c]ross-border data flows and the Internet serving as a marketplace or a distribution channel have enabled more cross-border trade, competition and innovation."[116] This rapid change has affected nearly every industry.[117] While the United States conducts transatlantic Internet-related business with numerous countries, this section focuses on the exchanges between

---

110. Stephanie Grimoldby, *What Could Outcome of Facebook's Facial Recognition Lawsuit Mean for Others?*, FORBES (July 7, 2016, 6:00 AM), http://www.forbes.com/sites/legalnewsline/2016/07/07/what-could-outcome-of-facial-recognition-suit-against-facebook-mean-for-others/#1abff23b29a0.

111. TEX. BUS. & COM. CODE ANN. § 503.001(d) (West 2009 & Supp. 2013).

112. Assemb. B. 6866, 2015-2016 Reg. Sess. (N.Y. Apr. 8, 2015); S.B. 4887, 2015-2016 Reg. Sess., at § 6 (N.Y. Apr. 22, 2015).

113. Antonucci & Morgan, *supra* note 94.

114. *The Economic Importance of Getting Data Protection Right: Protecting Privacy, Transmitting Data, Moving Commerce*, EUROPEAN CENTRE FOR INT'L POLITICAL ECON. & U.S. CHAMBER OF COMMERCE 5 (Mar. 2013), https://www.uschamber.com/sites/default/files/documents/files/020508_EconomicImportance_Final_Revised_lr.pdf.

115. *Id.* at 2–3.

116. *Id.* at 5.

117. *Id.*

the European Union and the United States, which the trade impact assessment described as "the most important economic link in the world."[118]

The European Union has historically created stricter protections for the collection and use of personal data. The EU Data Protection Directive[119] was enacted in 1995 to "balance the protections for individuals' privacy with the free movement of personal data within the EU."[120] An independent advisory panel, the Article 29 Working Party (WP29), was created under the Directive to give guidance to member states on issues regarding personal data processing and the free movement of data.[121] In 2012, the WP29 adopted an opinion on developments in biometric technologies.[122] At the outset, the opinion described the privacy harms that biometric technologies can produce:

> Biometric technologies are closely linked to certain characteristics of an individual and some of them can be used to reveal sensitive data. In addition many of them allow for automated tracking, tracing or profiling of persons and as such their potential impact on the privacy and the right to data protection of individuals is high. This impact is increasing through the growing deployment of these technologies. Every individual is likely to be enrolled in one or several biometric systems.[123]

The opinion went on to provide an updated framework of guidelines on the implementation of privacy principles in biometric technologies.[124] Biometric data is subject to the Directive framework, and cannot be processed unless a legal basis exists and the processing is "adequate, relevant and not excessive in relation to the purposes for which they are collected."[125] Additionally, under the Directive, individuals must know that their biometric information is being collected and used.[126] Individuals must be adequately informed about the type of data collected, the purposes

---

118. *Id.* at 6.

119. Council Directive 95/46, 1995 O.J. (L 281) 31 (EC), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.

120. Jayne Rothman, *Transatlantic Compliance Today*, NEW. L.J., Sept. 15, 2016, https://www.newlawjournal.co.uk/content/transatlantic-compliance-today.

121. *See Article 29 Working Party*, EUROPEAN COMM'N, http://ec.europa.eu/justice/data-protection/article-29/index_en.htm (last visited Jan. 28, 2018).

122. *See generally Opinion 3/2012 of Article 29 Data Protection Working Party on "Developments in Biometric Technologies"* (Apr. 27, 2012), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf.

123. *Id.* at 3.

124. *Id.*

125. *Id.* at 7.

126. *Id.* at 14.

of its collection, who the data is disclosed to, and their right to access, correct, or remove their data.[127] The opinion also emphasized security as a primary concern when collecting and using biometric data, and thus recommended "a high level of technical protection for the processing of biometric data, using the latest technical possibilities."[128]

Article 25(1) of the Data Protection Directive states that "the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of [the] Directive, the third country in question ensures an adequate level of protection."[129] Because of the United States' patchwork and self-regulating privacy structure, it was found to provide inadequate data privacy protection and EU companies were prohibited from transferring personal data to the United States.[130]

To bridge the vastly different legal approaches, the U.S.-EU Safe Harbor Privacy Principles were formulated.[131] The United States and the European Union developed the Safe Harbor Principles to serve as a self-regulatory framework that would allow transatlantic data transfers while ensuring the requirements of EU data protection law was met.[132] Essentially, U.S. businesses could opt into a set of data protection safeguards and certify compliance with the Principles.[133] However, in 2015 the European Court of Justice held that the Safe Harbor Privacy Principles did not adequately protect data transferred to the U.S. and declared the Principles invalid.[134]

Expedited negotiations led to an agreement on a new data privacy framework: the EU-U.S. Privacy Shield. Under the Privacy Shield, U.S. companies must commit to stringent obligations on "how personal data is processed and individual rights are guaranteed" and must publish their commitment.[135] The United States committed to limiting access of public

---

127. *Id.*

128. *Id.* at 28.

129. Council Directive 95/46, *supra* note 119.

130. Steven C. Bennett, *EU Privacy Shield: Practical Implications for U.S. Litigation*, THE PRAC. LAW., Apr. 2016, at 60, 61, http://files.ali-cle.org/thumbs/datastorage/lacidoirep/articles/TPL1604-Bennett_thumb.pdf.

131. *Id.* at 61.

