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

Follow this and additional works at: https://lawdigitalcommons.bc.edu/bclr

Part of the Civil Rights and Discrimination Commons, Commercial Law Commons, Computer Law Commons, Privacy Law Commons, Science and Technology Law Commons, and the State and Local Government Law Commons

Recommended Citation


This Notes is brought to you for free and open access by the Law Journals at Digital Commons @ Boston College Law School. It has been accepted for inclusion in Boston College Law Review by an authorized editor of Digital Commons @ Boston College Law School. For more information, please contact nick.zydzlowski@bc.edu.
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).


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. 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. 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. After collecting consumer information, data brokers aggregate that information into segments or marketable categories, often through automated predictive analysis tools. A study published by the Federal Trade Commission (FTC) found a number of these categories to be harmful to consumers and potentially discriminatory. 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. Data brokers often assign marketing “scores” to these categories and sell that information to employers and businesses such as loan companies. 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. To prevent potential private and public collection and use of an individual’s biometric identification data within various sectors).


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. The state statutes, however, offer conflicting definitions and standards of regulation.

This Note examines the developing regulation of biometric data in commercial industries. 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. Part II of this Note discusses the rise of state implementation of statutes that regulate businesses’ interaction with biometric data. 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. 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. 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.

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. A primary applica-
tion has been the collection and use of individuals’ biometric data in security and fraud prevention tools, enabling more accurate authentication of individuals.\textsuperscript{26} The United States, however, does not have a single, comprehensive federal law regulating businesses’ collection and use of biometric data.\textsuperscript{27} Without regulation, businesses are free to disclose an individual’s biometric data to third parties, such as data brokers.\textsuperscript{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.\textsuperscript{29}

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

\textsuperscript{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).

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

\textsuperscript{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).

\textsuperscript{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).

\textsuperscript{30} See infra notes 34–131 and accompanying text.

\textsuperscript{31} See infra notes 34–58 and accompanying text.
“big data” and its effect on discrimination. Section C of this Part discusses the use of biometric data in the traditional federal privacy landscape.

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. The WannaCry attack affected over 300,000 computers globally. The breach of Deep Root Analytics, a media firm working for the Republican National Committee, compromised data on 198 million American voters. Spotlighted by the media, the breach of Equifax, a prominent consumer credit reporting entity, exposed data on 143 million Americans. Businesses faced with the continuous threat of cyberattacks are often ill-equipped to adequately protect their consumers’ PII. Since 2005, over 8,000 data breaches have been publicly reported, compromising an estimated 10 billion records. 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”).
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).
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).
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


\(^{41}\) 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).


\(^{53}\) 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. The security feature relies on facial recognition in lieu of a password or fingerprint to unlock the device. Other companies are attempting to advance facial recognition authentication by requiring smiling or winking. 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. 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.

B. Modern Day Data Brokers and Discrimination

The use of big data has become embedded in the operations of global society. 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. 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 Olimstead & 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. 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. Nevertheless, there are numerous risks as well, such as the potential to enable opaque discrimination against entire classes of people. For example, predictive crime policing programs such as PredPol correlate the data of historical patterns to target potential crime geography. 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. 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.

In this dual landscape of beneficial and risky big data, the modern day data broker industry has immense potential to adversely impact consumers. 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-

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/2014/08/0001592370.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).
Data brokers collect consumer information, aggregate consumer data into segments or marketable categories, and then sell those categories to third parties.

The process begins when data brokers collect and purchase individuals’ information from both public and private sources. Public sources include federal, state, and local governments as well as social media sites, blogs, and the internet. Data brokers purchase consumers’ private information from commercial entities such as retailers and financial services companies. 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. As data brokers circumvent direct consumer contact, consumers often do not even know that data brokers collect, retain, and use their information. 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.

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).
These categories may ultimately be inherently discriminatory, leading to exploitation of consumers. 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. 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.

