Fordham Intellectual Property, Media and Entertainment Law Journal

Volume 29 *XXIX*
Number 2

Article 5

2019

Face Off: An Examination of State Biometric Privacy Statutes & Data Harm Remedies

Maya E. Rivera
Fordham University School of Law, mrivera81@law.fordham.edu

Face Off: An Examination of State Biometric Privacy Statutes & Data Harm Remedies

Cover Page Footnote

Managing Editor, Fordham Intellectual Property, Media & Entertainment Law Journal, Volume XXIX; J.D. Candidate, Fordham University, School of Law, 2019; B.A., Political Science, Hofstra University, 2014. The author would like to thank Professor Ron Lazebnik for his invaluable guidance, advice, and poignant questioning, Professor N. Cameron Russell for inspiring an investigation into this topic, and Professor Ken Rashbaum for his practitioner's perspective and suggestions. The author would also like to thank the staff and editorial board of the IPLJ, especially Sean Corrado for his patience and superb editorial insight. The author would like to give a special thanks to her friends and family for their love and support, especially her parents, Wilfredo and Maria Rivera, Daniel Rivera, Natasha Rivera, Roland Carvalho III, and Iliana Romero.

Face Off: An Examination of State Biometric Privacy Statutes & Data Harm Remedies

Maya E. Rivera*

As biometric authentication becomes an increasingly popular method of security among consumers, only three states currently have statutes detailing how such data may be collected, used, retained, and released. The Illinois Biometric Information Privacy Act is the only statute of the three that enshrines a private right of action for those who fail to properly handle biometric data. Both the Texas Capture or Use Biometric Identifier Act Information Act and the Washington Biometric Privacy Act allow for state Attorneys General to bring suit on behalf of aggrieved consumers. This Note examines these three statutes in the context of data security and potential remedies for victims of data breaches or mishandled data. Ultimately, this Note makes policy proposals for future biometric privacy statutes, particularly recommending a private right of action as the most effective remedy for victims of biometric data breaches.

* Managing Editor, Fordham Intellectual Property, Media & Entertainment Law Journal, Volume XXIX; J.D. Candidate, Fordham University School of Law, 2019; B.A., Political Science, Hofstra University, 2014. The author would like to thank Professor Ron Lazebnik for his invaluable guidance, advice, and poignant questioning, Professor N. Cameron Russell for inspiring an investigation into this topic, and Professor Ken Rashbaum for his practitioner's perspective and suggestions. The author would also like to thank the staff and editorial board of the IPLJ, especially Sean Corrado for his patience and superb editorial insight. The author would like to give a special thanks to her friends and family for their love and support, especially her parents, Wilfredo and Maria Rivera, Daniel Rivera, Natasha Rivera, Roland Carvalho III, and Iliana Romero.

INTRODUCTION

The idea of using your voice, eyes, or face as a means of interfacing with a computer system has been something that has captured the public imagination since the advent of science fiction television and film in the 20th century. Popular shows and films such as Star Trek, Robocop, and Back to the Future provided examples of a future where the unique biological traits of characters could be used as a means of controlling computers, creating databases, and even securing one's home.[1] Over the course of the last sixty years, however, the idea of using a device to autonomously authenticate one's biological traits went from being science fiction to reality. Today, nearly half of Americans use biometric authenticators[2]—such as fingerprint-readers or face-scanners—for security functions and payment authorization. Such authenticators have become increasingly accessible in consumer devices like smartphones and computers.[3]

Although many Americans do not seem to understand the technology or its implications, biometric authentication has

---

1 *See* Rowena Bonnette, *Biometrics in Movies Sci-Fi Security*, AVATIER (Jan. 31, 2017), https://www.avatier.com/blog/biometrics-in-sci-fi-movies [https://perma.cc/KCV5-GHYU].

2 *See* RACHEL L. GERMAN & K. SUZANNE BARBER, CONSUMER ATTITUDES ABOUT BIOMETRIC AUTHENTICATION 2 (2018).

