Boston College Law Review

Volume 60 | Issue 1 Article 8

1-29-2019

Big Data Discrimination: Maintaining Protection of Individual Privacy Without Disincentivizing Businesses' Use of Biometric Data to Enhance Security

Lauren Stewart
Boston College Law School, lauren.stewart@bc.edu

Recommended Citation
Lauren Stewart, *Big Data Discrimination: Maintaining Protection of Individual Privacy Without Disincentivizing Businesses' Use of Biometric Data to Enhance Security*, 60 B.C.L. Rev. 347 (2019), https://lawdigitalcommons.bc.edu/bclr/vol60/iss1/8

BIG DATA DISCRIMINATION: MAINTAINING PROTECTION OF INDIVIDUAL PRIVACY WITHOUT DISINCENTIVIZING BUSINESSES' USE OF BIOMETRIC DATA TO ENHANCE SECURITY

Abstract: Biometric identification technology is playing an increasingly significant role in the lives of consumers in the United States today. Despite the benefits of increased data security and ease of consumer access to businesses' services, lack of widespread biometric data regulation creates the potential for commercial misuse. Of particular concern is the use of biometric data by businesses, such as those within the data broker industry, to enable opaque discrimination against consumers. Although some states, such as Illinois, Texas, and Washington, have adopted comprehensive biometric data regulation statutes, the statutes do not offer a consistent approach. This Note argues that Congress should consider enacting a comprehensive statute. The industry-specific approach to privacy regulation of federal law, however, may leave regulation up to the states. Therefore, as more states look to regulate businesses' collection and use of biometric data, they should enact statutes that seek to balance protecting consumers' biometric data from discriminatory use and businesses' use of biometric data to enhance security and provide improved products and services.

INTRODUCTION

In 2017, Stanford University researchers published a study detailing the creation of a facial recognition algorithm that was able to predict an individual's sexual orientation with startling accuracy.[1] The researchers took 35,000 photographs of self-identified homosexual and heterosexual individuals from public dating websites.[2] The algorithm was designed to make the assumption that hereditary and personal grooming features, such as weight, hairstyle, and facial expressions, were proxies for sexual orientation.[3] The study was criti-

[1] *See* Heather Murphy, *The 'Gaydar Machine' Causes an Uproar*, N.Y. TIMES, Oct. 9, 2017, at D1 (detailing the method and results of a study that correctly predicted sexual orientation based upon a single photograph of an individual at a rate of 71% for females and 81% for males).

[2] *See id.* (noting that the images used in the study were taken from online dating profiles and were only images of white individuals).

[3] *See id.* (stating that the study's researchers, Dr. Kosinski and Mr. Wang, created the algorithm to correlate genetic facial features and an individual's personal "grooming choices" to be used as proxies, or substitutes for sexual orientation).

cized for the creation of a tool that collected data to categorize individuals based on sexual orientation and therefore had the potential to be used to exclude or discriminate against entire classes of individuals.[4]

Beyond concerns of potential discriminatory practices associated with the algorithm in the Stanford study, there is a growing fear of more widespread discrimination which could result from businesses' manipulation of biometric identification data.[5] In the past decade, businesses have implemented biometric identification technology to both ease consumer access to businesses' services and for use in security and fraud prevention measures.[6] Although there are currently no reports of businesses actually using an algorithm like the one created at Stanford, businesses routinely collect data sufficient to run such an algorithm through their use of biometric identification technology.[7] Despite this increase in collection of individuals' biometric data, there is no comprehensive regulation of businesses' collection, use, and disclosure of biometric data in the United States.[8]

[4] *See id.* (reporting critics' fears that sexual-determination technology could be used to discriminate); *see also* Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CALIF. L. REV. 671, 677 (2016) (affirming data mining's potential to segregate individuals within historically protected classes through automated processes); Frederik Zuiderveen Borgesius et al., *Open Data, Privacy, and Fair Information Principles: Towards a Balancing Framework*, 30 BERKELEY TECH. L.J. 2073, 2091–93 (2015) (analogizing data brokers' collection and use of consumer data to the surveillance industry's practice of "social sorting" because both create potentially detrimental categorizations of individual data).

[5] *See* Eduard Goodman, *Biometrics Won't Solve Our Data-Security Crisis*, HARV. BUS. REV. (Dec. 6, 2017), https://hbr.org/2017/12/biometrics-wont-solve-our-data-security-crisis [https://perma.cc/76C7-WVBQ] (noting that biometric technology can collect personal information such as race, gender, age, economic class, or health conditions, and thus it could be used to engage in discriminatory social sorting by segregating individuals through automated processes).

[6] *See* Xavier Larduinat, *3 Ways Biometric Technology Will Change the Face of Financial Services*, GEMALTO BLOG (Jan. 2, 2018), https://blog.gemalto.com/financial-services/2018/01/02/3-ways-biometric-technology-will-change-face-financial-services/ [https://perma.cc/45MV-WJ47] (attributing the increase in biometric technology to the dual benefits of increased security measures and ease of consumer access to businesses' services and products); Robinson Meyer, *Who Owns Your Face?*, THE ATLANTIC (July 2, 2015), https://www.theatlantic.com/technology/archive/2015/07/how-good-facial-recognition-technology-government-regulation/397289/ [https://perma.cc/TH9N-92DP] (stating that businesses such as Facebook, Microsoft, and Google have begun researching and implementing biometric technology).

[7] *See* Larduinat, *supra* note 6 (listing the increased use of biometrics such as fingerprint, facial, and voice recognition, iris scanning, and selfies as authentication measures for consumers); Press Release, *The Future Is Here: iPhone X*, APPLE: NEWSROOM (Sept. 12, 2017), https://www.apple.com/newsroom/2017/09/the-future-is-here-iphone-x/ [https://perma.cc/25CA-N6NZ] [hereinafter *Apple Press Release*] (detailing the method of Face ID to superimpose 30,000 infrared dots on an individual's face to create and digitally store a template of the user's face on the user's device and not on a cloud-based server to ensure optimal security).

[8] *See* Ted Claypoole & Cameron Stoll, *Developing Laws Address Flourishing Commercial Use of Biometric Information*, BUS. L. TODAY, May 2016, at 1, 4 (noting that the United States employs an industry-specific approach to privacy regulation, with several industry-specific laws that regulate

One of the largest collectors of individuals' data is the modern day data broker industry.[9] The modern day data broker industry exists to collect consumer data, aggregate and analyze that information, and then sell it to third parties, often for marketing purposes.[10] Data brokers collect and purchase consumer data from publicly accessible sources such as social media and government records, and from private sources such as commercial entities including other data brokers.[11] After collecting consumer information, data brokers aggregate that information into segments or marketable categories, often through automated predictive analysis tools.[12] A study published by the Federal Trade Commission (FTC) found a number of these categories to be harmful to consumers and potentially discriminatory.[13] For example, the FTC uncovered categories targeting consumers' race and income levels such as "Urban Scramble" and "Mobile Mixers" which targeted low income Latinos and African Americans.[14] Data brokers often assign marketing "scores" to these categories and sell that information to employers and businesses such as loan companies.[15] Discrimination can occur when individuals in low scoring categories are specifically targeted for exposure to advertisements for subprime credit and lower levels of service from those businesses or employers.[16] To prevent potential

private and public collection and use of an individual's biometric identification data within various sectors).

[9] *See* FED. TRADE COMM'N (FTC), FTC DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY 46–47 (2014) [hereinafter FTC DATA BROKERS], https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf [https://perma.cc/7W59-QGWQ] (stating that one data broker collected information on "1.4 billion consumer transactions and over 700 billion aggregated data elements" and another broker collected "3000 data segments for nearly every U.S. consumer").

[10] *See id.* at 3 (describing the business of the data broker industry); *Data Brokers and "People Search" Sites*, PRIVACY RIGHTS CLEARINGHOUSE (Oct. 17, 2017), http://www.privacyrights.org/content/data-brokers-and-your-privacy [https://perma.cc/JE7P-67HD] (defining the term data broker and differentiating between data brokers based upon the type of information sold to third parties).

[11] *See* FTC DATA BROKERS, *supra* note 9, at 11–14 (listing the sources from which data brokers obtain consumer information).

[12] *See id.* at 19–20 (describing the process data brokers use to categorize consumer data).

[13] *See id.* at 20 (noting that the different categorizations created the potential for discrimination by differentiating between consumers based on a variety of factors such as race, age, educational level, net worth, and specific health conditions); *see also* Barocas & Selbst, *supra* note 4, at 673–75 (noting that discrimination can occur through both intentional and inadvertent means within algorithms that use proxies that align with certain classes of people); Borgesius, *supra* note 4, at 2091–93 (noting that predictive algorithms can categorize individuals in a discriminatory manner).

[14] *See* FTC DATA BROKERS, *supra* note 9, at 20, 47 (listing different marketable categories created with consumers' data, that ranged from seemingly harmless to overtly harmful).

[15] *See* BRUCE SCHNEIER, DATA AND GOLIATH: THE HIDDEN BATTLES TO COLLECT YOUR DATA AND CONTROL YOUR WORLD 62 (2015) (describing how data brokers such as Acxiom sort individuals into categories that are then sold to businesses, employers, or other entities); FTC DATA BROKERS, *supra* note 9, at 31 (describing the system of attributing marketing scores to consumer data).

[16] *See* FTC DATA BROKERS, *supra* note 9, at 48 (stating that consumers assigned a low marketing score are unable to correct any false data attributed to that score and therefore are limited to marketing targeted to that score range).

commercial misuse, states are beginning to implement statutes that regulate businesses' collection, use, and disclosure or sale of biometric data.[17] The state statutes, however, offer conflicting definitions and standards of regulation.[18]

This Note examines the developing regulation of biometric data in commercial industries.[19] Part I of this Note discusses businesses' increased use of biometric technology in security tools, the discrimination caused by the modern data broker industry, and regulation of biometric data in the current federal privacy landscape.[20] Part II of this Note discusses the rise of state implementation of statutes that regulate businesses' interaction with biometric data.[21] Part III of this Note argues that as more states look to adopt biometric data laws, there must be some balance to the scope of regulation.[22] Specifically, there must be consideration of both protecting individual consumers' biometric data from discriminatory use and businesses' interest in the use of biometric data to enhance security.[23] Furthermore, this Note argues that either the states should implement biometric data statutes or Congress should implement comprehensive federal regulation similar to that in Washington state, which imposes a "commercial purpose" limitation on the scope of regulation.[24]

I. BIOMETRIC IDENTIFICATION IN A BIG DATA WORLD

In the past decade, businesses have implemented cutting edge biometric identification technology into every facet of society, including financial services, daycares, retailers, advertising, and social media.[25] A primary applica-

[17] *See* Sharon Roberg-Perez, *The Future Is Now: Biometric Information and Data Privacy*, 31 ANTITRUST 60, 61–63 (2017) (listing the three states that have biometric data regulation statutes and the additional states that have been in talks, have pending legislation, or have introduced bills regarding regulation of businesses' collection and use of biometric data).

[18] *See generally* Lara Tumeh, *Washington's New Biometric Privacy Statute and How It Compares to Illinois and Texas Law*, BLOOMBERG L.: PRIVACY L. WATCH, Oct. 16, 2017, at 1, 1–3, https://www.jdsupra.com/legalnews/washington-s-new-biometric-privacy-70894/ [https://perma.cc/GM4D-EJL6] (listing the differences in notice, consent, sale, and enforcement requirements among the three state statutes).

[19] *See infra* notes 25–251 and accompanying text.

[20] *See infra* notes 25–131 and accompanying text.

[21] *See infra* notes 132–203 and accompanying text.

[22] *See infra* notes 204–251 and accompanying text.

[23] *See infra* notes 204–251 and accompanying text.

[24] *See infra* notes 246–251 and accompanying text.

[25] *See* Claypoole & Stoll, *supra* note 8, at 1 (noting that it is common practice for banks to use voiceprint as a security measure in calls to customer service centers); Roberg-Perez, *supra* note 17, at 60 (defining biometrics as measurements of a person's physical being using either physiological or behavioral characteristics); Kathy Lohr, *Fingerprint Scans Create Unease for Poor Parents*, NPR: ALL THINGS CONSIDERED (Nov. 20, 2012), https://www.npr.org/2012/11/20/165225794/fingerprint-scans-create-unease-for-poor-parents [https://perma.cc/2K3C-ZJA9] (detailing the use of fingerprint identification in Mississippi for parents receiving state subsidized child care to ensure authentication); Meyer, *supra* note 6 (stating that businesses such as Facebook and the retail industry have begun researching and implementing biometric technology).

tion has been the collection and use of individuals' biometric data in security and fraud prevention tools, enabling more accurate authentication of individuals.[26] The United States, however, does not have a single, comprehensive federal law regulating businesses' collection and use of biometric data.[27] Without regulation, businesses are free to disclose an individual's biometric data to third parties, such as data brokers.[28] Data brokers can aggregate biometric data with both personally identifiable information ("PII") and non-PII to categorize individuals, which could lead to commercial misuse in the form of opaque discrimination, through use of biased models where consumers lack the ability to view and correct false or misleading information.[29]

This Part describes the current landscape created by the convergence of businesses' increased use of biometric technology with the unregulated data broker industry.[30] Section A of this Part discusses the rise of biometric data technology and its increased use in businesses' security and fraud prevention measures.[31] Section B discusses the modern day data broker industry's use of

[26] *See* Claypoole & Stoll, *supra* note 8, at 1 (describing the uses of biometric identification to authenticate consumers); Tim De Chant, *The Boring and Exciting World of Biometrics*, PBS NOVANEXT (June 18, 2013), https://www.pbs.org/wgbh/nova/next/tech/biometrics-and-the-future-of-identification/ [https://perma.cc/4DRP-8H2C] (noting that a significant rise in biometric technology occurred after the United States government invested vast amounts of money into biometric research and development in response to 9/11).

[27] *See* Claypoole & Stoll, *supra* note 8, at 4 (noting that federal privacy laws in the United States are tailored to specific industries).

[28] *See* FTC DATA BROKERS, *supra* note 9, at 13–14 (reporting that consumers' private information is purchased by data brokers from commercial entities such as retailers and financial services companies); *see also Data Brokers and "People Search" Sites*, *supra* note 10 (stating that data brokers' collection and use of consumer data is narrowly regulated and does not allow consumers to see the data collected about them or to correct any inaccuracies).

[29] *See* FTC DATA BROKERS, *supra* note 9, at 11–14, 20 (listing different types of marketable categories created through analysis and use of consumers' data collected from both public and private sources); *see also* Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814, 1828–31 (2011) (noting that United States federal law does not provide a single, universal definition of personally identifiable information ("PII") but rather defines PII in various ways such as any information that identifies a person, any nonpublic personal information, non-aggregate data, and specific types of data defined as PII by operation of statute). Information such as an individual's first and last name, address, telephone number, email address, and social security number are typically defined to be PII by statute, whereas non-PII is information that cannot be used on its own to identify a single person. Schwartz & Solove, *supra* note 29, at 1831–32, 1836–37; Michael Brennan, *Can Computers Be Racist? Big Data, Inequality, and Discrimination*, FORD FOUND.: EQUALS CHANGE BLOG (Nov. 18, 2015), https://www.fordfoundation.org/ideas/equals-change-blog/posts/can-computers-be-racist-big-data-inequality-and-discrimination/ [https://perma.cc/9EEA-FGZE] (stating that a major risk of using large data sets for predictive analysis is that its implementation is not free from biases).