132. Eduardo Ustaran, *The Privacy Shield Explained - Part 1*, PRIVACY & DATA PROT. J., April/May 2016, at 3, 3.

133. Bennett, *supra* note 130, at 61.

134. CHARLENE BROWNLESS & BLAZE D. WALESKI, PRIVACY LAW § 5.04 (2017).

135. European Commission Press Release IP/16/216, EU Commission and United States Agree on New Framework for Transatlantic Data Flows: EU-US Privacy Shield (Feb. 2, 2016), http://europa.eu/rapid/press-release_IP-16-216_en.pdf. By publishing their commitments, the

authorities to data and excluding personal data transferred to the United States from "indiscriminate mass surveillance."[136] Additionally, the European Commission and the U.S. Department of Commerce will conduct an annual joint review of the agreement.[137] Finally, the agreement provides various redress avenues for EU citizens who believe their data has been misused by U.S. entities.[138] Five months after the agreement was reached, the European Union officially adopted the Privacy Shield, "finding it to be adequate with respect to the processing of personal data from EU member states . . . to the US."[139]

The Privacy Shield will be popular among U.S. data importers.[140] Businesses who wish to join the Privacy Shield will be required to register and self-certify to the Department of Commerce and publicly commit to comply with the Privacy Shield.[141] Once a company registers and self-certifies, their commitment is "enforceable under US law and will remain enforceable regarding any personal data processed during the self-certification period, even if a company is no longer a participating company."[142] To encourage U.S. businesses to certify early, the Privacy Shield gave a nine-month grace period to businesses that certified within two months of the August 1, 2016 effective date.[143] During this grace period, businesses had time to "bring their existing contracts with onward transfer recipients" into compliance with the new framework.[144] Companies that waited to certify "must have all of their shield-related onward transfer agreements in place on the date of certification."[145]

While the self-certification process ensures that U.S. businesses can continue transatlantic business with the European Union, the process itself is not simple. To assist businesses considering joining the Privacy Shield, the Department of Commerce issued a guide to self-certification.[146] The

---

commitments are enforceable by the FTC under U.S. law. *Id.*

136. *Id*.

137. *Id*.

138. *Id*.

139. Rothman, *supra* note 120.

140. Lisa J. Sotto & Christopher D. Hydak, *The EU-US Privacy Shield: A How-To Guide*, LAW360 (July 19, 2016, 2:53 PM), https://www.law360.com/articles/815932/the-eu-us-privacy-shield-a-how-to-guide.

141. Rothman, *supra* note 120.

142. *Id.*

143. Sotto & Hydak, *supra* note 140.

144. *Id.*

145. *Id.*

146. *How to Join Privacy Shield: Guide to Self-Certification*, COMMERCE.GOV (July 12, 2016), https://www.commerce.gov/sites/commerce.gov/files/media/files/2016/how_to_join_privacy_shield_sc_cmts.pdf.

guide instructs businesses to (1) confirm eligibility to participate in the Privacy Shield, (2) develop a Privacy Shield compliant privacy policy, (3) provide a free complaint investigation mechanism, (4) ensure that a verification mechanism is in place to verify compliance with the framework, and (5) provide contract information for any issues that may arise under the Privacy Shield.[147] The guide seems relatively simple, however, companies "need to be undertaking privacy impact assessments to analyze what personally identifiable information is collected, used, processed and shared, understand and appropriately remediate compliance gaps, and make intelligent risk-related decisions with the next two- to three-year horizon in mind."[148]

The Privacy Shield is a step in the right direction for the United States. However, its protections are not directly intended for U.S. citizens.[149] The purpose of the agreement was to establish adequate safeguards in the United States so that data transfers to the European Union provide equivalent data protection standards as in the EU.[150] While the U.S. government is willing to work to establish data protections for other countries' citizens, it has lagged in providing those same protections to Americans. The next section outlines a framework that would provide adequate privacy protection to Americans while maintaining the high standards necessary for commerce between the United States and the European Union.

III. ANALYSIS

Biometric information creates unique problems for consumers and is not adequately regulated in the United States. To address these problems, a federal biometric information privacy statute should be enacted to provide consumers with adequate protection and to grant regulatory power to the Federal Trade Commission (FTC). As discussed below, this statute should be modeled on the Fair Credit Reporting Act and should broadly apply to the private industry's collection and use of biometric information.

A. The Problems

The advantages of biometric identification have become more

147. *Id.*

148. Rothman, *supra* note 120.

149. European Commission Press Release IP/16/433, Restoring Trust in Transatlantic Data Flows Through Strong Safeguards: European Commission Presents EU-U.S. Privacy Shield (Feb. 29, 2016), http://europa.eu/rapid/press-release_IP-16-433_en.pdf.

150. *Id.*

apparent as the technological boom and rise of the internet has allowed retailers to track and gather vast amounts of data on individuals. Without even resorting to biometric information, almost any retailer can buy or learn information regarding:

> Your age, whether you are married and have kids, which part of town you live in, how long it takes you to drive to the store, your estimated salary, whether you've moved recently, what credit cards you carry in your wallet and what Web sites you visit. Target can buy data about your ethnicity, job history, the magazines you read, if you've ever declared bankruptcy or got divorced, the year you bought (or lost) your house, where you went to college, what kinds of topics you talk about online, whether you prefer certain brands of coffee, paper towels, cereal or applesauce, your political leanings, reading habits, charitable giving and the number of cars you own.[151]

In addition to the information retailers can learn through online tracking and purchasing information from databases, companies employ various other methods to gather information about their customers. For example, many retailers use Wi-Fi signals from smart phones to track customers who visit their stores, using their movements to learn about specific individuals' behavior.[152] All of this information, including any biometric information collected by a company, is stored somewhere on a database and is generally retained according to company policies.[153]

1. Harms to Consumers

This constant tracking and collection of information poses a myriad of potential harms to consumers. Companies that collect and store aggregations of consumer data are at risk for security breaches where personal information is accessed by hackers.[154] As technology continues to evolve, a trend of increased cyber security breaches has emerged.[155] In 2014, a data breach of government databases at the U.S. Office of Personnel Management led to the theft of an estimated 22 million people's

151. McKenna, *supra* note 13, at 1066.

152. *Id.* at 1069.