As the last step in their operation, data brokers ultimately sell these categories to third parties such as employers, advertisers, and discount loan companies. A specific danger arises from data brokers’ and other entities’ use of predictive algorithms. Predictive algorithms do not merely categorize individuals based on known data but also create inferences about individuals. Target Corporation (“Target”), for example, used predictive algorithms to determine which of its female consumers were pregnant. 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.”\(^8^4\) 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.\(^8^5\) 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.\(^8^6\) 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.\(^8^7\)

Predictive models can function as discriminatory feedback loops because they are scalable, opaque, and able to cause damage.\(^8^8\) 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

\[^{83}\] 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. These models are opaque because consumers often do not have access to their data to confirm that it is incorrect or misleading. 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. Lastly, these models are scalable because they have the ability to be applied consistently across diverse and sizeable data sets.

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. When data brokers or businesses use opaque predictive algorithms, proof of discriminatory intent or impact is difficult to ascertain. At the point of data collection, it is often the case that no PII has actually been obtained. 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. 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).
individuals 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.
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. 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. 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.

Thus, the United States does not currently have a single, comprehensive federal law regulating businesses’ collection and use of biometric data. 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. HIPAA’s definition of “individually identifiable health information” can include certain biometric data. The Genetic Information Nondiscrimination Act protects individual’s genetic information from discrimination in insurance and employment contexts. The Privacy Act of 1974 provides potential barriers to entities from accessing or disclosing an
individual’s personally identifying data that is contained in federal records. Of note, the Children’s Online Privacy Protection Act (“COPPA”) provides extensive protection of minors’ privacy, including the collection of children’s biometric data. COPPA requires parental consent before photos, videos, or audio recordings that contain a child’s image or voice are collected. Additionally, COPPA allows businesses to verify parental consent using facial recognition technology.

The FTC has the authority to promulgate and enforce rules to protect consumers from “unfair and deceptive” business practices. Aside from enforcement of COPPA, however, the FTC has yet to create specific rules regarding businesses’ implementation and use of biometric data in technology. 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. In accordance with these best practices, businesses often subject the data they maintain to anonymization or de-identification techniques.

---

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).


113 See Children’s Online Privacy Protection Rule, supra 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).


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.\textsuperscript{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.\textsuperscript{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.\textsuperscript{120} The five core principles set forth include: (1) notice/awareness; (2) choice/consent; (3) access/participation; (4) integrity/security; and (5) enforcement/redress.\textsuperscript{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.\textsuperscript{122}

Notably, the Federal Communications Commission (FCC), not the FTC, currently has jurisdiction over regulation of Internet service providers (“ISPs”).\textsuperscript{123} The Trump Administration recently signed a Congressional Re-


\textsuperscript{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).


\textsuperscript{121} See id. at 7–11.

\textsuperscript{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).

\textsuperscript{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. 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. Importantly, ISPs are currently not prohibited from selling an individual’s data, including biometric data, to third parties such as data brokers. 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. 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.” Under the statute, biometric data is listed as a type of sensitive personal data. 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.


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).


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).

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).

See id. art. 4(14), at 34.

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

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

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.


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).


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.\footnote{See infra notes 143–203 and accompanying text.} 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
Use of Biometric Identifier Act (“CUBI”). Section B of this Part discusses the Washington statute enacted in 2017.

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. Part 1 of this Section discusses the fundamental provisions of the Illinois BIPA. Part 2 of this Section discusses the rise of class actions brought under the BIPA in Illinois and the obstacles facing plaintiffs. Part 3 of this Section discusses the similarities and differences between the Illinois BIPA and the Texas CUBI.

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. 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. The Illinois BIPA defines “biometric identifiers” as a “retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry.” 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.”

---

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. First, businesses must, in writing, notify consumers and obtain informed written consent for collection of biometric data. 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. Second, businesses are prohibited from selling or “otherwise profiting” from biometric data. Third, the statute allows a limited right to disclosure in certain enumerated circumstances. 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. Fifth, the statute creates a private right for an individual to bring a cause of action to enforce violations of the Illinois BIPA. Notably, Illinois is the only state with a biometric data regulation statute that provides individuals with such a private right of action. 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.