[30] *See infra* notes 34–131 and accompanying text.

[31] *See infra* notes 34–58 and accompanying text.

"big data" and its effect on discrimination.[32] Section C of this Part discusses the use of biometric data in the traditional federal privacy landscape.[33]

A. Use of Biometric Identification Data to Enhance Security

The year 2017 saw some of the largest, most advanced, and most publicly reported data breaches in history.[34] The WannaCry attack affected over 300,000 computers globally.[35] The breach of Deep Root Analytics, a media firm working for the Republican National Committee, compromised data on 198 million American voters.[36] Spotlighted by the media, the breach of Equifax, a prominent consumer credit reporting entity, exposed data on 143 million Americans.[37] Businesses faced with the continuous threat of cyberattacks are often ill-equipped to adequately protect their consumers' PII.[38] Since 2005, over 8,000 data breaches have been publicly reported, compromising an estimated 10 billion records.[39] According to Privacy Rights Clearinghouse, in the year 2017

[32] *See infra* notes 59–97 and accompanying text.

[33] *See infra* notes 98–131 and accompanying text.

[34] *See The World's Biggest Data Breaches*, GEMALTO (Oct. 20, 2017), https://www.gemalto.com/review/Pages/The-world's-biggest-data-breaches.aspx [https://perma.cc/UE8S-BD2R] (reporting that in the first half of 2017 there were "918 reported data breaches worldwide and almost 1.9 billion compromised data records worldwide").

[35] *See* Bill Chappell, *WannaCry Ransomware: What We Know Monday*, NPR: THE TWO-WAY (May 15, 2017), https://www.npr.org/sections/thetwo-way/2017/05/15/528451534/wannacry-ransomware-what-we-know-monday,causing%20major%20disruptions%20worldwide [https://perma.cc/5QAY-2N6C] (describing WannaCry as a ransomware attack that disabled infiltrated computers by demanding ransom payments in the cryptocurrency Bitcoin).

[36] *See* Katie Reilly, *Nearly 200 Million U.S. Voters' Personal Data Accidentally Leaked by Data Firm Contracted by RNC*, FORTUNE (June 20, 2017), http://fortune.com/2017/06/19/deep-root-analytics-voter-data-exposed/ [https://perma.cc/5KYG-SKRP] (noting that the exposed data included home addresses, dates of birth, phone numbers, and voters opinions on political issues).

[37] *See* Seena Gressin, *The Equifax Data Breach: What to Do*, FTC: CONSUMER INFO. (Sept. 8, 2017), https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do [https://perma.cc/6LA5-ZDEU] (stating that the breach exposed individuals' names, home addresses, Social Security numbers, dates of birth, driver's license numbers, and credit card numbers).

[38] *See* PONEMON INST., 2017 STATE OF CYBERSECURITY IN SMALL & MEDIUM-SIZED BUSINESSES 1 (2017), https://keepersecurity.com/assets/pdf/Keeper-2017-Ponemon-Report.pdf [https://perma.cc/Q73U-USA9] (noting that more than 50% of small businesses surveyed have been the target of cyber data attacks arising from employee negligence and lack of resources to implement extensive data security programs). New forms of malware and ransomware are being developed and used faster than cybersecurity programs designed to combat these attacks can be implemented. *See* Danny Palmer, *Ransomware Crooks Test a New Way to Spread Their Malware*, ZDNET (Jan. 31, 2018), http://www.zdnet.com/article/ransomware-crooks-test-a-new-way-to-spread-their-malware/ [https://perma.cc/7AW9-4C9G] (describing a recent form of ransomware named GandCrab that locks a victim's network until they pay to have it unlocked using the relatively unknown cryptocurrency Dash instead of the more widespread cryptocurrency Bitcoin).

[39] *Data Breaches*, PRIVACY RIGHTS CLEARINGHOUSE (Mar. 26, 2017), http://www.privacyrights.org/data-breaches [https://perma.cc/7SL5-SK7Q].

alone, 1.9 billion records were exposed.[40] In response, governments and businesses have increasingly implemented biometric identification systems to enhance security.[41] Technological advancements have made biometric identification systems economically accessible for commercial use, enabling businesses to more easily adopt security, authentication, and fraud prevention measures for the protection of consumers.[42]

Biometrics are defined as measurements of a person's physical being based upon physiological or behavioral characteristics.[43] The definition of biometric data or biometric identifiers commonly includes retina or iris scans, fingerprints, voiceprints, scans of hand or face geometry, or images derived from photographs.[44] Biometric "authentication" is defined as an automated method that relies on "unique" factors to identify individuals.[45] According to experts in biometrics, these unique identifiers should contain the following optimal traits: (1) immutable nature over time; (2) great variability within a set of people; (3) possession by the entire set of people and ability to be measured indefinitely over time; (4) ability to be measured electronically; and (5) consented to by individuals for collection.[46] Using the above described traits as identification points, the following three-step process is generally applied to create biometric measurements: (1) a device takes an image; (2) that image is transformed into a biometric identifier using patterns such as pitch and tone for voice recognition, or a finger's specific contours for fingerprint identification; and (3) the identifier is put into an algorithm that generates a digital template.[47] The value

[40] *See Data Breaches by Breach Type*, PRIVACY RIGHTS CLEARINGHOUSE (Mar. 26, 2017), https://www.privacyrights.org/data-breaches/breach-type?taxonomy_vocabulary_11_tid=2434 [https://perma.cc/N2Z4-78YP].

[41] *See* Larduinat, *supra* note 6 (describing the rise of biometric technology as an alternative method of verifying an individual's identity).

[42] *See* Claypoole & Stoll, *supra* note 8, at 1 (attributing increased and easier use of biometric identification systems to technology advances in "sensors, readers, and software"); Larduinat, *supra* note 6 (listing the increased use of biometrics such as fingerprint, facial, and voice recognition, iris scanning, and selfies as authentication measures for consumers).

[43] *See* Roberg-Perez, *supra* note 17, at 60 (determining the characteristics that may be properly used in biometric identification).

[44] *See* James L. Wayman et al., *Introduction* to BIOMETRIC SYSTEMS: TECHNOLOGY, DESIGN AND PERFORMANCE EVALUATION 1, 1 (James L. Wayman et al. eds., 2005) (defining biometric technologies); Roberg-Perez, *supra* note 17, at 60 (defining biometric authentication); *see also* Norberg v. Shutterfly, Inc., 152 F. Supp. 3d 1104, 1106 (N.D. Ill. 2015) (finding that the Illinois Biometric Information Privacy Act's definition of biometric identifiers includes scans of facial geometry and images derived from photographs); Claypoole & Stoll, *supra* note 8, at 1 (listing the common types of biometric authentication measures).

[45] *See* Roberg-Perez, *supra* note 17, at 60.

[46] *See* Wayman et al., *supra* note 44, at 3.

[47] Christopher A. Miles & Jeffrey P. Cohn, *Tracking Prisoners in Jail with Biometrics: An Experiment in a Navy Brig*, NAT'L INST. OF JUST. J., Jan. 2006, at 6 (stating that a template is a digital representation of the individual's unique biometric identifiers and can be stored in a database).

of biometric data lies in the data's unique and unchangeable nature, which provides much greater security than easily-hacked passwords.[48]

Biometric identification is being used across numerous sectors for data security, individual authentication, fraud prevention, and to provide consumers with a simpler security experience.[49] These sectors range from the government's use of fingerprint biometrics in border control and correctional facilities, to use in the private sector as a means to manage employees.[50] The banking and financial industries have been at the forefront of implementing biometric identification security tools.[51] For example, in 2017, U.S. Bank partnered with Amazon's Alexa devices to enable consumers to access and complete banking transactions through voiceprint recognition.[52] In 2016, MasterCard announced a new initiative to test replacing passwords with selfies through facial recognition technology, in addition to developing other methods of authentication through voice recognition and cardiac rhythm.[53] In the tech industry, the replacement of passwords with selfies or facial recognition technology has become a reality with the November 2017 release of Apple's iPh-

[48] *See* Claypoole & Stoll, *supra* note 8, at 1 (arguing that biometric data provides greater security when compared to traditional data security measures); Larduinat, *supra* note 6 (noting that biometric technology increases security for consumers). *Contra* Meyer, *supra* note 6 (suggesting that biometric data is not entirely secure because unlike changeable passwords and social security numbers, "[w]e're stuck with our faces").

[49] *See* Roberg-Perez, *supra* note 17, at 60 (predicting that mobile devices containing fingerprint recognition technology will increase to one billion within 2017). Experimental methods are being developed to measure biometrics based upon an individual's "ocular blood vessel pattern, ear shape, gait, heart rhythm, and online behavior." *Id.*

[50] *See* Claypoole & Stoll, *supra* note 8, at 1 (describing the FBI's Next Generation Identification program that is being developed to collect a range of biometrics including "fingerprints, iris scans, DNA profiles, voiceprints, palm prints and photographs" and that may be used in conjunction with the Department of Homeland Security and Defense biometric databases); Miles & Cohn, *supra* note 47 (stating that as early as 2000, the National Institute of Justice and Department of Defense considered using biometric identification for criminal justice purposes and implemented the Biometric Inmate Tracking System at a naval brig in Charleston); Matthew A. Karlyn & Christopher G. Ward, *Using Biometric Timekeeping? Be Aware of Potential Compliance Risks*, NAT'L L. REV. (Oct. 23, 2017), https://www.natlawreview.com/article/using-biometric-timekeeping-be-aware-potential-compliance-risks [https://perma.cc/9TT5-H3DM] (noting the increased use of biometric "timekeeping" in workplaces through fingerprint, hand, and iris scans to decrease fraudulent time worked data).

[51] *See* Claypoole & Stoll, *supra* note 8, at 1 (explaining that banks often use voiceprint as an authentication measure in calls to customer service centers).

[52] *See Customers Can Now Complete Banking Tasks with U.S. Bank Skill for Amazon Alexa*, U.S. BANK (Sept. 6, 2017), https://www.usbank.com/newsroom/news/customers-can-now-complete-banking-tasks-with-us-bank-skill-for-amazon-alexa.html [https://perma.cc/84LQ-YAVR]. Gareth Gaston, an Executive Vice-President at U.S. Bank stated that "[v]oice technology is going to be central to the future of digital interaction." *Id.*

[53] *See Replacing Passwords with Selfies*, MASTERCARD, https://newsroom.mastercard.com/videos/replacing-passwords-with-selfies/ [https://perma.cc/4DXA-TQHT] (describing the pilot program to replace traditional passwords with other identification measures such as selfies or photographs taken by consumers).

one X.[54] The security feature relies on facial recognition in lieu of a password or fingerprint to unlock the device.[55] Other companies are attempting to advance facial recognition authentication by requiring smiling or winking.[56] This additional movement adds a level of security by ensuring that the object being scanned is a living individual and not merely a photograph or constructed mask.[57] Although biometric identification technology has the potential to provide consumers with greater data security and privacy protection, its rapid implementation coincides with what scholars call the "age of big data," which may ultimately undermine any potential privacy benefits.[58]

B. Modern Day Data Brokers and Discrimination

The use of big data has become embedded in the operations of global society.[59] In general, the term "big data" is used to describe the sheer scale and interconnectedness of information collected and retained by individuals, governments, and businesses that provides economic and social value.[60] Given today's information-sharing environment, the benefits and risks of big data are

[54] *See Apple Press Release*, *supra* note 7 (detailing the features of Apple's iPhone X, including the ability to unlock and secure the device and make payments).

[55] *See id.* (explaining that Face ID projects 30,000 infrared dots on an individual's face to create and digitally store a template on the user's device, as opposed to a cloud-based server, to ensure optimal security).

[56] *See* Claypoole & Stoll, *supra* note 8, at 1.

[57] *See id.*; *see also Apple Press Release*, *supra* note 7 (stating that Face ID is specifically designed not to be fooled by inanimate objects).

[58] *See* Omer Tene & Jules Polonetsky, *Privacy in the Age of Big Data: A Time for Big Decisions*, 64 STAN. L. REV. ONLINE 63, 63 (2012), https://www.stanfordlawreview.org/online/privacy-paradox-privacy-and-big-data/ [https://perma.cc/83L9-UFQS] (defining the current time period as the "age of big data"); *see also* Larduinat, *supra* note 6 (attributing the implementation of biometric technology into businesses' services and products, in part to the increased level of security provided by biometric information).

[59] *See* Barocas & Selbst, *supra* note 4, at 673 (stating that "big data is the buzzword of the decade"); Kate Crawford & Jason Schultz, *Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms*, 55 B.C. L. REV. 93, 96 (2014) (acknowledging the scope of big data across industries and stating that "big data" is an ambiguous term that generally describes the "use of large data sets in data science and predictive analysis"); *see also* JOHN PODESTA ET AL., EXEC. OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES, 1, 5 (2014), https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf [https://perma.cc/U2TN-FVQ6] (reporting that as big data operations increasingly occur in real time, they are likely to impact numerous aspects of an individual's daily life).

[60] *See* Tene & Polonetsky, *supra* note 58, at 63 (explaining that the vast number of individuals, governments, and businesses that have access to data contributes to the global economy through "innovation, productivity, efficiency, and growth"); *see also* Kenneth Olmstead & Aaron Smith, *Americans' Experiences with Data Security*, PEW RES. CTR. (Jan. 26, 2017), http://www.pewinternet.org/2017/01/26/1-americans-experiences-with-data-security/ [https://perma.cc/YNE9-7A4Z] (stating that approximately 64% of Americans provided personal information to online services and nearly two-thirds of Americans have been the subject of a data breach or theft).

amplified.[61] For example, big data is used to improve educational institutions' provision of services to students, healthcare institutions' quality of treatment to patients, and has been used by companies such as Google to identify inequality in their hiring and employment structures.[62] Nevertheless, there are numerous risks as well, such as the potential to enable opaque discrimination against entire classes of people.[63] For example, predictive crime policing programs such as PredPol correlate the data of historical patterns to target potential crime geography.[64] A confirmation bias occurs, as police are sent to patrol areas with a history of arrests and criminal activity, often historically impoverished black and Hispanic neighborhoods, and inevitably find the crime they are looking for.[65] Additionally, big data has been used by advertisers in invasive consumer ad targeting and by insurance agencies to predict whether a potential customer is too "erratic" based upon their activity and use of "likes" on Facebook.[66]

In this dual landscape of beneficial and risky big data, the modern day data broker industry has immense potential to adversely impact consumers.[67] A 2017 study published by the FTC found that one broker collected data on "1.4 billion consumer transactions and over 700 billion aggregated data elements" and another broker collected "3000 data segments for nearly every U.S. con-

[61] *See* FTC, BIG DATA: A TOOL FOR INCLUSION OR EXCLUSION? UNDERSTANDING THE ISSUES, 1, 5, 8–9 (2016), https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf [https://perma.cc/Q9WJ-B2DM] (claiming that the expansion of big data use across industries has led to both beneficial and harmful retention and usage).

[62] *See id.* at 6–8.

[63] *See id.* at 8–9 (noting the risks of big data, including opaque discrimination through use of biased models where consumers are prevented from seeing the discriminatory algorithms and correcting false or misleading information); Borgesius, *supra* note 4 (analogizing data brokers' collection and use of consumer data to the surveillance industry's practice of "social sorting" because both create potentially detrimental categorizations of individual data).