153. Walker, *supra* note 37, at 858–60.

154. *See* Andre R. Jaglom, *Internet Distribution, E-Commerce and Other Computer Related Issues: Current Developments in Liability On-Line, Business Methods Patents and Software Distribution, Licensing and Copyright Protection Questions*, AM. L. INST. 2014, at 80, http://www.thsh.com/documents/Internet-Distribution-E-Commerce-and-Computer-Issues-2014.pdf ("The FTC itself acknowledges that breaches can happen." (internal quotation marks omitted)).

155. *Id.*

personal data.[156] The breach was historically damaging because of details contained in the stolen files,[157] including roughly 5.6 million people's fingerprints.[158] More recently, the Philippines' Commission on Elections was subject to hackers who accessed a database of 55 million voters in the Philippines.[159] Described as the largest government-related data breach in history,[160] the leaked information included "228,605 email addresses; 1.3 million passport numbers and expiry dates of overseas Filipino voters; and 15.8 million fingerprint records."[161] Adding insult to injury, a website was subsequently created that allowed users to search through the leaked information, including names, birth dates, addresses, height and weight, passport details, and fingerprint records.[162]

In these examples, individuals' actual fingerprints were not stolen, but that does not reduce the potential harms that may follow. The stored fingerprint information was likely authentication codes or templates that data from the individual fingerprints were converted into.[163] Once stolen, this information can be sold to a third party or used to recreate the fingerprint.[164] As more biometric authentication systems are implemented in the private industry, there are more opportunities for hackers to use stolen biometric information to bypass or fool supposedly secure authentication systems.[165] Stolen biometric information can be subsequently used for identity theft. For example, in response to the U.S.

---

156. Tom Iacuzio, *Accessing Safety in the Age of Biometrics*, THE EMBRY-RIDDLE NEWSROOM (Oct. 11, 2016, 5:01 PM), http://news.erau.edu/headlines/accessing-safety-in-the-age-of-biometrics/.

157. *Id.*

158. Peterson, *supra* note 7.

159. Stephen Mayhew, *Fingerprint and Passport Data Leaked in Philippines Voter Database Breach*, BIOMETRICUPDATE.COM (Apr. 7, 2016), http://www.biometricupdate.com/201604/fingerprint-and-passport-data-leaked-in-philippines-voter-database-breach.

160. Janvic Mateo, *Hackers Release Info on Philippine Voters Online*, PHIL. STAR, http://www.philstar.com/headlines/2016/04/22/1575585/hackers-release-info-philippine-voters-online (last updated Apr. 22, 2016, 12:00 AM).

161. James Temperton, *The Philippines Election Hack is 'Freaking Huge'*, WIRED (Apr. 14, 2016), http://www.wired.co.uk/article/philippines-data-breach-fingerprint-data.

162. Mateo, *supra* note 160.

163. Anna Myers, *Can the U.S. Legal System Adapt to Biometric Technology?*, IAPP: PRIVACY TECH (Aug. 12, 2016), https://iapp.org/news/a/can-the-u-s-legal-system-can-adapt-to-biometric-technology/.

164. Marc Goodman, *You Can't Replace Your Fingerprints*, SLATE (Feb. 24, 2015, 10:05 AM), http://www.slate.com/articles/technology/future_tense/2015/02/future_crimes_excerpt_how_hackers_can_steal_fingerprints_and_more.html ("To demonstrate this threat, Tsutomu Matsumoto, a security researcher at Yokohama National University, has devised a method allowing him to 'take a photograph of a latent fingerprint (on a wineglass, for example)' and re-create it in molded gelatin. The technique is good enough to fool biometric scanners 80 percent of the time. Hackers have also used everyday child's Play-Doh to create fingerprint molds good enough to fool 90 percent of fingerprint readers.").

165. *See id.* (estimating that thirty percent of businesses will use biometric identification by 2016).

Office of Personnel Management hack, an intra-agency group was tasked with investigating the potential for payment fraud and fake identity creation using stolen fingerprints.[166]

Stolen biometric information poses unique problems for consumers. A victim of identity theft can get a new credit card, change their passwords and pin numbers, or even change their Social Security number.[167] A victim of identity theft whose fingerprint data is stolen cannot change their fingerprints or get new ones.[168] Biometric information is permanently associated with a user and once stolen, it is out of the user's control forever.[169] A similarly unique problem is the fact that biometric information is inherently not a secret. It is common practice for consumers to keep their bank pin numbers a secret, but most people do not regularly wipe fingerprints they leave behind.[170] Hackers have already used high-resolution photos and fingerprints left on iPhone screens and other surfaces to circumvent fingerprint authentication technologies.[171]

This problem is not unique to fingerprints. A study conducted at Carnegie Mellon University used webcams and facial recognition technology to identify individuals on campus by linking the information gathered to photographs on Facebook.[172] About thirty-one percent of the students were identified in less than three seconds.[173] The researchers were also able to infer students' interests and Social Security numbers by combining face recognition with data mining algorithms and statistical re-identification techniques.[174]

Not only do consumers face potential breaches of their personal information, but they also have little to no say in what information is collected about them. Under our current federal privacy framework,

166. Jeremy Bergsman, *Biometrics Are Less Secure than Passwords – This Is Why*, BETANEWS (Aug. 24, 2016), https://betanews.com/2016/08/24/unsafe-biometrics/.

167. *Frequently Asked Questions - Can I Change My Social Security Number?*, SOC. SECURITY ADMIN., https://faq.ssa.gov/link/portal/34011/34019/Article/3789/Can-I-change-my-Social-Security-number (last visited Jan. 20, 2018).

168. Goodman, *supra* note 164.

169. Claire Gartland, *Biometrics Are a Grave Threat to Privacy*, N.Y. TIMES (July 5, 2016, 3:21 AM), https://www.nytimes.com/roomfordebate/2016/07/05/biometrics-and-banking/biometrics-are-a-grave-threat-to-privacy.