3 *See* J. Peter Bruzzese, *Windows 10 Puts Biometric Security Front and Center*, INFOWORLD (Mar. 25, 2015), https://www.infoworld.com/article/2901068/authentication/windows-10-biometric-security-front-and-center.html [https://perma.cc/ZAA5-68RR]; Alex Perala, *Smartphone Biometrics Are Officially Mainstream: Acuity*, MOBILE ID WORLD (Feb. 12, 2016), https://mobileidworld.com/smartphone-biometrics-are-officially-mainstream-acuity-102124/ [https://perma.cc/D7VD-HT65]. Fingerprint is now the main ID Method on Mobile. *Id.*

become increasingly popular in the last decade.[4] This appeal can be explained, in part, by the convenience it offers.[5] Because biometric identifiers are often parts of the human body, users of biometric authentication will typically always have their identifier with them.[6] Unlike a password or pin, a biometric identifier does not have be "memorized" and, similarly, cannot be "forgotten," making it a convenient alternative to older, more analog methods of authentication.[7] Further, biometric authenticators can enable a user to interface with data more quickly and efficiently than a traditional password.[8] For some users, the use of biometric authentication gives them the perception of a security advantage, the reasoning being that the use of an immutable biological characteristic might make it more difficult for malicious third parties to gain access to certain types of information by stealing the "password."[9] However, many cybersecurity experts have expressed skepticism at the idea that biometric authentication can provide any unique security advantage over more traditional means.[10]

---

4 *See* GERMAN & BARBER, *supra* note 2, at 11 fig.7. When asked "Have you ever personally provided identifying characteristics to an organization for such a computer-matched biometric comparison?" consumers polled by the University of Texas at Austin Center for Identity answered "No" or "Don't Know" 64.4% of the time. *Id.* 70.4% of consumers in the same poll said they had used fingerprint scanners before. *Id.* at 5 fig.2.

5 *See Biometric Security Systems: A Guide to Devices, Fingerprint Scanners and Facial Recognition Access Control*, IFSEC GLOBAL (Oct. 28, 2016), https://www.ifsecglobal.com/biometric-security-systems-guide-devices-fingerprint-scanners-facial-recognition/ [https://perma.cc/2CMM-PB9V]; *see also* VISA, GOODBYE, PASSWORDS. HELLO, BIOMETRICS. (2017).

6 *See* Tracy V. Wilson, *How Biometrics Works*, HOW STUFF WORKS, https://science.howstuffworks.com/biometrics.htm [https://perma.cc/EP6S-HKSH] (last visited Mar. 7, 2019); s*ee also infra* Section III.A.

7 *See* Wilson, *supra* note 6.

8 Lisa Eadicicco, *How to Make Your iPhone's Fingerprint Scanner More Reliable*, TIME (Dec. 12, 2016), http://time.com/4441448/how-to-improve-touch-id-iphone/ [https://perma.cc/T5KV-2H5B].

9 *See* Ramya Raju, *The Advantages of a Biometric Identification Management System*, M2SYS BLOG (Apr. 7, 2014), http://www.m2sys.com/blog/biometric-hardware/advantages-biometric-identification-management-system/ [https://perma.cc/S4WD-UMC6].

10 *See* April Glaser, *Biometrics Are Coming, Along with Serious Security Concerns*, WIRED (Mar. 9, 2016, 11:00 AM), https://www.wired.com/2016/03/biometrics-coming-along-serious-security-concerns/ [https://perma.cc/XW3D-YEA8].

Concerns about security are not unfounded given that instances of data breaches and cybercrime are on the rise.[11] Common targets include businesses, large and small, governments, and individuals.[12] From a security perspective, the sensitive nature of biometrics presents unique risks.[13] While biometric identifiers may be difficult to access, and in some cases deter malicious third parties like hackers, their irreplaceable nature imbues such data with a particular sensitivity.[14] Should a hacker successfully steal an individual's biometric data point, any information associated with that particular biometric authenticator can be put at risk.[15] Unlike a password or pin that can be changed if compromised, the permanence of certain biological traits results in a compromised individual never being able to securely use a stolen biometric for authentication again.[16] Simply put, if your fingerprint data is stolen, it is not possible to change your fingerprint. Despite this,

---

[11] *See Facts + Statistics: Identity Theft and Cybercrime*, INS. INFO. INSTIT., https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime [https://perma.cc/3ZRU-3K9C] (last visited Mar. 7, 2019).