[64] *See* CATHY O'NEIL, WEAPONS OF MATH DESTRUCTION: HOW BIG DATA INCREASES INEQUALITY AND THREATENS DEMOCRACY 85 (2016).

[65] *See id.* at 86–87 (noting that when police are sent into historically crime-filled neighborhoods, relatively minor crimes such as nuisances are increasingly reported, producing more data and therefore more policing).

[66] *See* SCHNEIER, *supra* note 15, at 62–63 (stating that the Internet works primarily due to individuals voluntarily giving up data that is then sold to advertisers for personalized targeting); Kevin Peachey, *Facebook Blocks Admiral's Car Insurance Discount Plan*, BBC (Nov. 2, 2016), http://www.bbc.com/news/business-37847647 [https://perma.cc/T44X-ZZ5J] (reporting that Facebook rejected Admiral Insurance's proposal to use prospective customers' Facebook activity to determine levels of risk and assign insurance rates based on criteria such as the user's likes and the content of their posts).

[67] *See* Barocas & Selbst, *supra* note 4, at 677 (suggesting that the use of big data has the ability to segregate individuals within historically protected classes through automated processes); Nathan Newman, Comment Letter on Big Data: A Tool for Inclusion or Exclusion, Project No. P145406, at 3–4 (Aug. 15, 2014), https://www.ftc.gov/system/files/documents/public_comments/2014/08/00015-92370.pdf [https://perma.cc/2YCR-5EHA] (describing "price discrimination" where companies offer different online prices for the same goods or services based upon the data collected about individuals).

sumer."[68] Data brokers collect consumer information, aggregate consumer data into segments or marketable categories, and then sell those categories to third parties.[69]

The process begins when data brokers collect and purchase individuals' information from both public and private sources.[70] Public sources include federal, state, and local governments as well as social media sites, blogs, and the internet.[71] Data brokers purchase consumers' private information from commercial entities such as retailers and financial services companies.[72] Data brokers also obtain consumer data from other data brokers, often making it difficult for the consumer to determine how their information was originally obtained.[73] As data brokers circumvent direct consumer contact, consumers often do not even know that data brokers collect, retain, and use their information.[74] Furthermore, as of 2018, there is little legal authority preventing data brokers and commercial entities from sharing, buying, or selling consumer data, affording consumers little recourse to object to these practices.[75]

Data brokers aggregate the collected data elements with other PII through predictive algorithms that generate categories of individuals for third parties to

[68] FTC DATA BROKERS, *supra* note 9, at 3 (reporting findings on nine data brokers' collection and storage of data on individual U.S. consumers and consumer transactions). Consumer transaction information that is obtained from commercial sources often includes information about purchases including the type of asset obtained, the price, the dates of transaction, and the means of providing payment. *Id.* at 13. Data elements include distinct data points about an individual such as his or her name, age, race, gender, marital status, and "derived data elements" such as an individual's interests. *Id.* at 19. Data segments or categories are created through the input of specific data elements into a predictive algorithm to place consumers into marketable categories. *Id.*

[69] *See id.* at 13–14, 19, 23.

[70] *See id.* at 11–14 (listing the sources from which data brokers obtain consumer information and recognizing that out of the nine data brokers reviewed in the report, none obtained data directly from consumers).

[71] *See id.* at 13–14. Federal government sources of consumer data include the U.S. Census Bureaus, the Social Security Administration, the U.S. Postal Service, and other federal agencies that collect information on individuals. *Id.* at 11. State and local government sources of consumer data include professional and recreational licenses, property and assessor records such as taxes, deeds, and mortgages, voter registration, court documents including criminal records and civil actions. *Id.* 12. Other sources of publicly available information include directories and information obtained on the Internet through sites such as LinkedIn, where profiles are not restricted in the user's privacy settings. *See id.* at 13, 13 n.40 (explaining that some social media sites such as Facebook restrict data brokers use of automated tools to collect data).

[72] *See id.* at 13–14.

[73] *See id.* at 46 (stating that out of the nine data brokers in the study, seven exchanged data with other data brokers).

[74] *See* FTC DATA BROKERS, *supra* note 9, at 46 (noting that data brokers do not collect consumer information directly from the consumer).

[75] *See Data Brokers and "People Search" Sites*, *supra* note 10 (stating that data brokers' collection and use of consumer data is narrowly regulated and does not allow consumers to see the data collected about them or to correct any inaccuracies).

purchase.[76] These categories may ultimately be inherently discriminatory, leading to exploitation of consumers.[77] For example, the FTC uncovered categories targeting consumers' race and income levels such as "Urban Scramble" and "Mobile Mixers" in which the underlying data contained a large percentage of low income Latinos and African Americans.[78] Other categories included "Rural Everlasting," which targeted individuals older than sixty-six who had low levels of education and owned almost no valuable assets, and "Diabetes Interest" and "Cholesterol Focus," which targeted individuals based on sensitive health information.[79]

As the last step in their operation, data brokers ultimately sell these categories to third parties such as employers, advertisers, and discount loan companies.[80] A specific danger arises from data brokers' and other entities' use of predictive algorithms.[81] Predictive algorithms do not merely categorize individuals based on known data but also create inferences about individuals.[82] Target Corporation ("Target"), for example, used predictive algorithms to determine which of its female consumers were pregnant.[83] The female consumers

[76] *See* SCHNEIER, *supra* note 15, at 62 (detailing how data brokers such as Acxiom sort individuals into categories that are then sold to businesses, employers, or other entities); FTC DATA BROKERS, *supra* note 9, at 19–20, 46–47 (describing the process of creating "data segments" from "data elements" and listing categorizations derived from sensitive consumer information such as age, ethnicity, income levels, and health issues).

[77] *See* SCHNEIER, *supra* note 15, at 62 (listing examples of categories created by data brokers to sell to third parties); *see also* Goodman, *supra* note 5 (noting that biometric technology has the ability to collect an individual's sensitive information such as race, gender, age, economic class or health conditions that could be used to categorize that individual in a discriminatory manner).

[78] *See* FTC DATA BROKERS, *supra* note 9, at 20, 47 (listing marketable categories specifically created based upon consumers' race and financial data).

[79] *See id.* (noting that the categorizations created the potential for discrimination by differentiating between consumers based on factors such as race, age, educational level, net worth, and specific health conditions).

[80] *See* SCHNEIER, *supra* note 15, at 62 (describing the types of third parties that purchase data categories created by data brokers); FTC DATA BROKERS, *supra* note 9, at 25 (explaining that third parties purchase selected categories from data brokers with the choice of including or excluding certain data segments or categories of consumers such as "Financially Challenged" or "Underbanked").

[81] *See* Crawford & Schultz, *supra* note 59, at 96 (stating that the sheer scale of information collected by big data inevitably includes individuals' sensitive information that can be discriminatorily used); Joshua A. Kroll et al., *Accountable Algorithms*, 165 U. PA. L. REV. 633, 680 (2017) (noting that the risk posed by automated algorithms is the inability to presently know the future discriminatory effects of the rules learned by the machines).

[82] *See* FTC DATA BROKERS, *supra* note 9, at 19 (describing that data brokers make assumptions about individuals based upon actual data to create "derived data elements"); Crawford & Schultz, *supra* note 59, at 98 (noting that big data algorithms can intake known public information about individuals to create a form of artificial PII).

[83] *See* Crawford & Schultz, *supra* note 59, at 94, 98 (detailing how Target Corporation's marketing department predicted which of its female customers were pregnant through aggregation of consumer data and use of predictive models). Notably, Target Corporation ("Target") wanted to advertise its pregnancy and baby products to females before the information was available through public birth

did not specifically disclose this information, yet Target aggregated patterns of purchase behavior to assign females a "pregnancy prediction score."[84] Target then gave this information to its marketing department to send pamphlets and coupons for pregnancy and baby-related products to female customers' homes based upon that score.[85] Predictive models like the one created by Target are often automated to recognize correlations and categorize individuals based on forecasts of future outcomes and estimations of unknown variables, such as using the frequency and types of products a customer purchases to estimate the stage of her pregnancy.[86] Potential discrimination can result from implementing algorithms that fail to prevent or correct implicit biases, introduce institutional prejudices, define the target variable in a manner that affects classes differently, or fail to introduce a sufficient range of factors.[87]

Predictive models can function as discriminatory feedback loops because they are scalable, opaque, and able to cause damage.[88] These models are able to cause harm because there is no current comprehensive federal law that gives consumers a right to correct inaccurate or false data, or assumptions made by

records. *See* Charles Duhigg, *Psst, You in Aisle 5*, N.Y. TIMES MAG., Feb. 19, 2012, at 30 (reporting that Target created these predictive models to attract female consumers before their competitors).

[84] *See* Duhigg, *supra* note 83 (stating that Target identified twenty-five products, including unscented lotion, vitamin supplements, and cotton balls, that, upon aggregated purchase over time, enabled Target to not only predict that a female was pregnant, but also her individual due date with near accuracy); *see also* Crawford & Schultz, *supra* note 59, at 98 (explaining that the current privacy laws do not reach Target's use of predictive data because it was created or inferred rather than directly obtained). Although retailers' use of predictive models is not currently regulated, consumers often lose trust in the marketplace when ads are seen as too personal or invasive, which therefore acts as a check on retailers' aggressive advertising practices. *See* FTC DATA BROKERS, *supra* note 9, at 48 (noting that an entity's targeted marketing based upon personal information can cause consumers to refrain from continued interaction with those entities).

[85] *See* Crawford & Schultz, *supra* note 59, at 95 (stating that although consumers are aware that retailers such as Target collect data about them, it is unlikely that they expect the use of predictive models to infer sensitive and private information); Duhigg, *supra* note 83 (detailing Target's targeted marketing of products to female consumers based upon Target's model's trimester prediction for each consumer).

[86] *See* Barocas & Selbst, *supra* note 4, at 677 (stating that to improve automated decision making, predictive algorithms are exposed to a set of observed characteristics to determine correlations or relationships within the data); Tene & Polonetsky, *supra* note 58, at 64 (providing the example of Kaiser Permanente using big data analytics to determine that the medication Vioxx had caused 27,000 deaths between 1999 and 2003).

[87] *See* Barocas & Selbst, *supra* note 4, at 675 (noting that the potential for discrimination can arise intentionally or inadvertently because algorithms are designed to use proxies for historically discriminated classes); Latanya Sweeney, *Discrimination in Online Ad Delivery*, COMM. ACM, May 2013, at 44, http://mags.acm.org/communications/may_2013?pg=47#pg47 [https://perma.cc/T3XR-WFST] (reporting that upon a Google search of a name "racially associated" with the black community, there was a significant increase in resulting advertising insinuating the individual had a criminal record).

[88] *See* O'NEIL, *supra* note 64, at 27, 31 (describing predictive algorithms that are opaque, scalable, and able to cause damage as "weapons of math destruction").

data brokers.[89] These models are opaque because consumers often do not have access to their data to confirm that it is incorrect or misleading.[90] Furthermore, even if data brokers allow consumers to see the data collected about them, the reports usually only include the individual data points but not the aggregated categorizations.[91] Lastly, these models are scalable because they have the ability to be applied consistently across diverse and sizeable data sets.[92]

Importantly, the methodology used in big data collection often allows data brokers and businesses to circumvent the already scant regulations surrounding the collection, use, and disclosure of PII.[93] When data brokers or businesses use opaque predictive algorithms, proof of discriminatory intent or impact is difficult to ascertain.[94] At the point of data collection, it is often the case that no PII has actually been obtained.[95] Models can use an individual's activity on Facebook, their recent geographic locations, or even the genre of music on a consumer's streaming service to infer and create attributes that are then used as proxies for race, gender, or socioeconomic status, all of which are arguably forms of PII.[96] As noted above, these models are not always accurate, and in-

[89] *See* FTC DATA BROKERS, *supra* note 9, at 48 (describing how consumers assigned a low marketing score are unable to correct any false data attributed to that score and therefore are limited to disparate marketing targeted to that score range); *Data Brokers and "People Search" Sites*, *supra* note 10 (stating that data brokers' collection and use of consumer data is narrowly regulated and does not allow consumers to see the data collected about them or to correct any inaccuracies).

[90] *See* FTC DATA BROKERS, *supra* note 9, at 49 (explaining that for products such as insurance, data brokers do not allow consumers to have access to the data collected about them and specific data that is accessible to consumers, is often difficult, if not impossible for consumers find).

[91] *See* O'NEIL, *supra* note 64, at 152 (providing that data brokers lack complete transparency with consumers by not disclosing the conclusions and categorizations made about consumers, but rather limit disclosure to the individually collected facts).

[92] *See id.* at 27, 31 (explaining that to be "scalable," a model must have the ability to be applied consistently across diverse and sizeable data sets). Credit rating models are an example of scalable models because after a score has been applied to an individual, that score can impact numerous other aspects of an individual's life. *See id.* at 30.

[93] *See* Barocas & Selbst, *supra* note 4, at 694, 701, 711 (stating that antidiscrimination law as it currently exists does not provide much recourse to claims of discrimination based upon data mining); Crawford & Schultz, *supra* note 59, at 101 (describing big data's ability to use data to discriminate in the credit loan and housing industries, escaping federal credit regulations and fair housing laws).

[94] *See* Barocas & Selbst, *supra* note 4, at 692–93 (stating that big data correlations and algorithms are formed from obscure proxies).

[95] *See* FTC DATA BROKERS, *supra* note 9, at 19 (describing how data brokers can make assumptions about individuals based off non-PII data to create "derived data elements"); Barocas & Selbst, *supra* note 4, at 692 (detailing how data mining is able to predict or make assumptions about individuals' undisclosed information using predictive analysis); Crawford & Schultz, *supra* note 59, at 100 (noting that the predictive models can essentially create an individual's PII, even though none of the data points alone constitute PII).

[96] *See* Barocas & Selbst, *supra* note 4, at 712 (listing types of consumer data used as proxies in predictive models); Crawford & Schultz, *supra* note 59, at 100–01 (describing the types of data that are used as proxies to develop consumer categories).

dividuals are rarely provided with the means to correct any false characterizations, enabling both intentional and inadvertent discrimination.[97]

C. Biometric Data in the Federal Privacy Landscape

The right to privacy has not been recognized as an absolute fundamental human right of United States citizens.[98] There is no specific protection for rights of privacy within the U.S. Constitution.[99] Only in 1965, in *Griswold v. Connecticut*, did the Supreme Court find a "penumbra" of privacy rights within the First, Third, Fourth, and Fifth Amendments.[100] Despite this rationale, some scholars have claimed that the right to privacy should cede to considerations of capitalism such as protection of the press, free market theory, or promotion of public welfare.[101] Although federal law in the United States is not entirely without data privacy regulation, regulations at the federal level are industry-specific and inconsistent across sectors.[102] Under many of these in-

[97] *See* FTC DATA BROKERS, *supra* note 9, at 48 (detailing that consumers assigned a low marketing "score" are unable to correct any false data attributed to that score and are therefore limited to marketing targeted to that score range); *Data Brokers and "People Search" Sites*, *supra* note 10 (noting that no federal law enables consumers to see the data collected about them or to correct any inaccuracies).