170. *See* Myers, *supra* note 163.

171. Bergsman, *supra* note 166.

172. *See generally* Alessandro Acquisti et al., *Face Recognition and Privacy in the Age of Augmented Reality*, J. PRIVACY AND CONFIDENTIALITY, no. 2, 2014, at 1, 4–14, http://repository.cmu.edu/cgi/viewcontent.cgi?article=1122&context=jpc.

173. *Id.* at 9; *See also* Declan McCullagh, *Face-Matching with Facebook Profiles: How it Was Done*, CNET (Aug. 4, 2011, 7:40 PM), https://www.cnet.com/news/face-matching-with-facebook-profiles-how-it-was-done/.

174. Acquisiti et al., *supra* note 172, at 10.

individuals do not have the explicit right to learn what information is collected and stored about them, who holds their personal information, or the methods that are used by entities collecting their personal information.[175] This issue became readily apparent when Facebook released its "Tag Suggestions" feature in 2011.[176] At first glance, the feature was simply a user-friendly tool that provided tagging suggestions for individuals in photos uploaded to the website.[177] However, Facebook would not have been able to launch a tool that automatically identified millions of individuals unless it had been operating some form of facial recognition biometric software without the knowledge or consent of its users.[178] The implementation of the "Tag Suggestions" feature was possible because of the lack of regulation of biometric information collection, and it is still operational because of the difficulty consumers face when attempting to sue Facebook without generally applicable biometric information privacy laws.[179]

Many types of facial recognition biometric software can identify individuals from a distance without their knowledge or consent.[180] Facial recognition technology can be used in closed-circuit television, which can record the exact location of individuals.[181] Facial recognition can also connect photos to Facebook or other social media profiles.[182] The Department of Homeland Security is developing a Biometric Optical Surveillance System that provides face-in-a-crowd detection.[183] Additionally, systems such as Face First allow retailers to identify the people entering their stores to assess whether they are likely to shoplift or whether they are "good customers."[184]

---

175. *See* McKenna, *supra* note 13, at 1075–77 (discussing the risks posed to consumers because of lack of control over the collection of personal information and the lack of understanding of how it is collected and used).

176. Charles Arthur, *Facebook in New Privacy Row Over Facial Recognition Feature*, GUARDIAN (June 8, 2011, 3:14 AM), https://www.theguardian.com/technology/2011/jun/08/facebook-privacy-facial-recognition.

177. *See id.*

178. McKenna, *supra* note 13, at 1067.

179. *See* Aguado, *supra* note 29, at 217–19 (discussing the difficulty of defining damages when suing Facebook under current privacy law).

180. Paul Ohm, *Sensitive Information*, 88 S. CAL. L. REV. 1125, 1143 (2015).

181. *Id.*

182. Paul Ohm, *The Future of Digital Evidence Searches and Seizures: The Fourth Amendment in a World Without Privacy*, 81 MISS. L.J. 1309, 1317 (2012).

183. *Biometric Security Poses Huge Privacy Risks*, *supra* note 11.

184. Adam Schwartz, *The Danger of Corporate Facial Recognition Tech*, ELECTRONIC FRONTIER FOUND. DEEPLINKS BLOG (June 7, 2016), https://www.eff.org/deeplinks/2016/06/danger-corporate-facial-recognition-tech.

An additional harm the collection of biometric information poses is the destruction of "intellectual privacy."[185] The term describes "our compelling interest in keeping our reading, viewing, and listening activities to ourselves—and the complimentary danger that exposure of these individual choices will constrain the freedom to explore and experiment with ideas and art."[186] Essentially, the risk is the "creation of a fishbowl society where a norm of disclosure forces all of us to act as if we are being watched at all times."[187] Alan Westin eloquently explained this harm in his book *Privacy and Freedom*:

> [One] state of privacy, anonymity, occurs when the individual is in public places or performing public acts but still seeks, and finds, freedom from identification and surveillance. He may be riding a subway, attending a ball game, or walking the streets; he is among people and knows that he is being observed; but unless he is a well-known celebrity, he does not expect to be personally identified and held to the full rules of behavior and role that would operate if he were known to those observing him. In this state the individual is able to merge into the "situational landscape." Knowledge or fear that one is under systematic observation in public places destroys the sense of relaxation and freedom that men seek in open spaces and public arenas.[188]

Businesses already track consumers' every move online for advertising and behavioral analysis purposes.[189] Biometric technologies would allow them to track us in the real world.[190] By incorporating facial recognition technology in closed-circuit TV systems, companies will possess the capability to instantly identify "individuals walking down the street or into a store."[191] Coupled with the pervasive collection of data via online activity and in-store interactions,[192] individuals' privacy will suffer. The potential harms that consumers face, in addition to the ever-evolving technological landscape, create a need for generally applicable legislation to regulate the collection of biometric data.

---

185. William McGeverant, *The Law of Friction*, 2013 U. CHI. LEGAL F. 15, 44 (2013).

186. *Id.*

187. *Id.* at 46.

188. ALAN F. WESTIN, PRIVACY AND FREEDOM 31 (1967); *see also* DANIEL J. SOLOVE ET AL., PRIVACY, INFORMATION, AND TECHNOLOGY 37 (2006).

189. Gartland, *supra* note 169.

190. *Id.*

191. *Id.*

192. *See* McKenna, *supra* note 13, at 1066–69.