[12] *See* Kevin McCoy, *Cyber Breach at Equifax Could Affect 143M U.S. Consumers*, USA TODAY (Sept. 7, 2017, 5:17 PM), https://www.usatoday.com/story/money/2017/09/07/credit-reporting-giant-equifax-says-cyber-breach-could-affect-143-m-u-s-consumers/643679001/ [https://perma.cc/G26L-6GMK]; Andrea Peterson, *OPM Says 5.6 Million Fingerprints Stolen in Cyberattack, Five Times as Many as Previously Thought*, THE WASHINGTON POST (Sep. 23, 2015), https://www.washingtonpost.com/news/the-switch/wp/2015/09/23/opm-now-says-more-than-five-million-fingerprints-compromised-in-breaches/?noredirect=on&utm_term=.21563242188b [https://perma.cc/AL5F-6C2B]; *Small Business Cyber Security and Data Breach Risks*, INSUREON, https://www.insureon.com/resources/research/small-business-cyber-security-poll [https://perma.cc/5JEN-CGCL] (last visited Mar. 7, 2019).

[13] *See* The Editors, *Biometric Security Poses Huge Privacy Risks*, SCIENTIFIC AMERICAN (Jan. 1, 2014), https://www.scientificamerican.com/article/biometric-security-poses-huge-privacy-risks/ [https://perma.cc/D79U-5SE8]; Chiara A. Sottile, *As Biometric Scanning Use Grows, So Does Security Risk*, NBC NEWS: MACH (July 24, 2016, 7:23 PM), https://www.nbcnews.com/mach/mach/biometric-scanning-use-grows-so-do-security-risks-ncna593161 [https://perma.cc/B6DJ-ULHA].

[14] *See supra* note 13.

[15] *See id.*

[16] *See id.*

biometric authentication's popularity as a service has proceeded undisturbed.[17]

Because of biometrics' relative novelty, there are currently no federal laws that specifically address the responsibilities of businesses collecting, using, or releasing biometric data.[18] While several states have attempted to address this concern, only three states have proven successful.[19] In 2008, Illinois passed the Biometric Information Privacy Act ("BIPA"), becoming the first state to pass a statute addressing biometric authentication.[20] One year later, Texas followed suit and passed the Capture or Use Biometric Identifier Act ("CUBI").[21] Following the passage of BIPA and CUBI, many states attempted to introduce their own legislation addressing biometric data security.[22] However, it was not until 2017, eight years after CUBI's passage, that Washington became the third state to introduce such a law, known as the Washington Biometric Privacy Act ("WBPA").[23] Unlike CUBI, which shared some features with the at-the-time recent BIPA, the WBPA distinguishes itself from its predecessors by adding unique features and excluding other specific provisions and ideas.[24]

---

17 *See* RACHEL L. GERMAN & K. SUZANNE BARBER, CURRENT BIOMETRIC ADOPTION AND TRENDS (2018); Alex Koma, *Study: Americans Increasingly Accept Biometric Tech for Security*, FEDSCOOP (Apr. 6, 2016), https://www.fedscoop.com/study-americans-increasingly-accept-governments-using-biometric-technologies-for-surveillance-security/ [https://perma.cc/3TUR-369F].

18 *See Biometric Data and the General Data Protection Regulation*, GEMALTO, https://www.gemalto.com/govt/biometrics/biometric-data [https://perma.cc/4SK2-FLUA] (last updated Feb. 18, 2018).

19 *See id*.

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

21 Capture or Use Biometric Identifier Act, TEX. BUS. & COM. CODE § 503.001 (2009).

22 *See* Divya Taneja, *Washington Enacts a Biometric Privacy Statute in a Departure from the Existing Standard*, PROSKAUER: NEW MEDIA AND TECH. L. BLOG (June 13, 2017), https://newmedialaw.proskauer.com/2017/06/13/washington-enacts-a-biometric-privacy-statute-in-a-departure-from-the-existing-standard/ [https://perma.cc/T4GN-LFR4].

23 Washington Biometric Privacy Act, WASH. REV. CODE § 19.375 (2017); *see also* Taneja, *supra* note 22; Rebecca Yergin, *Washington Becomes Third State with a Biometric Law*, COVINGTON: INSIDE PRIVACY (May 31, 2017), https://www.insideprivacy.com/united-states/state-legislatures/washington-becomes-the-third-state-with-a-biometric-law/ [https://perma.cc/3X9F-ASD3].