[98] *See* McKay Cunningham, *Privacy in the Age of the Hacker: Balancing Global Privacy and Data Security Law*, 44 GEO. WASH. INT'L L. REV. 644, 663 (2012) (stating that the United States does not provide its citizens with a comprehensive right to privacy). In contrast, in May 2018, Europe implemented the General Data Protection Regulation ("GDPR"), a comprehensive data protection law that is directly binding on all EU member states. *See* DANIEL J. SOLOVE & PAUL H. SCHWARTZ, PRIVACY LAW FUNDAMENTALS 264 (7th ed. 2017) (noting the direct application of the GDPR with a few exceptions for EU member states to implement further legislation).

[99] *See* Griswold v. Connecticut, 381 U.S. 479, 483–85 (1965) (holding that although there is no enumerated right to privacy in the Constitution, in certain cases, the courts have found rights in "penumbras" where they are not explicitly stated in the Constitution because their "existence is necessary in making the express guarantees fully meaningful").

[100] *See id.* at 484 (determining that "penumbra" rights of "privacy and repose" exist in the First, Third, Fourth, and Fifth Amendments to the Constitution). A penumbra, as used by the Court in *Griswold*, is a place from which a right is implied or inferred from specific guarantees in the Constitution. *See id.* at 484.

[101] *See* Richard Posner, *The Right of Privacy*, 12 GA. L. REV. 393, 404, 422 (1978) (describing Judge Posner's economic theory of privacy that protection of individual privacy inhibits the free flow of information and thereby market efficiency); Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 214, 216–18 (1890) (detailing the circumstances in which the right to privacy must cede to public welfare, freedom of the press, and freedom of capital markets).

[102] *See* SOLOVE & SCHWARTZ, *supra* note 98, at 34–35 (listing a number of United States federal privacy laws that are specific to sectors such as healthcare, credit reporting, education, and financial industries); Theodore Rostow, *What Happens When an Acquaintance Buys Your Data?: A New Privacy Harm in the Age of Data Brokers*, 34 YALE J. ON REG. 667, 676 (2017) (calling commercial privacy regulations in U.S. federal law a "patchwork"); *see also* Cunningham, *supra* note 98, at 664 (detailing the sectoral approach of the United States regarding privacy regulations as opposed to a comprehensive approach). The "sectoral" approach signifies industry-specific privacy legislation whereas the "comprehensive" approach indicates privacy legislation that is applicable across indus-

dustry-specific regulations, the duties imposed upon businesses and definitions of key terms such as "PII" are fragmented and varied.[103] There is, however, a level of consistency in the types of activities subjected to regulation, such as an entity's collection, use, disclosure, and retention of PII.[104] For example, the Gramm-Leach-Bliley Act of 1999 addresses financial institutions' collection and use of nonpublic personal information, the Family Educational Rights and Privacy Act addresses educational institutions' collection and use of student records, and the Health Insurance Portability and Accountability Act ("HIPAA") addresses covered entities' collection and use of protected health information.[105]

Thus, the United States does not currently have a single, comprehensive federal law regulating businesses' collection and use of biometric data.[106] Rather, in line with the United States' sectoral approach, there are several industry-specific laws that govern private and public collection and use of an individual's biometric identification data within financial, educational, commercial, and healthcare institutions.[107] HIPAA's definition of "individually identifiable health information" can include certain biometric data.[108] The Genetic Information Nondiscrimination Act protects individual's genetic information from discrimination in insurance and employment contexts.[109] The Privacy Act of 1974 provides potential barriers to entities from accessing or disclosing an

tries. *See* Cunningham, *supra* note 98, at 664 (describing that the United States takes a sectoral approach and the EU takes a comprehensive approach).

[103] *See* Cunningham, *supra* note 98, at 665 (stating that the definition of PII differs under the Fair Credit Reporting Act, Video Privacy Protection Act, and the Gramm-Leach-Bliley Act); Rostow, *supra* note 102, at 677–78 (providing examples of sectoral differences such as the Health Insurance Portability and Accountability Act's inapplicability to "non-covered entity" data such as that produced by Apple devices, Google searches, or wearable devices and the Gramm-Leach-Bliley Act's application to data used only by "financial institutions").

[104] *See* Rostow, *supra* note 102, at 677 (noting that of the federal privacy statutes that do provide regulation, they only protect the means by which an entity interacts with the data).

[105] *See* Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801–6809 (2012) (addressing disclosure of nonpublic personal information); Family Educational Rights and Privacy Act, 20 U.S.C. § 1232(g) (2012) (addressing the limitations on disclosure of protected education records); Health Information Portability and Accountability Act, 42 U.S.C. § 1320d-6 (2012) (listing the limitations of disclosure of individually identifiable health information).

[106] *See* Claypoole & Stoll, *supra* note 8, at 4 (noting that several industry-specific federal laws regulate biometric identification data).

[107] *See id.*; *see also* Roberg-Perez, *supra* note 17, at 63 (listing the different sector-specific federal laws that address biometric data).

[108] *See* 42 U.S.C. § 1320d(6) (defining the term "individually identifiable health information" to include data obtained from an individual by a qualified entity that concerns health conditions or health care of an individual that either identifies the individual or can reasonably be believed to identify the individual).

[109] *See* 29 U.S.C. § 1182 (2012) (stating that accessibility of health insurance may not be predicated based on an individual's genetic information). Genetic information is defined under the Genetic Information Nondiscrimination Act as information about an individual's and their family members' genetic tests. *See Genetic Information Discrimination*, EQUAL EMP. OPPORTUNITY COMM'N, https://www.eeoc.gov/laws/types/genetic.cfm [https://perma.cc/HN6D-9MDR].

individual's personally identifying data that is contained in federal records.[110] Of note, the Children's Online Privacy Protection Act ("COPPA") provides extensive protection of minors' privacy, including the collection of children's biometric data.[111] COPPA requires parental consent before photos, videos, or audio recordings that contain a child's image or voice are collected.[112] Additionally, COPPA allows businesses to verify parental consent using facial recognition technology.[113]

The FTC has the authority to promulgate and enforce rules to protect consumers from "unfair and deceptive" business practices.[114] Aside from enforcement of COPPA, however, the FTC has yet to create specific rules regarding businesses' implementation and use of biometric data in technology.[115] Rather, the FTC has issued best practices including, "privacy by design," increasing transparency, giving consumers a method to opt-in or opt-out of biometric information collection, and obtaining clear and concise consent from individuals.[116] In accordance with these best practices, businesses often subject the data they maintain to anonymization or de-identification techniques.[117] Anonymiza-

[110] *See* Privacy Act of 1974, 5 U.S.C. § 552(a) (2012) (regulating the collection, maintenance, use, and disclosure of PII and records of individuals that are maintained by federal agencies).

[111] *See* Child Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–6506 (2012) (listing photos, videos, or audio files containing a child's image or voice as personal information under the statute).

[112] *See* 15 U.S.C. § 6501(9) (stating that acceptable consent from a child's parent must be obtained using any reasonable effort, including through use of new technology); *Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business*, FTC (June 2017), https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance [https://perma.cc/349J-GUG7] (detailing the requirements an entity subject to the Child Online Privacy Protection Act must follow including notice and consent).

[113] *See Children's Online Privacy Protection Rule*, *supr*a note 112 (stating that authorized methods of verifying parental consent include having a parent submit two photos, a driver's license or photo ID and a second photo, and authenticating the photos with facial recognition technology).

[114] *See* Federal Trade Commission Act, 15 U.S.C. § 45(a)(2) (2012) (listing the scope of the FTC's authority to protect consumers).

[115] *See* FTC, FACING FACTS: BEST PRACTICES FOR COMMON USES OF FACIAL RECOGNITION TECHNOLOGIES 1–2 (2012) [hereinafter FACING FACTS], https://www.ftc.gov/sites/default/files/documents/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies/121022facialtechrpt.pdf [https://perma.cc/Q5QL-RNV5] (recommending best practices businesses should implement if planning to or already using biometric facial recognition technology); *see also* Claypoole & Stoll, *supra* note 8, at 3 (describing the FTC's publication "Facing Facts" that provides guidance for businesses overseen by the FTC).

[116] *See* FACING FACTS, *supra* note 115, at 1–2 (describing the recommended best practices for businesses' collection and use of biometric facial recognition technology).

[117] *See* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1703, 1707–08 (2010) (noting that entities that maintain databases often use anonymization techniques to provide greater security for individuals' information). Anonymization or de-identification can occur through a number of techniques, the most common being the determination and elimination of any information that identifies an individual, followed by either suppression, generalization, or aggregation. *See id.* at 1713–15 (listing the methods of anonymization used to de-identify an individual before that data is released to a third party). Suppression is the dele-

tion has been championed as ensuring an individual's privacy, and is distinct from mere de-identification, which is defined as a method to remove personal information without the explicit guarantee of irreversibility.[118] Some scholars, however, criticize these theories' promises of data security, as computer scientists have conducted studies to prove that both anonymized and de-identified data can be easily re-identified.[119]

Furthermore, in 1998 the FTC put forth a version of Fair Information Practice Principles ("FIPPs") as a framework for developing privacy laws in an age of rapid technological development.[120] The five core principles set forth include: (1) notice/awareness; (2) choice/consent; (3) access/participation; (4) integrity/security; and (5) enforcement/redress.[121] Of particular note, whereas the FTC's best practices and FIPPs provide non-binding structures to regulate an entity's collection, use, and disclosure of an individual's PII through notice and consent requirements, they do not provide a mechanism to protect consumers against the "creation" of PII through predictive algorithms.[122]

Notably, the Federal Communications Commission (FCC), not the FTC, currently has jurisdiction over regulation of Internet service providers ("ISPs").[123] The Trump Administration recently signed a Congressional Re-

tion of the identifying information, generalization changes the identifying information, and aggregation is the combination of groups of similar data sets. *See id.* (explaining that each method is forced to reconcile increased privacy protections with diminishing utility of the data as it is anonymized).

[118] *See* Ira S. Rubinstein & Woodrow Hartzog, *Anonymization and Risk*, 91 WASH. L. REV. 704, 710–11 (2016) (delineating between anonymization and de-identification).

[119] *See* Ohm, *supra* note 117, at 1724–25 (stating that theories of anonymization have been disproven through development of re-identification techniques including the combination of anonymized data with outside information); Simson L. Garfinkel, *De-Identification of Personal Information*, NAT'L INST. OF STANDARDS & TECH 1–3 (2015), http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8053.pdf (noting the issues with the definitions and usage of anonymization and de-identification).

[120] *See* FTC, PRIVACY ONLINE: A REPORT TO CONGRESS 7–11 (1998) [hereinafter PRIVACY ONLINE], https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf [https://perma.cc/SB5Z-L7NY] (listing the Fair Information Practice Principles ("FIPPs") the FTC encourages legislatures to consider when constructing new privacy regulations).

[121] *See id.* at 7–11.

[122] *See* FACING FACTS, *supra* note 115, 1–2 (recommending best practices such as notice and consent and opt-in and opt-out mechanisms for businesses implementing facial recognition technology); PRIVACY ONLINE, *supra* note 120, at 7–11 (listing the five core FIPPs principles); *see also* Crawford & Schultz, *supra* note 59, at 106 (noting the difficulty in regulation at the initial collection of a single data element because often nothing collected is considered PII and it is not possible to determine at that point any potential predictive privacy harms).

[123] *See In re* Protecting and Promoting the Open Internet, Report and Order on Remand, 30 FCC Rcd. 5601, paras. 398–403 (2015) (authorizing the Federal Communications Commission's (FCC) regulation of broadband companies). The FCC's Open Internet Order determined that broadband companies are "common carriers," which are specifically exempted from the FTC's jurisdiction under the FTC Act. *See* Brian Naylor, *Congress Overturns Internet Privacy Regulation*, NPR (Mar. 28, 2017), https://www.npr.org/2017/03/28/521831393/congress-overturns-internet-privacy-regulation [https://perma.cc/YV26-BKT7] (noting that the nullification of the FCC's Broadband Privacy Rule provides a path for the FTC as the sole regulator of internet privacy issues); Arielle Roth, *Three Issues to Watch as the FCC Writes Privacy Rules for Broadband Companies*, HUDSON INST. (Aug. 15,

view Act that nullified the Broadband Privacy Rule, an FCC rule that had yet to take effect but would have regulated ISPs' collection and sale of consumer data.[124] Following the nullification of this rule, ISPs can continue to record and sell individuals' browsing data, are not required to inform consumers what information they collect or who they sell it to, and can force individuals to resolve complaints by arbitration.[125] Importantly, ISPs are currently not prohibited from selling an individual's data, including biometric data, to third parties such as data brokers.[126]

The European Union's General Data Protection Regulation ("GDPR"), effective as of May 25, 2018, applies extraterritorially to U.S. businesses that offer goods or services to, or monitor the behavior of EU individuals.[127] The GDPR defines biometric data as "personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person which allow or confirm the unique identification of that natural person."[128] Under the statute, biometric data is listed as a type of sensitive personal data.[129] The processing of sensitive personal data is entirely prohibited, subject to a number of enumerated exceptions including, but not limited to, obtaining explicit consent, specified public interest considerations, and certain exemptions in the fields of employment and social protection law.[130] At

2016), https://www.hudson.org/research/12769-three-issues-to-watch-as-the-fcc-writes-privacy-rules-for-broadband-companies [https://perma.cc/YP3F-CPW4] (describing the FCC's Open Internet Order granting the FCC authority to regulate broadband companies).

[124] *See* S.J. Res. 34, 115th Cong. (2017) (stating the Senate and House of Representatives joint resolution to nullify the FCC's Broadband Privacy Rule).

[125] *See* Devin Coldewey, *Everything You Need to Know About Congress' Decision to Expose Your Data to Internet Providers*, TECH CRUNCH (Mar. 29, 2017), https://techcrunch.com/2017/03/29/everything-you-need-to-know-about-congress-decision-to-expose-your-data-to-internet-providers/ [https://perma.cc/9PPA-CVCL] (listing ISP conduct that is not subject to regulation).

[126] *See* Alina Selyukh, *FCC Chairman Goes After His Predecessor's Internet Privacy Rules*, NPR: THE TWO-WAY (Feb. 24, 2017), https://www.npr.org/sections/thetwo-way/2017/02/24/517050966/fcc-chairman-goes-after-his-predecessors-internet-privacy-rules [https://perma.cc/T7H8-SRLH] (explaining that without regulation, Internet service providers ("ISPs") would not be prohibited from using or selling an individual's data). Proponents of the FCC's Broadband Privacy Act claim that ISPs can obtain more data on consumers than individual websites or non-broadband companies. *See id.* (noting that ISPs can obtain consumer data from each individual website or internet-based service that a consumer accesses).

[127] *See* Commission Regulation (EU) 2016/679, art.3, 2016 O.J. (L 119) 1, 32–33 [hereinafter General Data Protection Regulation] (expanding the territorial scope of regulation of data controllers and processors that process "personal data" of individuals who are located in the EU).

[128] *See id.* art. 4(14), at 34.

[129] *See id.* art. 9, at 38–39 (listing the categories of data that are prohibited from processing subject to a list of enumerated exceptions).