2. Lack of Oversight and Regulation

The FTC has recognized the fact that the growing popularity of data collection in private industries has created increased privacy and data security concerns for consumers.[193] The FTC is perhaps the most equipped to handle the unique concerns that the collection of biometric information creates, as it has undertaken the role of enforcing privacy and data security.[194] Private industry's collection and use of biometric information would logically fall within the scope of the FTC's general data privacy enforcement. However, its current power to regulate is too limited to adequately protect consumers.[195]

The FTC's authority to regulate general data privacy arises out of Section 5 of the FTC Act, which prohibits "[u]nfair or deceptive acts or practices in or affecting commerce."[196] The FTC views the Act as a "'broad consumer protection mandate' that Congress intended to allow the Commission to respond to the 'unanticipated, unenumerated threats' consumers face in the marketplace."[197] Even if the FTC's power to regulate unfair or deceptive practices is broad, the question of whether the FTC's authority extends to regulating private industry's collection of biometric information is unclear absent clearly granted statutory authority.

The FTC lacks binding judicial precedent to support its authority to regulate the collection of biometric information. The most significant case, *Federal Trade Commission v. Wyndham*, established that data security was within the FTC's authority.[198] However, that decision was limited in scope and accompanied by many critics.[199] In *Wyndham*, the FTC alleged that a hotel chain failed to "maintain reasonable and

193. In 2015, the FTC held a workshop to explore consumer privacy and security issues related to the "Internet of Things," or the "ability of everyday objects to connect to the Internet and to send and receive data." FTC STAFF REPORT, INTERNET OF THINGS – PRIVACY AND SECURITY IN A CONNECTED WORLD 10 (2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

194. Aguado, *supra* note 29, at 227.

195. Rebecca Lipman, *Online Privacy and the Invisible Market for Our Data*, 120 PENN. ST. L. REV. 777, 789–90 (2016) (discussing the limited oversight the FTC can provide under 15 U.S.C. § 45(a)(1) (2012)).

196. 15 U.S.C. § 45(a)(1).

197. Evans, *supra* note 35, at 201 (citing Plaintiff's Response in Opposition to the Motion to Dismiss by Defendant Wyndham Hotels & Resorts LLC at 2, FTC v. Wyndham Worldwide Corp., No. 2:13-CV-01887-ES-SCM (D.N.J. June 17, 2013)).

198. 10 F. Supp. 3d 602, 612 (D.N.J. 2014), *aff'd*, 799 F.3d 236 (3d Cir. 2015).

199. Evans, *supra* note 35, at 189 ("Industry commentators were quick to point out that the district court's ruling on FTC's authority is far from the type of unambiguous authority necessary to keep up with the speed of the changing electronic landscape.").

appropriate data security for consumers' sensitive personal information," allowing hackers to access the consumers' information.[200] Ultimately, the court determined that "the contour of an unfairness claim in the data-security context, like any other, is necessarily 'flexible' such that the FTC can apply Section 5 [of the FTC Act] 'to the facts of particular cases arising out of unprecedented situations.'"[201] However, this ruling is far from the unambiguous authority necessary to regulate biometric information.

One potential avenue for the FTC to regulate the collection of biometric information is through consent orders. Current FTC enforcement of data privacy is largely reliant upon consent orders regarding data security practices.[202] The consent orders generally contain an agreement between the FTC and a business that the business will "institute more robust data security procedures and make long-term commitments to third party security assessments."[203] Because the consent orders are "private actions negotiated between the alleged violators and the FTC," they can be used as fair notice that other companies should implement similar practices.[204] Additionally, the FTC has announced that "in the absence of clear statements to the contrary, a company's online privacy policy would be considered to apply equally to a company's offline collection and use of data."[205] However, this route to regulating biometric information is unlikely to be successful. Outside of BIPA's requirement that businesses publish policies relating to their collection and use of biometric information,[206] companies have little incentive to include biometric-specific language in their online privacy policies.

Arguments against the FTC's regulation of data privacy practices posit that the FTC's unfair practices authority does not encompass data security and that the matter is better suited for the legislature, which can weigh the "costs and benefits of cybersecurity policy."[207] However, biometric information collection poses risks that are much higher than general information and data security risks. Biometric characteristics are irreplaceable and perhaps most importantly, "they are, by their nature,

---

200. *Wyndham*, 10 F. Supp. 3d at 607.

201. *Id.* at 620.

202. *See, e.g.*, Mauricio F. Paez, *Lessons from in re* HTC America Inc.*: FTC's Broadening Approach to Consumer Data Security Leaves Unwary Manufacturer or Developer with More than it Bargained for*, JONES DAY (Mar. 2013), http://www.jonesday.com/lessons_from_htc_america/.

203. Evans, *supra* note 35, at 202.

204. *Id.*

205. Jaglom, *supra* note 154, at 73.

206. 740 ILL. COMP. STAT. ANN. § 14/5 (West 2010).

207. Evans, *supra* note 35, at 203.

identifying information."[208] And the FTC is well equipped with knowledge and expertise regarding data collection practices:

> [T]he FTC sums the problem up well: "Consumers face a landscape of virtually ubiquitous collection of their data." And the FTC makes an important point to consider when legislating to protect consumer data: "Whether such collection occurs online or offline does not alter the consumer's privacy interest in his or her data." In the FTC's report and in other industry and privacy advocate reports, there are similarly proposed privacy protection measures. While some suggestions are specific as to a particular type of web or mobile applications or technology, the proposals all include instituting "privacy by design," which entails: data security measures, reasonable retention and storage practices, clear notice and transparency, simplified choices, and accountability.[209]

The FTC has limited power to regulate private industry's collection and use of biometric information. Absent explicitly-granted Congressional power, the FTC is not currently capable of providing adequate protection to consumers. However, given explicit regulatory authority via legislation, the FTC is well equipped to protect consumers from violations of their privacy from developing technologies.

B. Addressing the Problems of Biometric Data

As discussed above, the United States does not adequately protect consumers from the collection and use of their biometric information. As biometric technologies become more popular in the private industry, potential harms to consumers become more apparent, such as the risk of hackers stealing information from databases and the lack of consumer power and access to information regarding what data companies are collecting about them and how they use that data. Current state laws governing biometric information are conflicting, and there is no general federal law to protect consumers.