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. 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).
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. Shutterfly challenged the class action on the basis that the Illinois BIPA excluded photographs from its definition of biometric identifiers. 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.

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. Shifting from the consumer context to the employment
context, the more recent class actions nearly all center on employers’ use of biometric technology to track employee work hours and activities.\footnote{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).} 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.\footnote{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).}

In one particular class action suit, \textit{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.\footnote{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).}

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.\footnote{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).} Defendants in these class actions have relied on the United States Supreme Court’s ruling in \textit{Spokeo v. Robins} to claim that the plaintiffs have not sufficiently alleged an injury for the


\footnote{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, \textit{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).}

\footnote{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).}

\footnote{See 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, \textit{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).}

\footnote{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).}
court to grant Article III standing.\footnote{374} Under \textit{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.\footnote{375} In a recent notable case, \textit{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.\footnote{376} 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.\footnote{377} 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.\footnote{378} 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.”\footnote{379} A further distinction arose in the Illinois Appellate Court case, \textit{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.”\footnote{380}
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.\textsuperscript{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.\textsuperscript{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.\textsuperscript{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.\textsuperscript{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.\textsuperscript{181} The statute provides that “biometric identifiers” include a “retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry.”\textsuperscript{182} Similar to the Illinois BIPA, the Texas CUBI contains several foundational requirements.\textsuperscript{183} The Texas CUBI requires businesses to provide

\begin{footnotes}
\item 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).
\item 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).
\item 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).
\item 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).
\item 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).
\item 182 TEX. BUS. & COM. CODE ANN. § 503.001(a).
\item 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.
\end{footnotes}
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.”\textsuperscript{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.”\textsuperscript{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.\textsuperscript{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.”\textsuperscript{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.”\textsuperscript{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.”\textsuperscript{197} Although the Texas biometric law does include a commercial purpose limitation, unlike Washington, commercial purpose is left

\begin{footnotesize}
\begin{itemize}
\item\textsuperscript{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”).
\item\textsuperscript{193} Wash. H.B. 1493 § 3(5) (defining the term “enroll” as it is used in the statute).
\item\textsuperscript{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 \textit{for any purpose}).
\item\textsuperscript{195} Wash. H.B. 1493 § 3(4) (listing the definition of “commercial purpose” within the statute).
\item\textsuperscript{196} Id. § 3(8) (defining “security or law enforcement” purposes within the statute).
\item\textsuperscript{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).
\end{itemize}
\end{footnotesize}
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).
Business and Consumer Interests in Biometric Data Regulation

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 214–238 and 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. 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. 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. Nest sells the doorbell-camera product in Illinois but disables the facial recognition feature. Nest states that due to Illinois legislation, the feature is disabled in that state as a preventative measure. The purpose of the facial recognition feature in this product is to distinguish between known and unknown faces to provide homeowners with greater security. 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. 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 plaintiff’s 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. 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. 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.” 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. 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.

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/ijb/2017/12/lawpulse/illinoisbiometricprivacylawbacknews [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 counter-weight 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).


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. 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. 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. For example, Nest’s doorbell familiar faces feature is not disabled to consumers in Washington. 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. 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.
Additionally, Congress should implement a comprehensive federal statute that regulates businesses’ collection, use, and disclosure of biometric data.\footnote{246 See Claypoole & Stoll, supra note 8, at 4 (noting that there is no single comprehensive federal privacy regulation in the United States).} 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.\footnote{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).} 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.\footnote{248 See Roberg-Perez, supra note 17, at 64 (articulating the issues with different regulations in different jurisdictions).} 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.\footnote{249 See id. (noting the issues for both consumers and businesses from the lack of a comprehensive federal statute).} 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.\footnote{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).} 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.\footnote{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).}

**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-

---

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

\footnote{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).}

\footnote{248 See Roberg-Perez, supra note 17, at 64 (articulating the issues with different regulations in different jurisdictions).}

\footnote{249 See id. (noting the issues for both consumers and businesses from the lack of a comprehensive federal statute).}

\footnote{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).}

\footnote{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