[130] *See id.* art. 9(2)–(4), at 38–39 (listing the situations in which a data controller or processor is not prohibited from processing an individual's sensitive personal data). Personal data under the GDPR is defined as "any information relating to an identified or identifiable natural person." *Id.* art. 4(1), at 33. Consent under the GDPR requires "freely given, specific, informed and unambiguous indication"

the time of publication of this Note the GDPR only recently took effect, and its total potential impact on U.S. businesses has yet to be ascertained.[131]

II. MODERN PIONEERS: STATE BIOMETRIC DATA STATUTES

Regulations addressing businesses' use of biometric data are being developed at the cross-section of society's need for greater data security and big data's discriminatory impact on consumers.[132] Over-regulation risks disincentivizing technological development and use of biometric data to enhance security.[133] Under-regulation risks exposing entire categories of people to discriminatory practices.[134] As noted above, the industry-specific approach of federal privacy law does not provide a comprehensive scheme for the regulation of biometric data.[135] As a result, states have increasingly sought to regulate businesses' collection, use, retention, and disclosure of biometric data.[136] Three states' statutes, Illinois, Texas, and Washington, do provide comprehensive biometric data regulation, however, the statutes lack consistency.[137] In addi-

of the individual's agreement to the processing of his or her personal data made by a "statement or by a clear affirmative action." *Id.* art. 4(11), at 34.

[131] *See* Yaki Faitelson, *Yes, The GDPR Will Affect Your U.S.-Based Business*, FORBES (Dec. 4, 2017), https://www.forbes.com/sites/forbestechcouncil/2017/12/04/yes-the-gdpr-will-affect-your-u-s-based-business/#4eb2d5146ff2 [https://perma.cc/F9PT-9ZBC] (noting that the GDPR will affect different United States based businesses differently depending on the application of the territorial reach of the GDPR).

[132] *See* Claypoole & Stoll, *supra* note 8 (regarding both the vast benefits and risks surrounding biometric technology as the reason for increased regulation surrounding its use by private and public entities).

[133] *See* Daisy Contreras, *Illinois Issues: The Battle Over Transparency and Privacy in the Digital Age*, NPR ILL. (July 13, 2017), http://nprillinois.org/post/illinois-issues-battle-over-transparency-and-privacy-digital-age#stream/0 (reporting that business advocates critique Illinois privacy statutes as imposing a technological development "chilling effect"). According to Carl Szabo of NetChoice, some already developed facial recognition technology cannot be used in Illinois. *See id.* (noting the comprehensive scope of Illinois's BIPA); Meyer, *supra* note 6 (quoting Szabo of NetChoice that "requiring consent before every use of the technology would create universal complexities that would eliminate many of the benefits of facial recognition").

[134] *See* O'NEIL, *supra* note 64, at 27, 31, 153 (noting the danger caused by opaque and scalable predictive algorithms for which there is no information accountability); Barocas & Selbst, *supra* note 4, at 675 (explaining that potential discrimination can occur in both intentional and inadvertent ways through designing algorithms that use proxies for historically discriminated classes).

[135] *See* Claypoole & Stoll, *supra* note 8, at 4 (describing that aligned with the United States' industry-specific approach to privacy regulation, there are several industry-specific laws that govern private and public collection and use of an individual's biometric identification data within financial, educational, and healthcare institutions).

[136] *See* Roberg-Perez, *supra* note 17, at 62–63 (listing the additional states that have been in talks, have pending legislation or have introduced bills proposing regulation of collection and use of biometric data).

[137] *See* Tumeh, *supra* note 18 (listing the differences in notice, consent, sale, and enforcement requirements among the three state statutes). California recently passed a comprehensive privacy act, the California Consumer Privacy Act of 2018, set to take effect on January 1, 2020. *See* California Consumer Privacy Act of 2018, A.B. 375, 2017–2018 Leg., Reg. Sess. (Cal. 2018) (describing the

tion, Alaska, Connecticut, Massachusetts, Michigan, Montana, New Hampshire, and New York have looked to adopt their own versions of biometric data regulations.[138] Despite the growing interest in regulation, some states have not been successful in passing any biometric regulation statutes, as both Montana's and Connecticut's proposed bills did not survive the state legislative process.[139]

As states' interest in regulation of businesses' interaction with biometric data increases, it is important to understand the existing legal framework surrounding state biometric data regulation.[140] Section A of this Part discusses the 2008 Illinois Biometric Information Privacy Act ("BIPA"), the recent surge of class action lawsuits brought under the BIPA, and the 2009 Texas Capture or

purpose of the act and providing the text of the act). The law includes biometric information in the definition of personal information and provides consumers with a number of rights including: (i) the right to require disclosure of their personal information a business collects, including what it is used for, and whether it is disclosed or sold and to whom; (ii) the right to opt-out of a business selling personal information to third parties; (iii) the right to be forgotten—or to have a business delete personal information upon request; and (iv) the right to receive equal services and pricing. *See id.* §§ 1798.100, 1798.105, 1789.110, 1798.115, 1798.120, 1798.125, 1798.135, 1798.140(b), 1798.140(o)(1)(E) (describing consumers' rights under the act and the inclusion of biometric information in the definition of personal information). At the time this Note was written, the California statute had not yet passed, and thus exceeds the scope of this analysis.

[138] *See* Establishing a Committee to Study the Use and Regulation of Biometric Information, Sess. Laws, Ch. 21, H.B. 523 (N.H. 2018) (passing the biometric regulation bill to establish a committee); A9793, Assemb., Reg. Sess. (N.Y. 2018) (proposing a biometric data law identical to the Illinois BIPA); S8547, Senate, Reg. Sess. (N.Y. 2018) (proposing a biometric data law identical to the Illinois BIPA); H.B. 72, 30th Leg., 1st Sess. (Ala. 2017) (proposing notice and consent requirements for the collection of biometric information as well as an expansive definition of biometric data); H.B. 5522, Gen. Assemb., Jan. Sess. (Conn. 2017) (stating the purpose of regulating retailer's use of facial recognition software for marketing purposes); H.B. 1985, 190th Gen. Assemb., Reg. Sess. (Mass. 2017) (providing that § 1 of Ch. 93H of Massachusetts's General Laws would be amended to include "biometric indicator" within the definition of "personal information"); H.B. 5019, 99th Leg., Reg. Sess. (Mich. 2017) (proposing a biometric privacy act that contains notice, consent, retention, sale and disclosure requirements); H.B. 518, 65th Leg., Reg. Sess. (Mont. 2017) (proposing regulation of a private entity's collection, use, storage, and disclosure of an individual's biometric data); H.B. 523, 165th Gen. Court, Reg. Sess. (N.H. 2017) (amending the proposed biometric regulation bill to instead establish a committee to "study the use and regulation" of biometric information). Section 2 of Ch. 93H of the Massachusetts General Laws requires the adoption of regulations regarding any person that "owns or licenses personal information" of a resident of Massachusetts. *See* MASS. GEN. LAWS ch. 93H, § 2(a) (2018) (detailing the mandated regulations regarding the personal information of Massachusetts residents).

[139] *See Bill Actions*, MONT. LEGISLATURE, http://laws.leg.mt.gov/legprd/law0210W$BSIV.ActionQuery?P_BILL_DFT_NO5=LC2063&Z_ACTION=Find&P_Sess=20171 [https://perma.cc/CK3B-B6KQ] (noting that the bill died in the Standing Committee on April 28, 2017); *Bill Status*, CONN. GEN. ASSEMBLY, https://www.cga.ct.gov/asp/cgabillstatus/cgabillstatus.asp?selBillType=Bill&bill_num=HB05522&which_year=2017 [https://perma.cc/326B-SZ3Y] (noting that the bill was referred to the Joint Committee on General Law in January 2017 and never passed).

[140] *See infra* notes 143–203 and accompanying text.

Use of Biometric Identifier Act ("CUBI").[141] Section B of this Part discusses the Washington statute enacted in 2017.[142]

A. Biometric Data Statutes in Illinois and Texas

Despite the fact that Illinois and Texas implemented comprehensive statutes regulating businesses' collection and use of biometric information in 2008 and 2009 respectively, both statutes remained largely latent until the surge of class action suits brought under the Illinois BIPA beginning in 2015.[143] Part 1 of this Section discusses the fundamental provisions of the Illinois BIPA.[144] Part 2 of this Section discusses the rise of class actions brought under the BIPA in Illinois and the obstacles facing plaintiffs.[145] Part 3 of this Section discusses the similarities and differences between the Illinois BIPA and the Texas CUBI.[146]

1. The Illinois Biometric Information Privacy Act

In 2008, Illinois became the first state to enact a comprehensive law addressing businesses' collection and use of biometric information.[147] The statute broadly defines "biometric information" as "any information" that is "based on an individual's biometric identifier used to identify an individual," without regard for the method by which it is obtained, used, or disclosed.[148] The Illinois BIPA defines "biometric identifiers" as a "retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry."[149] The BIPA specifically excludes from the definition of "biometric identifier," photographs, demographic data, and physical characteristics such as "height, weight, hair color, or eye color."[150]

[141] *See infra* notes 143–188 and accompanying text.

[142] *See infra* notes 189–203 and accompanying text.

[143] *See* Claypoole & Stoll, *supra* note 8, at 2 (noting Illinois BIPA's relative anonymity until five class actions brought by Illinois residents in 2015 claimed violations of the Illinois BIPA).

[144] *See infra* notes 147–159 and accompanying text.

[145] *See infra* notes 160–180 and accompanying text.

[146] *See infra* notes 181–188 and accompanying text.

[147] *See* Biometric Information Privacy Act, 740 ILL. COMP. STAT. §§ 14/1–14/99 (2009); Roberg-Perez, *supra* note 17, at 61 (noting that Illinois was the first state to pass comprehensive biometric data regulations in 2008).

[148] 740 ILL. COMP. STAT. § 14/10 (providing the definition of biometric information). Notably the Biometric Information Privacy Act ("BIPA")'s definition of biometric information excludes information "derived" from the types of identifiers that are excluded from the definition of biometric identifiers. *See id.*

[149] *See id.*

[150] *See id.* (listing the types of identifiers excluded from the definition of "biometric identifier" within the statute). Notably, biometric information collected from an individual that is subject to regulation under the Genetic Information Privacy Act or the Health Insurance Portability and Accountability Act is not included in the Illinois statute's definition of "biometric identifier." *See id.*

The BIPA contains five foundational requirements in regulating businesses' collection and use of biometric data.[151] First, businesses must, in writing, notify consumers and obtain informed written consent for collection of biometric data.[152] Furthermore, the notice must state the fact that biometric data is being collected or stored, and must also state the specific purpose and length of time for which the data is being collected, stored, and used.[153] Second, businesses are prohibited from selling or "otherwise profiting" from biometric data.[154] Third, the statute allows a limited right to disclosure in certain enumerated circumstances.[155] Fourth, retention of the data is permitted only until the initial purpose for collection of the information has been satisfied, or within three years of the data subject's last interaction with the business.[156] Fifth, the statute creates a private right for an individual to bring a cause of action to enforce violations of the Illinois BIPA.[157] Notably, Illinois is the only state with a biometric data regulation statute that provides individuals with such a private right of action.[158] Individuals may sue to recover the greater of actual damages or the statutory damages of $1,000 for each negligent violation of the statute and $5,000 for each intentional or reckless violation.[159]

2. The Rise of Class Actions Under the BIPA

Only in 2015 did the Illinois BIPA gain national recognition after five class action lawsuits were filed against Facebook and Shutterfly that claimed improper collection and use of Illinois residents' biometric data.[160] Four of these suits specifically claimed that Facebook's tagging suggestion feature violated the Illinois BIPA by collecting and retaining individuals' facial features

[151] *See* Claypoole & Stoll, *supra* note 8, at 2.

[152] *See* 740 ILL. COMP. STAT. § 14/15(b).

[153] *See id.* § 14/15(a).

[154] *See id.* § 14/15(c). The law does not directly specify the definition necessary for "otherwise profiting" for a violation of the statute. *See id.*

[155] *See id.* § 14/15(d) (listing the circumstances in which an entity may disclose collected biometric information including the individual's consent, completion of a financial transaction, requirement under a state or federal ordinance, or due to a warrant or court subpoena).

[156] *See id.* § 14/15(a) (detailing the measures required for retention and destruction of collected biometric information).

[157] *See id.* § 14/20.

[158] *See id.* (providing individuals with a private right to commence action under the Illinois BIPA); Capture or Use of Biometric Identifier Act, TEX. BUS. & COM. CODE ANN. § 503.001(b) (West 2017) (stating that to enforce a violation of the statute, the Texas attorney general may bring an action); H.B. 1493, 65th Leg., Reg. Sess. § 4(2) (Wash. 2017) (stating that the Washington statute may only be enforced by the attorney general).

[159] *See* 740 ILL. COMP. STAT. § 14/20 (listing an individual's right to bring a private cause of action and the potential recovery available). In addition to damages, an individual may collect reasonable attorney's fees and costs. *See id.*

[160] *See* Claypoole & Stoll, *supra* note 8, at 2 (noting Illinois BIPA's relative anonymity until five class actions brought by Illinois residents in 2015 claimed violations of the Illinois BIPA).

without their consent.[161] In *Norberg v. Shutterfly*, the plaintiff alleged that Shutterfly violated the BIPA by creating, collecting, and storing "face templates" of individuals captured from photographs submitted to Shutterfly.[162] Shutterfly challenged the class action on the basis that the Illinois BIPA excluded photographs from its definition of biometric identifiers.[163] The United States District Court of the Northern District of Illinois rejected Shutterfly's motion, reasoning that the Illinois BIPA's definition could reasonably include scans of facial geometry and images derived from photographs.[164]

Following the 2015 class action suits brought against Facebook and Shutterfly, the years 2016 and 2017 saw a massive increase in class actions regarding the Illinois BIPA.[165] Shifting from the consumer context to the employment

[161] *See* Complaint at 1, 8, Gullen v. Facebook Inc., No. 15-CV-07681 (N.D. Ill. Aug. 31, 2015) (claiming a violation of the BIPA because the plaintiff never consented to Facebook's tagging feature that scans photographs for biometric information, collects that data, and suggests individuals to "tag" or designate as persons in the photograph); Complaint at 1–2, 11, Patel v. Facebook Inc., 290 F. Supp. 3d 950 (N.D. Ill. 2015) (No. 15-CV-04265) (alleging Facebook violated § 15(b) of the BIPA for failing to comply with the statute's notice and consent requirements); Complaint at 7, 10–11, Pezen v. Facebook Inc., No. 15-CV-03484 (N.D. Ill. Apr. 21, 2015) (claiming a violation of the BIPA because Facebook failed to obtain notice and consent as required by the statute); Complaint at 15–16, Licata v. Facebook Inc., No. 15-CH-05427 (N.D. Ill. Apr. 1, 2015) (claiming violations of the BIPA due to Facebook's noncompliance with the statute's notice and consent requirements); *see also* Claypoole & Stoll, *supra* note 8, at 3 (noting that the plaintiffs in each class action claimed they were not Facebook users at the time Facebook captured and stored their biometric information).

[162] *See* Norberg v. Shutterfly, Inc., 152 F. Supp. 3d 1104, 1106 (N.D. Ill. June 2015) (noting that the plaintiffs were not consumers of Shutterfly).

[163] *See id.* at 1105–06 (stating that the defendants brought a Rule 12(b)(6) motion to dismiss and claimed that biometrics derived from photographs are outside the scope of Illinois BIPA's definition of biometric identifiers).