Additionally, the Privacy Shield may protect transatlantic commerce for the foreseeable future, but its strength and ability to survive judicial scrutiny is questionable. Digital Rights Ireland, an Irish civil liberties group, has already brought a complaint against the Privacy Shield in the Court of Justice of the European Union's lower court.[210] The challenge

---

208. Walker, *supra* note 37, at 843.

209. McKenna, *supra* note 13, at 1081 (citations omitted).

210. Glyn Moody, *Privacy Shield Legal Spat Puts EU-US Data Flows at Risk Again*, ARS TECHNICA (Oct. 27, 2016, 7:34 AM), http://arstechnica.co.uk/tech-policy/2016/10/privacy-shield-

seeks "to annul the framework" for allegedly inadequate privacy protections.[211] If the challenge succeeds and the Privacy Shield is annulled, hundreds of companies will again be unsure of their ability to continue to conduct data transfers between the United States and the European Union.[212] However, if the United States provided more robust privacy protections through legislation, challenges such as this would not affect U.S. business interactions with the European Union, at least so far as biometric data transfers are concerned.

These issues can be resolved with legislative action. Congress should use the Fair Credit Reporting Act (FCRA)[213] as a template to craft adequate biometric privacy laws. The FTC has experience with data protection initiatives and has actively advocated for further protections to be afforded to consumers. The FTC should thus be delegated the power to enforce the biometric privacy law and to promulgate rules to further protect consumers.

1. The Fair Credit Reporting Act as a Template

Protection for consumers' biometric information will only be as strong as the laws or regulations that are put in place to govern the private industry's collection and storage of this sensitive information. It is fitting that the database industry's roots originate from consumer reporting agencies, which are regulated by one of the most comprehensive consumer privacy laws in the United States — the Fair Credit Reporting Act.[214] This section will outline the essential provisions of the FCRA and explain how it can be used as a template for a potential biometric information privacy law.

Credit reporting agencies have existed since roughly 1899, but controversy surrounding the industry came to a head in the 1960s.[215] Multiple questionable practices existed in the industry, ranging from the collection of "lifestyle information" such as sexual orientation and drinking habits to the fabrication of negative information in order to fill

---

legal-challenge-eu-us-data-flows/.

211. *Id.*

212. *Id.*

213. 15 U.S.C. § 1681 (2012).

214. *See* Daniel J. Solove & Chris Jay Hoofnagle, *A Model Regime of Privacy Protection*, 2006 U. ILL. L. REV. 357, 359 (2006) ("The database industry has its roots in the rise of consumer reporting agencies . . . .").

215. Retail Credit Co., the first major credit reporting agency, was founded in 1899. *The Fair Credit Reporting Act (FCRA) and the Privacy of Your Credit Report*, ELECTRONIC PRIVACY INFO. CTR., https://epic.org/privacy/fcra/ (last visited Jan. 28, 2018).

quotas of negative information on consumers.[216] Consumers did not have the right to see what was in their files and were unable to correct inaccurate information in their credit reports.[217] This in turn had a direct impact on multiple aspects of consumers' lives, from their ability to purchase a home to their ability to find employment.[218] In response to the public outcry caused by these practices, Congress enacted the FCRA in 1970.[219]

The FCRA regulates consumer reporting agencies and affords consumers privacy rights in consumer reports. A "consumer reporting agency" is defined as any person who "regularly engages . . . in the practice of assembling or evaluating consumer credit information . . . for the purpose of furnishing consumer reports to third parties . . . ."[220] A "consumer report" is defined by the Act as any "communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness . . . credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living" for the purpose of determining eligibility for credit, insurance, employment, or other authorized purposes under § 1681b.[221] Authorized purposes listed in § 1681b include:

> (1) in response to a court order or grand jury subpoena; (2) to the person to whom the report pertains; (3) to a "person which [the agency] has reason to believe" intends to use the information in connection with (a) the extension of credit to a consumer, (b) employment purposes, (c) insurance underwriting, (d) licensing or the conferral of government benefits, (e) assessment of credit risks associated with an existing credit obligation or (f) a "legitimate business need" when engaging in "a business transaction involving the consumer"; (4) to establish a person's capacity to pay child support; (5) to an agency administering a state plan for use to set initial or modified child support award; or (6) to the FDIC or National Credit Union Administration.[222]

The FCRA is worded to be broadly applicable. If an entity collects information for the purposes listed in § 1681b to provide to others, then that entity becomes a consumer reporting agency.[223] Entities that are not

---

216. *Id.*

217. *Id.*

218. *Consumer Protection Law*, JUSTIA, https://www.justia.com/consumer/consumer-protection-law/ (last visited Jan. 28, 2018).

219. 15 U.S.C. § 1681 (2012).

220. *Id.* § 1681a(f).

221. *Id.* § 1681a(d)(1).

222. DANIEL J. SOLOVE & PAUL M. SCHWARTZ, PRIVACY LAW FUNDAMENTALS 154–55 (2015) (citing 15 U.S.C. § 1681b(a) (2012)).

223. *Id.* at 154.

considered traditional consumer reporting agencies can thus be subject to the FCRA. An example of this broad reach is the settlement reached between Spokeo and the Federal Trade Commission in 2012 for Spokeo's alleged violations of the FCRA.[224] Spokeo is a data broker that "collects personal information about consumers," "create[s] detailed personal profiles," and then sells the profiles to companies.[225] The FTC alleged that Spokeo marketed these profiles as a tool for employment screening, encouraging recruiters to "Explore Beyond the Resume."[226] Because Spokeo marketed the profiles to companies in the human resources and recruiting industries, it was operating as a consumer reporting agency and could thus be held liable for failing to ensure that the profiles were accurate and used for legal purposes, and for failing to tell companies about their obligations under the FCRA.[227]