24 *Compare* WASH. REV. CODE § 19.375 (2017), *with* TEX. BUS. & COM. CODE § 503.001 (2009), *and* 740 ILL. COMP. STAT. 14/1 (2008).

While these statutes recognize the unusual challenges that biometric authentication poses, each proposes different approaches in defining biometrics and enforcement options. There is evidence to suggest, however, that BIPA, the oldest of these state biometric statutes, might be the most effective privacy law of its peers due to the private right of action it provides and its hardline stance against the sale of biometric data.[25] This Note will attempt to examine the language of these statutes, analyze their functions critically amongst the current backdrop of legal options available in addressing cybersecurity threats, and suggest elements that should be included in biometric privacy statutes moving forward. Part I will examine data privacy law in the United States, the basics of biometric technology, and introduce the three current biometric privacy statutes. remedies for consumer data breaches, biometrics, and the statutory language of BIPA, CUBI, and the WBPA. Part II will discuss the remedies available to data breach victims, and their limitations. Part III will closely examine and explain the statutory language of BIPA, CUBI, and the WBPA. Finally, Part IV will critically examine BIPA, CUBI, and the WBPA, and offer recommendations for creating ideal biometric privacy legislation moving forward.

I. BIOMETRICS AND DATA PRIVACY LAW IN THE UNITED STATES

A. Data Insecurity

In the world of computing, data is "information in digital form that can be transmitted or processed."[26] "Information" can be anything, including strings of plain text, numbers, pictures, and executable software programs.[27] On most computers, this information is converted into a binary number sequence, made up of zeroes and ones, and stored on a hardware drive that the

---

[25] *See* discussion *infra* Section III.A.

[26] *Data*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/data [https://perma.cc/L3N2-A2YQ] (last visited Mar. 7, 2019).

[27] *See Data*, TECH TERMS, https://techterms.com/definition/data [https://perma.cc/94RQ-8Y5C] (last visited Mar. 7, 2019).

computer can read.[28] Nearly all businesses today use computers to operate.[29]

As a result of this reliance on computers, businesses often store sensitive and private data on their computers in some capacity.[30] Consequently, when sensitive data is leaked or accessed, it can be potentially harmful if it falls into the wrong hands. A data breach occurs when data is stolen, compromised, or otherwise unintentionally disclosed.[31] The term data breach usually invokes the image of malicious hackers who gain access to sensitive data through illicit means such as using targeted malware, tricking third-party service providers, or even targeting unprotected personal devices.[32] A data breach, however, can be as simple as an employee stealing information that he is entrusted with throughout the course of his work.[33] Regardless of how a breach occurs, its consequences impact a shockingly high number of Americans each year with increasing frequency.[34] In 2016 alone, there were at least two data breaches made public for each day of the year.[35] In 2014, some estimates concluded that up to 47% of American adults have

---

[28] *See id*.

[29] *See* C.D. Crowder, *Uses for Computers in Business*, CHRON, http://smallbusiness.chron.com/uses-computers-business-56844.html [https://perma.cc/9CK6-T6YR] (last visited Mar. 7, 2019).

[30] *See Data Security*, FED. TRADE COMM'N, https://www.ftc.gov/tips-advice/business-center/privacy-and-security/data-security [https://perma.cc/46ZK-U2KY] (last visited Mar. 3, 2019); Kelly Sheridan, *Large Majority of Businesses Store Sensitive Data in Cloud Despite Lack of Trust*, DARK READING (Apr. 16, 2018), https://www.darkreading.com/cloud/large-majority-of-businesses-store-sensitive-data-in-cloud-despite-lack-of-trust/d/d-id/1331538 [https://perma.cc/P6PT-9BR4].

[31] *See* Margaret Rouse, *Data Breach*, TECHTARGET, https://searchsecurity.techtarget.com/definition/data-breach [https://perma.cc/G3LA-8CTR] (last visited Mar. 7, 2019).