[164] *See id.* at 1106 (denying the defendant's motion to dismiss because the plaintiff stated a viable claim for relief under the Illinois BIPA in consideration of the Illinois BIPA's definition of biometric identifiers); *see also In re* Facebook Biometric Info. Privacy Litig., 185 F. Supp. 3d 1158, 1171–72 (N.D. Ill. 2016) (denying the defendant's motion to dismiss because images derived from photographs could reasonably fall within the scope of the Illinois BIPA's definition of biometric identifiers).

[165] *See* Carley Daye Andrews et al., K&L GATES LLP, *Litigation Under Illinois Biometric Information Privacy Act Highlights Biometric Data Risks* (Nov. 7, 2017), http://www.klgates.com/litigation-under-illinois-biometric-information-privacy-act-highlights-biometric-data-risks-11-07-2017/ [https://perma.cc/U8DY-J84S] (describing the increasing trend of class actions brought under the Illinois BIPA); Daniel B. Pasternak, *Illinois Employers Face a Recent Rash of Class Action Lawsuits Filed Under State Biometric Information Privacy Law*, NAT'L L. REV. (Nov. 27, 2017), https://www.natlawreview.com/article/illinois-employers-face-recent-rash-class-action-lawsuits-filed-under-state [https://perma.cc/87E9-G8X2] (stating that at least thirty suits claiming violations of the BIPA have been brought in Illinois since August 2017). In response to the rising number of class actions, the Illinois House and Senate have put forward bills to amend the scope of the BIPA. *See* S.B. 3053, 100th Gen. Assemb., Reg. Sess. (Ill. 2018) (proposing amendments to the BIPA); H.B. 5103, 100th Gen. Assemb., Reg. Sess. (Ill. 2018) (proposing amendments to the BIPA). One proposal exempts the application of the BIPA to private entities if the collected biometric information is used exclusively for employment, human resources, fraud prevention, or security purposes. Ill. S.B. 3053 (proposing amendments to limit the scope of application of the BIPA to private entities); Ill. H.B. 5103 (proposing amendments to limit the scope of application of the BIPA to private entities). The Senate bill further excludes from the definition of biometric identifiers, physical or digital photographs and data

context, the more recent class actions nearly all center on employers' use of biometric technology to track employee work hours and activities.[166] The claims range from alleging that employers did not inform their employees about the businesses' policies for the use, retention, and destruction of collected fingerprint data to claiming that the employers failed to obtain employees' written consent before collecting, using, or storing the biometric information.[167] In one particular class action suit, *Howe v. Speedway LLC*, the plaintiffs claimed that the employer, Speedway LLC, improperly disclosed the employees' biometric fingerprint data to an "out-of-state-vendor," the supplier of the fingerprint time-tracking machines.[168]

Despite the rise in number of class action lawsuits, plaintiffs continue to face a number of obstacles in bringing a suit under the BIPA including issues of standing and the constitutionality of the statute.[169] Defendants in these class actions have relied on the United States Supreme Court's ruling in *Spokeo v. Robins* to claim that the plaintiffs have not sufficiently alleged an injury for the

generated from physical or digital photographs. Ill. S.B. 3053 (proposing exclusions to the definition of biometric identifier). As of Fall 2018, the bills are still in committee. *See Bill Status of SB3053*, ILL. GEN. ASSEMBLY http://www.ilga.gov/legislation/BillStatus.asp?GA=100&DocTypeID=SB&DocNum=3053&GAID=14&SessionID=91&LegID=110583 [https://perma.cc/47YG-TU5J] (noting that the bill is re-referred to Assignments); *Bill Status of HB5103*, ILL. GEN. ASSEMBLY, http://www.ilga.gov/legislation/BillStatus.asp?DocNum=5103&GAID=14&DocTypeID=HB&LegId=110644&SessionID=91&GA=100 [https://perma.cc/YR3K-W6Z8] (noting that the bill is re-referred to the Rules Committee).

[166] *See* Complaint at 2–3, Fields v. ABRA Auto Body & Glass LP, No. 2017-CH-12271 (Ill. Cir. Ct. Sept. 8, 2017) [hereinafter Fields Complaint] (detailing a class action by employees of ABRA Auto Body & Glass claiming that the company violated the Illinois BIPA by failing to provide notice and obtain written consent required under the statute to collect and store employee fingerprints to monitor checking in and out of work); Complaint at 6–8, Knobloch v. Chi. Fit Ventures LLC, No. 2017-CH-12266 (Ill. Cir. Ct. Sept. 8, 2017) [hereinafter Knobloch Complaint] (detailing a class action suit brought by members of a chain of exercise facilities, Crunch Fitness, claiming that the gym violated the Illinois BIPA both by collecting members' fingerprint data without proper notice and consent, and illegally retaining that data); Andrews, *supra* note 161(listing the different targets of the BIPA class action suits, including retailers, online service providers, to employers); *see also* Adam Janofsky, *Fingerprint-Scanning Time Clocks Spark Privacy Lawsuits*, WALL STREET J. (Jan. 11, 2018), https://www.wsj.com/articles/biometric-time-clocks-spark-a-wave-of-privacy-lawsuits-1515364278 [https://perma.cc/SUT6-5UBE] (noting recent suits against fifty companies claiming violation of the Illinois BIPA due to use of biometric technology that scans fingerprints).

[167] *See* Fields Complaint, *supra* note 166, at 2–3 (claiming violations of the BIPA for lack of notice and written consent); Knobloch Complaint, *supra* note 166, at 6–8, (claiming violations of the BIPA for lack of notice, proper consent, and postage of a data retention schedule).

[168] *See* Complaint at 1–3, 8–9, Howe v. Speedway LLC, No. 2017-CH-11992 (Ill. Cir. Ct. Sept. 1, 2017) [hereinafter Howe Complaint] (detailing a class action by employees of Speedway claiming that the company's collection and storage of employee fingerprints to authenticate employees violated the Illinois BIPA by failing to adhere to the statute's notice, consent, and data retention requirements and by allegedly disclosing the data to a third party).

[169] *See* Pasternak, *supra* note 165 (describing the issues within the BIPA that are being litigated in 2017 and likely to have an effect on subsequent cases).

court to grant Article III standing.[170] Under *Spokeo*, the Court held that "allegations of bare procedural violations of a federal statute," without evidence of harm, do not satisfy the concrete injury requirement of Article III.[171] In a recent notable case, *Santana v. Take-Two Interactive Software, Inc.*, the United States Court of Appeals for the Second Circuit affirmed, on grounds of lack of Article III standing, the dismissal by the United States District Court for the Southern District of New York of a claim that the defendant, Take-Two Inc., violated the Illinois BIPA.[172] Take-Two Inc., a videogame maker, created a basketball video game platform that enabled users to create personalized virtual avatars by using the game console's camera to scan the player's face and head.[173] In addition to claiming that the defendant did not comply with the BIPA's written data retention requirements, the plaintiffs claimed that the defendant failed to maintain adequate data security by transferring "unencrypted scans of face geometry" on the Internet rather than on a secure network and by failing to subject the stored face scans to de-identification methods such as anonymization.[174] The Second Circuit held the plaintiffs' claim failed to state a "risk of real harm" that the plaintiffs' biometric information would be "improperly accessed by third parties."[175] A further distinction arose in the Illinois Appellate Court case, *Rosenbach v. Six Flags Entertainment Corp.*, where the court found that plaintiffs are only "aggrieved" as required under the statute if they state an actual injury or harm, and not just a mere "technical violation."[176]

[170] *See* Spokeo v. Robins, 136 S. Ct. 1540, 1547–50 (2016) (listing the pleading requirements a plaintiff must meet to be granted Article III standing); *see also* Lujan v. Defs. of Wildlife, 504 U.S. 555, 559 (1992) (holding that Article III limits the authority of federal courts to decide "cases and controversies"). Under *Lujan*, sufficient standing requires three elements: (1) a concrete injury; (2) the injury is fairly traceable to actions of the defendant; and (3) it must be likely, and not speculative, that the injury is redressable by a favorable holding. *See* 504 U.S. at 560–61.

[171] *See Spokeo*, 136 S. Ct. at 1549 (explaining that a "risk of real harm" may be sufficient to satisfy the element of concrete injury but a "bare procedural violation" absent a concrete harm is not sufficient).

[172] *See* Santana v. Take-Two Interactive Software, Inc., 717 F. App'x 13, 16–17 (2d Cir. 2017) (stating that the plaintiffs' claim failed to sufficiently state a concrete injury and therefore lacked Article III standing).

[173] *See id.* at 13–14 (describing the 3-D scanning mechanism that allows players of Take-Two's game to create individualized avatars for use in the game only after the user first agrees to the End User License Agreement).

[174] *See id.* at 14, 16 (listing the claims against the defendant including the violation of Illinois BIPA's requirement that businesses use the "reasonable standard of care within [the] industry" to ensure the security of the biometric data collected and used by the business); *see also* 740 ILL. COMP. STAT. § 14/15(e) (2018) (listing the data security requirements for businesses that collect and use biometric information).

[175] *See Santana*, 717 F. App'x at 16–17 (refusing to find that an actual data breach need occur for there to be a "risk of real harm" to confer a sufficient injury to grant Article III standing); *see also Spokeo*, 136 S. Ct. at 1549 (stating the standard to find a "risk of real harm" for Article III standing).

[176] *See* Rosenbach v. Six Flags Entm't Corp., No. 2-17-0317, 2017 WL 6523910, at *4–5 (Ill. App. Ct. 2d Dist. Dec. 21, 2017); *see also Spokeo*, 136 S. Ct. at 1549 (providing that an injury sufficient for Article III standing may include a "risk of real harm").

The discrepancy between the harm required for a plaintiff to meet Article III standing versus the statutory "aggrieved" person standard has yet to be resolved.[177]

Notably, some courts have granted Article III standing based upon an interpretation that the purpose of the BIPA is to prevent personal invasions of privacy as opposed to merely improper disclosure or misuse of biometric data.[178] The United States District Court for the Northern District of Illinois, in *Monroy v. Shutterfly, Inc.*, denied the defendant's motion to dismiss by finding that the BIPA did not require claims of actual harm and therefore, plaintiffs had Article III standing.[179] Whereas in *Monroy* the biometric data obtained by the defendant was collected from a third party without the consent of the plaintiff, in *Santana* and *Rosenbach*, the plaintiffs voluntarily gave their data to the defendants.[180]

3. The Texas CUBI vs. The Illinois BIPA

Following the implementation of the Illinois BIPA, Texas enacted a state biometric law, the CUBI, in § 503.001 of the Texas Business and Commercial Code in the year 2009.[181] The statute provides that "biometric identifiers" include a "retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry."[182] Similar to the Illinois BIPA, the Texas CUBI contains several foundational requirements.[183] The Texas CUBI requires businesses to provide

[177] *See Santana*, 717 F. App'x at 16–17 (stating that the plaintiffs' claim failed to sufficiently state a concrete injury and therefore lacked Article III standing); Howe v. Speedway LLC, No. 17-cv-07303, 2018 WL 2445541, at *4 (N.D. Ill. May 31, 2018) (noting the distinction between Article III and statutory standing but only addressing whether the plaintiff suffered an injury in fact for Article III standing); *Rosenbach*, 2017 WL 6523910, at *4–5 (finding that a party is not "aggrieved" under the terms of the BIPA statute if the party only claims a procedural violation without any injury or harmful consequence); *see also* Rosenbach v. Six Flags Entm't Corp., 98 N.E. 3d 36 (Ill. App. Ct. 2d Dist. May. 2018) (allowing a petition for leave to appeal).

[178] *See* Monroy v. Shutterfly, Inc., No. 16-C-10984, 2017 WL 4099846, at *1, *8–9 (N.D. Ill. Sept. 15, 2017) (stating that the question of whether the plaintiff suffered actual damages is not determinative where the plaintiff claims an invasion of privacy).

[179] *See id.* at *1, *8–9 (claiming that the defendant allegedly violated the BIPA after collecting and storing biometric data of the plaintiff, without his consent, from a photograph uploaded by a third party).

[180] *See Santana*, 717 F. App'x at 13–14 (describing the 3-D scanning mechanism that allows players of Take-Two's game to create individualized avatars for use in the game only after the user first agrees to the End User License Agreement); *Monroy*, 2017 WL 4099846, at *1 (claiming that a Shutterfly user uploaded a photograph of the plaintiff onto the defendant's site without the plaintiff's knowledge or consent); *Rosenbach*, 2017 WL 6523910, at *2 (describing the fingerprint-scanning mechanism employed by the defendant in order to authenticate season-pass holders).

[181] TEX. BUS. & COM. CODE ANN. § 503.001 (2017); *see* Tumeh, *supra* note 18 (noting that Illinois was the first to adopt a biometric regulation statute in 2008, followed by Texas).

[182] TEX. BUS. & COM. CODE ANN. § 503.001(a).

[183] *See* Claypoole & Stoll, *supra* note 8, at 3 (listing fundamental provisions contained in the Texas statute). *See generally* 740 ILL. COMP. STAT. § 14/1–14/99; TEX. BUS. & COM. CODE ANN. § 503.001.

notice and obtain informed consent before collection or use of an individual's biometric data.[184] Unlike in Illinois, however, no further specific notice and consent requirements are mandated in Texas.[185] The Texas CUBI prohibits businesses from selling, leasing, or disclosing biometric data, with some exceptions such as with consent of the data subject, when disclosure is required under another law, or when disclosure is required pursuant to a warrant.[186] The statute additionally imposes retention limitations where destruction is required, "within a reasonable time," but no later than one year after the initial collection of the data.[187] Notably, unlike the Illinois BIPA, the Texas CUBI does not afford individuals a private right to action, but rather enforcement of the statute can only be brought through the state attorney general.[188]

B. Washington's Biometric Data Statute

In 2017, Washington became the third state to enact a biometric data protection statute.[189] The Washington statute defines a "biometric identifier" as "data generated by automatic measurements of an individual's biological characteristics, such as fingerprint, voiceprint, eye retinas, iris, or other unique biological patterns or characteristics that is used to identify a specific individual."[190] In contrast to the Illinois and Texas statutes, Washington's definition of "biometric identifier" does not include a record of "hand or face geometry" and excludes physical or digital photographs.[191] The Washington definition is

[184] TEX. BUS. & COM. CODE ANN. § 503.001(b) (listing the notice and consent requirements for collection and use of an individual's biometric information).

[185] *Compare* 740 ILL. COMP. STAT. § 14/15(a) (stating to specifically satisfy the notice requirement an entity must state the fact that biometric data is being collected or stored and the specific purpose and length of time the data is being collected, stored, and used), *with* TEX. BUS. & COM. CODE ANN. § 503.001(b).

[186] TEX. BUS. & COM. CODE ANN. § 503.001(c)(1).

[187] *Id.* § 503.001(c)(2–3), (c-1).

[188] *Compare* 740 ILL. COMP. STAT. § 14/20 (providing that an individual whose rights have been violated under the BIPA has a private right of action to enforce those claims in court), *with* TEX. BUS. & COM. CODE ANN. § 503.001(d) (stating that to enforce a violation of the statute, the Attorney General may bring an action with civil penalties not to exceed more than $25,000 for each violation). As the Texas statute does not contain a private cause of action, there have not been any class actions like those brought in Illinois. *See* TEX. BUS. & COM. CODE ANN. § 503.001(d).