Spokeo ultimately settled the claim with the FTC, but this case serves an example of the FCRA's malleable scope. Similarly, a biometric information privacy statute should turn on the purposes of companies' collection and use of biometric information. Instead of applying the statute to a specific industry, such as online businesses or data brokers, a biometric information privacy statute should be worded to apply broadly to any entity that collects and uses biometric information.[228] Additionally, the definition of biometric information should be broad enough to encompass all potential forms of biometric information, instead of following BIPA's example and excluding certain types of biometric information such as physical descriptions and photographs.[229]

The FCRA also provides safeguards to ensure the accuracy of consumer reports. Specifically, a consumer reporting agency is required to "follow reasonable procedures to assure maximum possible accuracy of the information concerning the individual about whom the [consumer] report relates."[230] Consumers have the ability to dispute the completeness or accuracy of the information in the report, and the agency must

224. Press Release, Fed. Trade Comm'n, Spokeo to Pay $800,000 to Settle FTC Charges Company Allegedly Marketed Information to Employers and Recruiters in Violation of FCRA (June 12, 2012), https://www.ftc.gov/news-events/press-releases/2012/06/spokeo-pay-800000-settle-ftc-charges-company-allegedly-marketed.

225. *Id.*

226. *Id.*

227. *See generally* Complaint, United States v. Spokeo, Inc., Civ. No. 12-05001 (C.D. Cal. June 12, 2012), https://www.ftc.gov/sites/default/files/documents/cases/2012/06/120612spokeocmpt.pdf.

228. This will avoid the issue of patchwork federal legislation outlined in Part II.B.1.

229. *See supra* notes 103–04 and accompanying text.

230. 15 U.S.C. § 1681e(b) (2012).

reinvestigate and fix any errors found, free of charge.[231] If the dispute is not resolved, the consumer can file a statement about the dispute that must be provided with and specifically noted in subsequent consumer reports by the agency.[232]

Upon a consumer's request, consumer reporting agencies are required to disclose, among other things, "[a]ll information in the consumer's file at the time of the request, except . . . any information concerning credit scores or any other risk scores or predictors relating to the consumer" as well as the source of the information and a list of each entity who obtained a consumer report.[233] If an end-user of a consumer report takes an adverse action regarding a consumer, then the user must provide notice to the consumer and provide information for the consumer to contact the consumer reporting agency that prepared the report.[234] Consumers can thus gain knowledge of the information that is collected about them. A provision such as this is vital to a biometric information privacy statute because consumers are generally unaware of the information that is collected about them by private industries.[235]

The FCRA also has multiple provisions to protect consumers from identity theft and fraud. When a consumer alerts one consumer reporting agency of potential fraud, that agency must notify the other consumer reporting agencies.[236] Victims of identity theft can require creditors to disclose information about the fraudulent transactions completed in the individual's name.[237] Identity theft victims can block the reporting of information related to the identity theft.[238] An identity theft provision in a biometric information privacy statute should also provide extensive protections for consumers. Because biometric information is inherent to individuals and cannot be changed, identity theft is a primary concern that must be addressed in the statute.[239]

Finally, the FCRA provides a private cause of actions for consumers. An entity who "willfully fails to comply with any requirement" of the FCRA is liable to the consumer for actual damages or damages between $100 and $1,000, as well as punitive damages and attorneys' fees and

231. *Id.* § 1681i(a)(1).
232. *Id.* § 1681i(b)–(c).
233. *Id.* § 1681g(a)(1).
234. *Id.* § 1681m(a).
235. *See* discussion *supra* Part III.A.1.
236. 15 U.S.C. § 1681c-1(a).
237. *Id.* § 1681g(e)(1).
238. *Id*. § 1681c-2.
239. *See supra* notes 162–73 and accompanying text.

costs.[240] Negligent failure to comply with any requirement of the FCRA results in liability to the consumer for actual damages as well as attorneys' fees and costs.[241] The FTC also has the power to enforce the FCRA.[242]

2. The Result

The problems that biometric information pose to consumers and the lack of protection currently available mirror the concerns that led to the enactment of GINA. Just as with GINA, the current federal law governing the collection and use of biometric information is incomplete and does not provide substantive protections to consumers.[243] State laws such as BIPA and CUBI vary on the approach taken to regulating biometric information and the level of protection they provide.[244] The state laws differing definitions of biometric information may be confusing to companies that conduct business online, and do not protect the general public from the myriad of potential harms that the collection of biometric information will inevitably pose.[245]

The biometric privacy legislation that this Comment proposes is based on the FCRA. By using the FCRA's basic provisions as a template for a new law regulating the private industry's collection and use of biometric data, a biometric privacy framework can be crafted that will provide adequate protections to U.S. consumers. Additionally, by delegating enforcement of the biometric privacy framework to the FTC, the FTC will be able to expand upon its ability to regulate data privacy issues.

The biometric privacy statute (BPS) should initially set out a broad definition of biometrics. By using a technology-neutral definition and instead focusing on the type of data that is collected by biometric technologies, the framework will provide a flexible standard that can be applied to new and evolving technologies developed in the future.[246] The BPS should also use a broad term to cover potential collectors and users of biometric information, such as "biometric data collectors." This will ensure that the framework does not apply to a single industry, such as cable

240. 15 U.S.C. § 1681n(a).

241. *Id.* § 1681o.

242. *Id.* § 1681s(a)(1).

243. *See supra* notes 71–76 and accompanying text.

244. *See* discussion *supra* Part II.B.2.

245. *Id*.

246. *See* Michael Birnhack, *Reverse Engineering Informational Privacy Law*, 15 YALE J. L. & TECH. 24, 36–37 (2012) (discussing justifications for technology-neutral legislation and explaining that the goal is to "speak in broader terms that can encompass more than one technology and . . . cover future technologies that are not yet known at the time of legislation").

records or medical records.[247] Instead, it will apply to any entity that collects biometric information, much like the FCRA applied to Spokeo even though it was not considered a traditional consumer reporting agency.