[32] *See* Eric Basu, *The Top 5 Data Breach Vulnerabilities*, FORBES (Nov. 5, 2015, 11:44 AM), https://www.forbes.com/sites/ericbasu/2015/11/05/the-top-5-data-breach-vulnerabilities/#39dfa1ae4d04 [https://perma.cc/NSU3-9SRZ].

[33] *See id*.

[34] *See* Mike Snider, *Your Data was Probably Stolen in Cyberattack in 2018 – and You Should Care*, USA TODAY (Dec. 28, 2019, 6:00 AM), https://www.usatoday.com/story/money/2018/12/28/data-breaches-2018-billions-hit-growing-number-cyberattacks/2413411002/ [https://perma.cc/3BAX-M7TG].

[35] *See generally 2016 Data Breaches*, PRIVACY RIGHTS CLEARINGHOUSE: DATA BREACHES, https://www.privacyrights.org/data-breaches [https://perma.cc/ZH5P-M9Z3] (last visited Mar. 7, 2019).

had their private information stolen through data breaches.[36] As incidents of cybercrime and data breaches increase in frequency each day, there are concerns that such events are inevitable; as former Federal Bureau of Investigation Director Robert Mueller once expressed, "there are only two types of companies: those that have been hacked and those that will be."[37]

B. Biometric Basics

The process of using anatomical or behavioral traits and characteristics as a form of automatic identification is known today as biometric authentication.[38] These unique traits and characteristics, or "biometric identifiers," can include a fingerprint, voice, iris, and facial shape.[39] Biometric authentication can be used to accomplish a wide variety of technological objectives including securing computers, accessing financial information, or even tracking attendance in a workplace.[40]

Biometric authentication works by capturing an individual's unique biological identifier and storing it as a data point.[41] This data point is then used as a means of comparing the trait against future instances of its use.[42] For example, a fingerprint reader works by capturing an image of the unique pattern of ridges on your finger, and then compares that image from that point forward with any input from a fingerprint that the reader receives.[43] If the

---

[36] *See* Jose Pagliery, *Half of American Adults Hacked This Year*, CNN (May 28, 2014, 9:25 AM), http://money.cnn.com/2014/05/28/technology/security/hack-data-breach/index.html [https://perma.cc/H42K-KYJ8].

[37] Robert S. Mueller III, Director, Fed. Bureau of Investigation, Address at RSA Cyber Security Conf. (Mar. 1, 2012).

[38] *See An Overview of Biometric Recognition*, COMPUT. SCI. ENG'G, MICH. ST. U., https://web.archive.org/web/20120107071003/http://biometrics.cse.msu.edu/info.html [https://perma.cc/4LUK-S895] (last visited Mar. 7, 2019).

[39] *See id*.

[40] *See* John Trader, *The Top 5 Uses of Biometrics Across the Globe*, M2SYS BLOG (Aug. 9, 2016), http://www.m2sys.com/blog/biometric-hardware/top-5-uses-biometrics-across-globe [https://perma.cc/Q3U7-28ZH].

[41] *See* COMPUT. SCI. ENG'G, MICH. ST. U., *supra* note 38; Wilson, *supra* note 6.

[42] *See* COMPUT. SCI. ENG'G, MICH. ST. U., *supra* note 38; Wilson, *supra* note 6.

[43] *See* Chris Woodford, *Biometric Fingerprint Scanners*, EXPLAIN THAT STUFF!, http://www.explainthatstuff.com/fingerprintscanners.html [https://perma.cc/SFN9-AHH8] (last updated June 28, 2018).

input received matches the previously captured fingerprint image, the technology decides that the user's identity has been verified and can grant access to secured data or trigger an activity of some kind.[44] This same basic principle can be applied to other forms of biometric authentication such as iris scanners, facial recognition, or voiceprints.