[189] *See generally* H.B. 1493, 65th Leg., Reg. Sess. (Wash. 2017) (noting that the statute was enacted in 2017).

[190] *Id.* § 3(1).

[191] *See* 740 ILL. COMP. STAT. § 14/10 (2008) (listing the types of identifiers, including scans of hand or face geometry, in the definition of "biometric identifier" under the BIPA); TEX. BUS. & COM. CODE ANN. § 503.001(a) (listing the types of data, including records of hand or face geometry, that are included within the definition of "biometric identifier" under the Texas statute); H.B. 1493, 65th Leg., Reg. Sess. (Wash. 2017) § 3(1) (excluding physical or digital photographs from the definition of biometric identifier). *See generally* Tumeh, *supra* note 18, at 1 (noting the differences between the Illinois, Texas, and Washington definitions of biometric identifiers). In Illinois, the inclusion of scans of "hand or face geometry" and the U.S. District Court for the Northern District of Illinois's decision

instead limited to biometric information that has been "enrolled."[192] A business "enrolls" biometric information if it captures an individual's biometric identifier, converts it into a "reference template that cannot be reconstructed into the original output image," and stores that template in a database that "matches the biometric identifier to a specific individual."[193]

Furthermore, Washington's statute attempts to preserve businesses' use of biometric data by regulating only the collection, retention, use, and disclosure of biometric identifiers for a "commercial" purpose.[194] A commercial purpose is defined as "a purpose in furtherance of the sale, lease, or distribution of biometric data to third parties for the purpose of marketing goods and services which are unrelated to the initial transaction in which a person first gains possession of an individual's biometric identifier."[195] Notably, these requirements expressly exclude businesses' collection of biometric data for "security or law enforcement" purposes, as defined as "preventing shoplifting, fraud, or any other misappropriation or theft of a thing of value."[196] The Illinois BIPA does not limit the scope of regulation to a commercial purpose and further directly states the need for biometric regulation due to increased use of biometrics in "security screenings."[197] Although the Texas biometric law does include a commercial purpose limitation, unlike Washington, commercial purpose is left

to include data generated from photographs in the BIPA's definition of biometric identifiers gave rise to most of the recent class actions brought under the Illinois BIPA. *See In re Facebook*, 185 F. Supp. 3d at 1171 (denying the defendant's motion to dismiss, as images derived from photographs could reasonably fall within the scope of Illinois BIPA's definition of biometric identifiers); *Norberg*, 152 F. Supp. 3d at 1106 (denying the defendant's motion to dismiss because the plaintiff stated a viable claim for relief under the Illinois BIPA in consideration of the Illinois BIPA's definition of biometric identifiers).

[192] *See* WASH. REV. CODE § 19.375.020(1)–(2) (2018) (stating the notice, consent, and opt-out requirements a "person" must abide by before enrolling an individual's biometric identifier in a "database for a commercial purpose").

[193] Wash. H.B. 1493 § 3(5) (defining the term "enroll" as it is used in the statute).

[194] *See* WASH. REV. CODE § 19.375.020(1), (6)–(7) (limiting regulation to biometric identifiers that are "enrolled" for a "commercial" purpose, creating an exception to regulation of biometric data collected for a "security" purpose). *Contra* 740 ILL. COMP. STAT. § 14/15(b) (listing the broad requirements for an entity's collection, receipt, capture, or purchase of biometric information *for any purpose*).

[195] Wash. H.B. 1493 § 3(4) (listing the definition of "commercial purpose" within the statute).

[196] *Id.* § 3(8) (defining "security or law enforcement" purposes within the statute).

[197] *Compare* 740 ILL. COMP. STAT. §§ 14/5(a), 14/15(b)–(c) (noting the increased use of biometrics in "security screenings" and noting that a business must comply with the BIPA regulations regarding collection and use of biometric data for all purposes), *with* WASH. REV. CODE § 19.375.020(1), (6)–(7) (limiting regulation to biometric identifiers that are "enrolled" for a "commercial" purpose, creating an exception to the regulation for biometric data collected for a "security" purpose).

undefined and the question of whether it includes security purposes has yet to be addressed.[198]

The Washington statute imposes varying notice and consent requirements in "context-dependent" circumstances.[199] Businesses that seek to share or sell individuals' biometric data for commercial purposes must first provide notice, and either obtain consent or provide a mechanism for individuals to opt out of the subsequent use of the data for commercial purposes.[200] The statute imposes data retention limitations for a time period "no longer than is reasonably necessary" to comply with the law or a court order, protect against crime, fraud, or liability, and to provide individuals with the service for which the biometric data was initially obtained.[201] Similar to Texas, and unlike Illinois, Washington does not afford individuals a private right to action.[202] Rather, enforcement of Washington's statute can only be brought by the state attorney general as a violation of Washington's Unfair Business Practices-Consumer Protection Act.[203]

III. SEEKING BALANCE: PREVENTING BIG DATA DISCRIMINATION AND PRESERVING BUSINESSES' USE OF BIOMETRIC TECHNOLOGY TO ENHANCE SECURITY

A business's collection and use of biometric data presents both risks and benefits in the context of today's unregulated data broker landscape.[204] A primary danger is the potential for individuals' biometric data to be subject to commercial misuse.[205] One form of commercial misuse is the aggregation of biometric data with other PII or non-PII to opaquely discriminate against con-

[198] *See* TEX. BUS. & COM. CODE ANN. § 503.001(b)–(c) (regulating an entity's capture and possession of biometric data for commercial purposes but leaving the term undefined in the statute); Tumeh, *supra* note 18 (noting the lack of clarity surrounding the Texas statute's use of "commercial purpose").

[199] WASH. REV. CODE § 19.375.020(2) (noting that sufficient notice and consent is "context-dependent" and that notice is adequate if by a "procedure reasonably designed to be readily available to affected individuals").

[200] *Id.* § 19.375.020(3), (5).

[201] *Id.* § 19.375.020(4).

[202] *Compare* TEX. BUS. & COM. CODE ANN. § 503.001(d) (stating that in order to enforce a violation of the statute, the attorney general may bring an action), *and* Wash. H.B. 1493 § 4(2) (stating that the Washington statute may only be enforced by the attorney general), *with* 740 ILL. COMP. STAT. § 14/20 (providing individuals with a private right of action).

[203] *See* Wash. H.B. 1493 § 4(2) (stating that the Washington statute may only be enforced by the attorney general under chapter 19.86 of the consumer protection act).

[204] *See* FTC DATA BROKERS, *supra* note 9, at 13–14, 47 (reporting that consumers' data is purchased by data brokers from commercial entities such as retailers and financial services companies and used to create both beneficial and harmful marketable categories).

[205] *See* Barocas & Selbst, *supra* note 4, at 677 (affirming data mining's potential to segregate individuals within historically protected classes through automated processes); FTC DATA BROKERS, *supra* note 9, at 20, 47 (describing the marketable categories created and sold by data brokers that have immense potential to cause harm to consumers).

sumers.[206] Here, as is common for the data broker industry, consumers are left without recourse to alter, control, or protest their harmful data profiles or categorizations.[207] Despite these potential risks, over-regulation of biometric data may disincentivize technological development and businesses' use of biometric data to enhance security.[208] Although federal law in the United States is not entirely without data privacy regulation, regulations at the federal level are industry-specific and inconsistent across sectors.[209] As biometric technology has an increasingly daily impact upon individuals across the United States, and as more states have stepped up to adopt biometric data laws, there must be some balance and consistency to the scope of regulation.[210] Section A of this Part critiques the Illinois BIPA as overly broad and unduly burdensome on businesses.[211] Section B of this Part argues that as states look to implement statutes that regulate businesses' interaction with biometric data, they should look to model Washington's biometric statute because it provides a better balance of protecting both consumer and business interests.[212] Furthermore, as technology increasingly enables the dissemination of data across the United States, Congress should implement a comprehensive federal statute that regulates businesses' collection, use, and disclosure of biometric data.[213]

[206] *See* Goodman, *supra* note 5 (noting that biometric technology has the ability to collect an individual's sensitive information such as race, gender, age, economic class or health conditions); FTC DATA BROKERS, *supra* note 9, at 20, 47 (explaining that the different categorizations created potential discrimination by differentiating between consumers based on a variety of factors from race, age, educational level, net worth, to specific health conditions).

[207] *See* FTC DATA BROKERS, *supra* note 9, at 49 (stating for products such as insurance, data brokers do not allow consumers to have access to the data collected about them and specific data that is accessible to consumers is often difficult, if not impossible, for consumers find).

[208] *See* Contreras, *supra* note 133 (reporting that business advocates critique Illinois's privacy statutes as imposing "chilling effect" on technological development). According to Carl Szabo of NetChoice, some already developed facial recognition technology cannot be used in Illinois. *See id.* (noting the comprehensive scope of Illinois's BIPA); Meyer, *supra* note 6 (quoting Szabo of NetChoice that "requiring consent before every use of the technology would eliminate many of the benefits of facial recognition").

[209] *See* SOLOVE & SCHWARTZ, *supra* note 98, at 34–35 (listing a number of United States federal privacy laws that are specific to sectors such as healthcare, credit reporting, education, and financial industries); Rostow, *supra* note 102, at 676 (describing the "patchwork" of commercial privacy regulations in U.S. federal law); Claypoole & Stoll, *supra* note 8 (providing examples of several industry-specific federal laws that govern private and public collection and use of an individual's biometric identification data).

[210] *See infra* notes 214–251 and accompanying text; *see also* Roberg-Perez, *supra* note 17, at 64 (noting that as ease of data dissemination increases, an issue arises if an individual's data is compromised because it could be subject to different levels of protection depending on the differing jurisdiction's regulations). Data dissemination on the Internet is "predicted to exceed 2.3 zettabytes annually within the next three years." Roberg-Perez, *supra* note 17, at 63. A zettabyte is a unit representing digital information, that is equivalent to 2^{70} bytes. *See Zettabyte*, OXFORD ENG. DICTIONARY (2d ed. 2014.

[211] *See infra* notes 214–238and accompanying text.

[212] *See infra* notes 239–251 and accompanying text.

[213] *See infra* notes 246–251 and accompanying text.

A. Inability to Operate: How the Illinois BIPA Inhibits Businesses' Use of Biometric Technology for Security Purposes

To provide better security and service to consumers, businesses develop and implement biometric technologies including fingerprint, facial and voice recognition, iris scanning, and use of selfies as innovative methods of authentication.[214] The Illinois BIPA's attempt to protect individual privacy, however, provides a nearly unlimited scope of regulation that could stymie growth of the data security industry and thwart the purpose of many new technologies that provide security through biometric identification.[215] For example, the company Nest, owned by Alphabet, Google's parent company, produces a doorbell equipped with a camera with facial recognition technology that can be trained to identify familiar and unfamiliar faces.[216] Nest sells the doorbell-camera product in Illinois but disables the facial recognition feature.[217] Nest states that due to Illinois legislation, the feature is disabled in that state as a preventative measure.[218] The purpose of the facial recognition feature in this product is to distinguish between known and unknown faces to provide homeowners with greater security.[219] Providing written notice and obtaining written consent from any individual that happens upon one's front porch hinders the ultimate purpose of this facial recognition security feature.[220] This is a clear example of

[214] *See* Larduinat, *supra* note 6 (crediting the rise in biometric technology to the complementary benefits of increased consumer security and access to businesses' services and products); Meyer, *supra* note 6 (stating that businesses such as Facebook, Microsoft, and Google have begun researching and implementing biometric technology).

[215] *See* Biometric Information Privacy Act, 740 ILL. COMP. STAT. § 14/15(b) (2018) (listing the broad requirements for an entity's collection, receipt, capture, or purchase of biometric information); Contreras, *supra* note 133 (reporting that business advocates critique Illinois privacy statutes as imposing a technological development "chilling effect"); *Learn More About Familiar Face Detection and Managing Your Library*, NEST SUPPORT, https://nest.com/support/article/Familiar-face-alerts [https://perma.cc/3V49-A2V8] [hereinafter *Nest Familiar Faces*] (noting that the facial recognition feature of a doorbell security camera, used to identify unfamiliar faces, is unavailable to consumers in Illinois).

[216] *See Nest Familiar Faces*, *supra* note 215 (stating that Nest's "familiar face detection feature" can be trained to recognize familiar faces); *see also* Ally Marotti, *Google's Art Selfies Aren't Available in Illinois. Here's Why*, CHI. TRIB. (Jan. 17, 2018), http://www.chicagotribune.com/business/ct-biz-google-art-selfies-20180116-story.html (stating that the company Nest is owned by Alphabet).

[217] *See Nest Familiar Faces*, *supra* note 215 (noting that Nest's "familiar face detection feature" is disabled on Nest cameras used in Illinois).

[218] *See id.*

[219] *See id.* (describing how Nest's "familiar face detection feature" can be trained to recognize familiar faces and reject unknown faces and thereafter alert the homeowner to the familiarity of the face).

[220] *See id.* (explaining that use of the feature and compliance with the law in some states may require that individuals obtain consent before the doorbell camera identifies people).

both businesses and consumers being deprived of the use of biometric identification technology to enhance security.[221]

As further evidenced by the recent Illinois class actions, application of the BIPA is overly broad and has had unintended consequences.[222] In some of these cases, although the plaintiffs did not claim improper use of biometric data or disclosure due to a data breach, the courts granted Article III standing based upon the interpretation that the purpose of the BIPA is to prevent personal invasions of privacy as opposed to merely improper disclosure or misuse of biometric data.[223] The effect of the Illinois BIPA is particularly harsh when a business obtains the biometric data of an individual who did not personally provide their own biometrics.[224] For example, in *Monroy v. Shutterfly*, a Shutterfly user uploaded a group photo from which the defendant, Shutterfly, obtained the biometric information of the plaintiff, who was not a Shutterfly user, without his knowledge or consent.[225] In all situations, the BIPA requires that written notice be provided and written consent be obtained before collection of biometric identifiers.[226] If businesses using biometric technology do not implement means to provide written notice and to obtain written consent from unknowing individuals, they could be in violation of the BIPA.[227]

In other cases, the courts dismissed class actions for lack of Article III standing or failure to meet the "aggrieved" standard under the state statute.[228]

[221] *See id.* (stating that no consumer in Illinois will have access to the facial recognition feature on the doorbell camera product).

[222] *See* Fields Complaint, *supra* note 166, at 2–3 (detailing class action by employees of ABRA Auto Body & Glass, claiming that the company's collection and storage of employee fingerprints to monitor checking in and out of work violated the Illinois BIPA in that the company failed to obtain the notice and written consent required under the statute); Knobloch Complaint, *supra* note 166, at 6–8 (detailing a class action suit by members of a chain of exercise facilities, Crunch Fitness, claiming that the gym's collection of members' fingerprints violated the Illinois BIPA when the facilities failed to obtain the notice and consent, and improperly retained data contrary to policies required under the statute).

[223] *See* Patel v. Facebook Inc., 290 F. Supp. 3d 950, 950–952, 953–954 (N.D. Cal. 2018) (consolidating three class action suits against Facebook and finding standing where the plaintiffs had not consented to the collection and storage of biometric data); Monroy v. Shutterfly, Inc., No. 16-C-10984, 2017 WL 4099846, at *1, *8–9 (N.D. Ill. Sept. 15, 2017) (stating that an invasion of privacy claim does not turn on whether the plaintiff suffered actual damages).