The BPS should also set out specific authorized purposes that the collected information can be used for. This will provide consumers with the knowledge of how their biometric information is used. Procedures concerning maximum accuracy and safety of biometric information databases[248] should be included, as well as provisions ensuring transparency. These requirements can be modeled on BIPA. Like BIPA, the BPS should prohibit companies from profiting from an individual's biometric information and should require companies to publish privacy policies concerning biometric information collection, retention, and deletion.[249]

Additionally, the BPS should require mandatory disclosures to consumers upon request and mandatory notice to a consumer if his or her biometric information is used to take an adverse action. Consumers should also be provided with the ability to dispute the accuracy of biometric information kept about them, opt-out of collection of biometrics, and remove their biometrics from a database. The option for complete removal of biometric information does not parallel any provision of the FCRA, however, the sensitive nature of biometric information must be protected.[250] It is individual to each consumer, and as such consumers should have the option to protect themselves by completely removing their biometric information from databases.[251]

Identity theft and fraud provisions like those in the FCRA will be beneficial not only to consumers, but also to businesses. Identity theft and fraud pose even greater risks to consumers' biometric information because of its uniqueness and permanence.[252] Once a fingerprint is stolen, it cannot be changed like a password or a pin number. The BPS should thus require biometric data collectors to disclose any breaches in security to consumers and to any other relevant entities. Additionally, the BPS should require biometric data collectors to develop a plan for action after a security

247. *See* discussion *supra* Part III.B.1.

248. The technical aspects of secure databases are outside the scope of this Comment, however, it is imperative that security is included because of the unique identity theft issues that biometric information leads to. *See* discussion *supra* Part III.A.1.

249. *See supra* notes 92–94 and accompanying text.

250. *See* discussion *supra* Part III.A.1.

251. *See id*.

252. *See id*.

breach and mandate security diagnostics procedures so that biometric data collectors will catch the security holes and ensure they are fixed.

The BPS should preempt all state laws. This will establish a single, generally applicable law governing the collection and use of biometric information in the United States. As previously discussed, BIPA and CUBI do not take the same approach to regulating biometric information and provide differing levels of protection.[253] By preempting these and future state laws governing biometric information, the BPS will eradicate confusion caused by multiple laws and will provide businesses with consistent regulations.[254]

Finally, the BPS should provide a private cause of action for consumers and also delegate enforcement power to the FTC. Consumers will thus be able to procure damages for breaches of the BPS, while the FTC will regulate biometric data collection practices as a whole. The FTC will no longer have to rely on consent orders as the principal method to regulate privacy and security issues.[255] In fact, the FTC will be able to better implement the plans that FTC Chairwoman Edith Ramirez outlined in her keynote address at the Technology Policy Institute Aspen Forum in August 2016.[256] In her speech, Ramirez outlined three ways the FTC intends to empower consumers and ensure they have control over personal data.[257] First, the FTC will "continue its research and policymaking efforts to . . . keep pace with innovation."[258] Second, the FTC will use its "authority to make sure companies are protecting consumer privacy and safeguarding consumer data."[259] And third, the FTC will foster innovation and incentivize companies to develop new privacy tools.[260]

Combining the FTC's enforcement power with a general biometric privacy framework will ensure that companies are transparent about their data practices, improve consumers' ability to manage the information that is collected about them, and safeguard biometric databases from potential breaches in security. The framework will fit seamlessly into the United States' sectoral privacy laws but will afford broader protection to

253. *See supra* text accompanying notes 98–105.

254. This mirrors Congress's conclusions when enacting GINA. *See* discussion *supra* Part II.B.1.

255. *See supra* notes 202–05 and accompanying text.

256. *See generally* Edith Ramirez, Chairwoman, Fed. Trade Comm'n, Keynote Address at the Technology Policy Institute Aspen Forum: Protecting Consumer Privacy in the Digital Age: Reaffirming the Role of Consumer Control (Aug. 22, 2016), https://www.ftc.gov/system/files/documents/public_statements/980623/ramirez_-_protecting_consumer_privacy_in_digital_age_aspen_8-22-16.pdf.

257. *See generally id.*

258. *Id.* at 10.

259. *Id.* at 11.

260. *Id.* at 12.

consumers by providing a flexible standard that will cover any entity that collects and uses biometric information.

IV. CONCLUSION

The United States does not adequately protect consumers from the collection and use of their biometric information. Biometric information is unlike other personal information because it is unique to each individual and cannot be changed or altered. As biometric technologies become more popular in the private industry, the need for regulation has grown. Biometric information collection puts consumers at risk to identity thefts and hackers. Stolen biometric information has the potential to damage consumers in ways that normal identity thefts do not because of the unique nature of biometric characteristics. The current federal framework provides almost no protection for consumers' biometric information. While state statutes such as BIPA provide some protection, that protection does not necessarily extend to out of state consumers and can lead to vast class actions and a wide range of potential damages and causes of action. Additionally, the United States' current privacy regime does not afford adequate privacy protections to EU citizens. While the Privacy Shield will protect transatlantic commerce between the United States and the European Union for the foreseeable future, its strength and ability to survive judicial scrutiny is questionable.

These issues can be resolved with legislative action that implements the biometric privacy statute outlined above. The FCRA can be used as a template to craft adequate biometric privacy laws. The FTC should be given the power to enforce the framework because it has experience with data protection initiatives and has actively advocated for further protections to be afforded to consumers. The biometric privacy framework will provide sufficient privacy protections to consumers, allow them to better understand biometric data collection practices, and ensure they will not remain in the dark about the information that companies have collected regarding their biometric characteristics.