[224] *See Monroy*, 2017 WL 4099846, at *1, *8–9 (stating that the question of whether the plaintiff suffered actual damages is not determinative when the plaintiff claims an invasion of privacy due to the defendant's collection of the plaintiff's biometric data without his knowledge or consent).

[225] *See id.* at *1 (describing how the business obtained the plaintiff's biometric data).

[226] *See* 740 ILL. COMP. STAT. § 14/15(b) (listing the requirements regarding an entity's collection, receipt, capture, or purchase of biometric information).

[227] *See Monroy*, 2017 WL 4099846, at *1, *8–9 (allowing the plaintiff's suit to go forward without a claim of actual harm or damages).

[228] *See* Santana v. Take-Two Interactive Software, Inc., 717 F. App'x 13, 16–17 (2d Cir. 2017) (stating that the plaintiffs claim failed to sufficiently state a concrete injury and therefore lacked Article III standing); Rosenbach v. Six Flags Entm't Corp., No. 2-17-0317, 2017 WL 6523910, at *4–5 (Ill. App. Ct. 2d Dist. Dec. 21, 2017) (finding that a party is not "aggrieved" under the terms of the

Notably, *Santana v. Take-Two Interactive Software, Inc.*, and *Howe v. Speedway*, concern issues of disclosure to third parties and not merely notice and consent violations, unlike the majority of class actions under the Illinois BIPA.[229] In both *Santana* and *Howe*, the plaintiffs respectively claimed that the defendants failed to properly protect the individuals' biometric data from access by third parties and improperly distributed the individuals' biometric data directly to a third party.[230] The United States Court of Appeals for the Second Circuit, in *Santana* held that the claim failed to state a "risk of real harm" that the plaintiff's biometric information would be "improperly accessed by third parties."[231] In *Howe*, the United States District Court for the Northern District of Illinois found that the plaintiff alleged a mere procedural violation and therefore did not state an injury sufficient to establish Article III standing, and remanded the case back to state court.[232] Despite the plaintiff's claim that the defendants disclosed employee biometric data, fingerprints, to an out-of-state third party vendor, the court stated that the complaint did not indicate that the defendant "released, or allowed anyone to disseminate," the biometric data..[233] Additionally, the court distinguished the facts in *Monroy* and similar cases in which Article III standing was granted, stating that in those cases, the bio-

BIPA statute if the party only claims a procedural violation without any injury or harmful consequence); *see also* Spokeo v. Robins, 136 S. Ct. 1540, 1549 (2016) (noting that a "risk of real harm" may be sufficient to satisfy the element of concrete injury but a "bare procedural violation" absent a concrete harm, is not sufficient).

[229] *See Santana*, 717 F. App'x at 13, 16 (claiming that the defendant failed to maintain adequate data security by transferring "unencrypted scans of face geometry" on the Internet rather than on a secure network); Howe Complaint, *supra* note 168, at 1–3, 8–9 (detailing a class action suit by employees of Speedway, claiming that the company's practice of collecting and storing employee fingerprints to authenticate employees violated the Illinois BIPA by failing to adhere to the statute's notice, consent, and data retention requirements and further by allegedly leading to disclosure of the data to a third party).

[230] See *Santana*, 717 F. App'x at 13, 16–17 (alleging that the defendants transferred "unencrypted scans of face geometry" on the Internet rather than on a secure network); Howe Complaint, *supra* note 168, at 3 (claiming the defendant improperly disclosed the employees' biometric fingerprint data to an "out-of-state third-party vendor").

[231] See *Santana*, 717 F. App'x at 16–17 (finding that the defendant's failure to maintain the plaintiff's data with a "reasonable standard of care" was not a sufficient "harm" under the statute). Notably, the Second Circuit specifically refused to find that an actual data breach need occur for there to be a "risk of real harm" to confer a sufficient injury to grant Article III standing. *Id.*; *see also Spokeo*, 136 S. Ct. at 1549 (determining the concrete injury standard for Article III standing).

[232] *See* Howe v. Speedway LLC, No. 17-cv-07303, 2018 WL 2445541, at *6–7 (N.D. Ill. May 31, 2018) (stating that the plaintiff did not allege an injury-in-fact sufficient to find Article III standing). The court noted the distinction between Article III standing and statutory standing. *See id.* at *4.

[233] *See id.* (stating that the defendant did not improperly disclose the plaintiff's data to a third-party); Howe Complaint, *supra* note 168, at 3 (alleging that the defendants violated the BIPA by disclosing biometric data to a third party); *see also* Matthew Hector, *Illinois' Biometric Privacy Law Back in the News*, ILL. BAR J., Dec. 2017, at 10, https://www.isba.org/ibj/2017/12/lawpulse/illinois biometricprivacylawbacknews [https://perma.cc/8QMU-V2CN] (stating that a class action against L.A. Tan Enterprises settled for $1.5 million after the plaintiffs claimed the business violated the BIPA by disclosing consumers' fingerprint scans to an out-of-state vendor).

metric data collection was entirely non-consensual whereas in *Howe*, any reasonable person would have known upon voluntarily scanning their fingerprint that biometric data was being collected. [234] Article III standing limitations, at least for some bare procedural violations, appear to serve as a judicial counterweight on Illinois's nearly unlimited scope of regulation of businesses' implementation and use of biometric technology.[235]

Despite the fact that some courts have taken a more relaxed position regarding the requirements of the BIPA, ambiguity within various terms of the statute are still at issue.[236] The intention of the statute, the primacy of individual privacy, is however, sufficiently clear.[237] Should these issues go before the Supreme Court, the Court could rule in line with the words and intention of the statute, thereby solidifying its overly broad and burdensome impact upon businesses.[238]

B. Allowing Biometric Technology for Security: State and Federal Regulation Should Model Washington's Statute

The Washington statute's "commercial purpose" limitation to the regulation of biometric data offers a better balance between consumer and business interests.[239] The statute explicitly excludes regulation of biometric information

[234] *See Howe*, 2018 WL 2445541, at * 5–6 (differentiating cases where the collection and storage of an individual's biometric data without their knowledge and consent could be a sufficient injury for Article III standing); *Monroy*, 2017 WL 4099846, at *1, *8–9 (allowing the plaintiff's suit to go forward without a claim of actual harm or damages).

[235] *See Spokeo*, 136 S. Ct. at 1549 (noting that a "bare procedural violation" absent a concrete harm, is not sufficient); *Santana*, 717 F. App'x at 16–17 (finding that failure to provide consumers with data retention policies was not a harm sufficient to confer standing); *Rosenbach*, 2017 WL 6523910, at *2, *5 (finding that failure to obtain written consent and to disclose retention policies was not a harm sufficient to confer standing); *see also* Howe Complaint, *supra* note 168, at 3 (alleging that the defendants violated the statute by disclosing biometric data to a third party).

[236] *See Santana*, 717 F. App'x at 13, 16–17 (stating that the plaintiff's claim failed to sufficiently state a concrete injury and therefore lacked Article III standing); *Rosenbach*, 2017 WL 6523910, at *4–5 (finding that a party is not "aggrieved" under the terms of the BIPA statute if the party only claims a procedural violation without any injury or harmful consequence); Howe Complaint, *supra* note 168, at 3 (alleging that the defendants violated the statute by disclosing biometric data to a third party).

[237] *See* 740 ILL. COMP. STAT. § 14/5 (listing "public welfare, security, and safety" as rationale for implementing regulation of biometric information); Ben Byer, *Washington's New Biometric Privacy Law: What Businesses Need to Know*, DAVIS WRIGHT TREMAINE LLP (July 24, 2017), https://www.dwt.com/Washingtons-New-Biometric-Privacy-Law-What-Businesses-Need-to-Know-07-24-2017/ [https://perma.cc/RCD5-3EUV] (noting that Illinois's statute provides greater protection for individual consumers).

[238] *See* Claypoole & Stoll, *supra* note 8, at 3 (listing fundamental provisions contained in the Illinois BIPA that regulate businesses' collection and use of biometric data); Pasternak, *supra* note 165 (describing the BIPA issues that are being litigated in 2017 such as standing and constitutionality, that are likely to have an effect on subsequent cases).

[239] *See* WASH. REV. CODE § 19.375.020(1) (stating that regulation is limited to "commercial purpose[s]"); H.B. 1493, 65th Leg., Reg. Sess. § 3(4) (Wash. 2017) (listing the definition of "com-

collected and used for "security" purposes.[240] Rather than entirely limit the sale or disclosure of biometric data, the distinction between "commercial" and "security" purposes directly attempts to mitigate the harms caused by the data broker industry by regulating an entity's sale, lease, or disclosure of biometric data to third parties for unrelated marketing purposes.[241] This distinction allows greater latitude for businesses to implement biometric technology into products and services for the purpose of consumer security while attempting to protect consumers from data brokers' harmful practices.[242] For example, Nest's doorbell familiar faces feature is not disabled to consumers in Washington.[243] Therefore, as more states look to implement statutes that regulate businesses' collection, use, and disclosure of biometric data, they should implement a "commercial purpose" limitation to the scope of regulation similar to Washington's.[244] This limitation on the scope of regulation provides a better balance of protecting individual consumers' biometric data from discriminatory use and businesses implementation of biometric technology to use biometric data to enhance security.[245]

mercial purpose" within the statute as "a purpose in furtherance of the sale, lease, or distribution of biometric data to third parties for the purpose of marketing goods and services which are unrelated to the initial transaction in which a person first gains possession of an individuals' biometric identifier"); Byer, *supra* note 237 (claiming that Washington's statute provides greater protection for businesses' use of biometric data). *Contra* 740 ILL. COMP. STAT. § 14/15(b) (listing the broad requirements for an entity's collection, receipt, capture, or purchase of biometric information *for any purpose* [emphasis added]).

[240] *See* Wash. H.B. 1493 § 3(4) (stating that a "commercial" purpose as defined under the statute does not include a "security or law enforcement purpose").

[241] *See id.* (defining "commercial purpose" within the statute as relating to prohibited marketing); Byer, *supra* note 237 (noting that Illinois's statute provides greater protection for individual consumers and Washington's statute provides greater protection for businesses' use of biometric data); Tumeh, *supra* note 18 (describing that the commercial purpose limitation does not directly apply to a business' own internal use of biometric information but rather to disposition of that data to third parties for prohibited marketing purposes).

[242] *See* WASH. REV. CODE ANN. § 19.375.020(7) (excluding from regulation a business' collection of biometric data for "security" purposes); Wash. H.B. 1493 § 3(4) (defining "security" purposes as "preventing shoplifting, fraud, or any other misappropriation or theft of a thing of value"); *see also* FTC DATA BROKERS, *supra* note 9, at 48 (describing how businesses offer differing levels of service to consumers based upon assigned categories derived from potentially discriminatory data algorithms).

[243] *See Nest Familiar Faces*, *supra* note 215 (stating that Nest's "familiar face detection feature" is disabled on Nest cameras used in Illinois).

[244] *See* Wash. H.B. 1493 § 3(4) (listing the definition of "commercial purpose" within the statute); *see also* H.B. 72, 30th Leg., 1st Sess. (Alaska 2017) (stating Alaska's proposed biometric data regulation); H.B. 1985, 190th Gen. Court, Reg. Sess. (Mass. 2017) (stating Massachusetts's proposed biometric data regulation); H.B. 5019, 99th Leg., Reg. Sess. (Mich. 2017) (stating Michigan's proposed biometric data regulation); Tumeh, *supra* note 18 (explaining that the commercial purpose limitation applies to disclosure to third parties for prohibited marketing purposes).

[245] *See* Barocas & Selbst, *supra* note 4, at 675 (noting that algorithms can be designed, either intentionally or inadvertently to use proxies, such as geographic location or income level, to discriminate against individuals); Borgesius et al., *supra* note 4, at 2091–93 (noting that predictive algorithms

Additionally, Congress should implement a comprehensive federal statute that regulates businesses' collection, use, and disclosure of biometric data.[246] Despite the fact that biometric data provides both benefits and risks, the risks of misuse, improper disclosure, or a data breach necessitate stringent regulation for protection.[247] As ease of data dissemination increases across the United States, businesses and consumers face the issue of different levels of protection for data depending on each jurisdiction's own regulations.[248] A comprehensive federal statute that regulates businesses' collection, use, and disclosure of biometric data would provide greater clarity, allowing businesses to operate consistently across states and would provide consumers certainty regarding their data protection rights.[249] It is more likely, however, that the states will be left to comprehensively regulate biometric data due to the industry-specific nature of federal privacy regulation.[250] Therefore, the states must take action and follow Washington's statute to balance protecting consumers' biometric data from discriminatory use and businesses' use of biometric data to enhance security.[251]

CONCLUSION

Businesses continue to implement innovative biometric identification technology across industries to better authenticate and provide security for individuals, and ease consumers' access to businesses' services. Despite the ben-

can categorize individuals in a discriminatory manner); Contreras, *supra* note 133 (reporting the critique that Illinois privacy statutes are an impediment to technological development). According to Carl Szabo of NetChoice, some already developed facial recognition technology cannot be used in Illinois. *See* Contreras, *supra* note 133 (discussing the comprehensive scope of Illinois's BIPA).

[246] *See* Claypoole & Stoll, *supra* note 8, at 4 (noting that there is no single comprehensive federal privacy regulation in the United States).

[247] *See id.* at 1 (describing the benefits and risks of biometric data as compared to traditional data security measures); Larduinat, *supra* note 67 (noting that biometric technology enables increased security for consumers). *Contra* Meyer, *supra* note 68 (suggesting that biometric data is not entirely secure because unlike other traditional forms of security, individuals are unable to change their biometric information).

[248] *See* Roberg-Perez, *supra* note 17, at 64 (articulating the issues with different regulations in different jurisdictions).

[249] *See id.* (noting the issues for both consumers and businesses from the lack of a comprehensive federal statute).

[250] *See* Cunningham, *supra* note 98, at 664 (differing between the United States' sectoral approach to privacy regulations and Europe's single comprehensive approach); Rostow, *supra* note 102, at 676 (describing the industry specific nature of commercial privacy regulations under United States federal law).

[251] *See* Tumeh, *supra* note 18 (explaining that the commercial purpose limitation provides greater consideration for businesses because it only regulates disclosure to third parties for prohibited marketing purposes); *see also* FTC DATA BROKERS, *supra* note 9, at 13–14, 47 (reporting that consumers' data is purchased by data brokers from commercial entities such as retailers and financial services companies and used to create both beneficial and harmful marketable categories); Larduinat, *supra* note 6 (attributing both increased security and accessibility of businesses' services and products to the rise in biometric technology).

efits this technology provides for consumers, it coincides with the data broker industry's immense aggregation of data to sort individuals into potentially discriminatory categories. Overregulation, however, risks disincentivizing businesses from implementing potentially beneficial technology into their product and services. Current federal laws and regulations do not go far enough to comprehensively prevent the potential misuse of individual's sensitive biometric data. The three state statutes, Illinois, Texas, and Washington, that do provide comprehensive biometric data regulation do not offer a consistent approach. As more states look to adopt biometric data laws, there must be some balance and consistency to the scope of regulation to protect both individual consumers' biometric data from discriminatory use and businesses' use of biometric data to enhance security.

LAUREN STEWART