The particular sensitivity of biometric data raises serious concerns in the age of cybercrime. If compromised, information such as credit card numbers, passwords, and other sensitive information can be used to commit fraud, identity theft, harassment among other crimes.[45] Despite this increased risk of harm, there are ways for almost all of those forms of data to be replaced over time one way or another.[46] When a biometric data point is stolen however, there is no way to replace an individual's biometric identifier.[47] Unlike the film *Face/Off*, face-replacing technology with no risk of biological rejection and minimal recovery time does not currently exist.[48] The increased risk of harm caused by the theft of biometric data can potentially last in perpetuity, forever restricting an individual from using that biometric identifier as a security point safely ever again. As incidents of data breaches increase in frequency, reports of massive biometric data breaches

---

44 *See id.*

45 *See* Jessica Dickler, *41 Million Americans Have Had Their Identities Stolen*, CNBC (Oct. 11, 2016, 8:31 AM), https://www.cnbc.com/2016/10/10/41-million-americans-have-had-their-identities-stolen.html [https://perma.cc/W5KZ-SNKL].

46 *See Data Breaches 101: How They Happen, What Gets Stolen, and Where It All Goes*, TREND MICRO USA (Oct. 23, 2015), https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/data-breach-101 [https://perma.cc/Q6GW-2MRU].

47 *See* The Editors, *supra* note 13; Sottile, *supra* note 13.

48 *Cf.* FACE/OFF (Paramount Pictures 1997). While plastic surgeries exist that can change a person's face, undergoing a procedure significant enough to create a new facial biometric is not without psychological or ethical concerns. *See Changing Identity—Face Transplant Ethics*, ROYAL FREE LONDON NHS, https://www.royalfree.nhs.uk/services/services-a-z/plastic-surgery/facial-reconstruction-and-face-transplants/changing-identity-face-transplant-ethics/ [https://perma.cc/48BL-G2KX] (last visited Mar. 7, 2019). Further, recovery from facial surgery is a difficult and lengthy process unlike the relatively quick procedure in *Face/Off*. *Compare Human Caniomaxillo Allotransplantation: A Face Transplant Research Study*, JOHN HOPKINS MEDICINE: COMPREHENSIVE TRANSPLANT CENTER, https://www.hopkinsmedicine.org/transplant/programs/reconstructive_transplant/face_transplant.html#rehabilitation [https://perma.cc/3HX6-HLM8] (last visited Mar. 7, 2019), *with* FACE/OFF (Paramount Pictures 1997).

both in America[49] and abroad[50] raise serious questions about how victims of such breaches can protect themselves.

C. *Today's Biometric Data Privacy Statutes*

Illinois's Biometric Information Privacy Act was first introduced to the Illinois Senate in February 2008 following the bankruptcy of a San Francisco based company known as Pay by Touch.[51] Pay By Touch provided vendors with devices that used biometric authentication to allow consumers to pay for their goods by connecting their financial information to their fingerprint.[52] Following the company's bankruptcy and dissolution, consumers were given no information as to what would become of the biometric data or financial information they had provided to Pay By Touch.[53] This incident was an impetus for BIPA's drafting and eventual passage.[54] One year later in 2009, Texas passed its own biometric privacy statute known as the Capture or Use Biometric Identifier Act Information Act. Finally, after an eight-year gap, Washington passed its Washington Biometric Privacy Act in 2017.

Each of these statutes sets out to regulate the Capture or Use Biometric Identifier Act data in different ways, particularly with regard to enforcement against entities who misuse or misplace that data.[55] Although the remedies these statutes propose represent only a portion of potential remedies available to data breach victims, enforcement in the world of data privacy law remains complicated and ever-changing due to the relatively new kinds of harm that technology presents.[56]

---

49 *See* Peterson, *supra* note 12.

50 *See* Rohith Jyothish, *The World's Biggest Biometric Database Keeps Leaking People's Data*, FAST CO. (Jan. 1, 2018), https://www.fastcompany.com/40516447/the-worlds-biggest-biometric-database-keeps-leaking-peoples-data [https://perma.cc/K58A-YJHP].

51 *See* Justin O. Kay, *The Illinois Biometric Information Privacy Act*, DRINKER BIDDLE & REATH 1, https://www.acc.com/sites/default/files/2019-02/Drinker-Biddle-2017-1-BIPA-Article-2.pdf [https://perma.cc/U9RQ-JRUM] (last visited Mar. 10, 2019).

52 *See id*.

53 *See id*.

54 *See id*.

55 *See infra* Part III.

56 *See infra* Part II.

II. CURRENT DATA BREACH ENFORCEMENT REMEDIES

When a data breach occurs, it can often be difficult or impossible to hold the party who compromised the data legally responsible. Consequently, consumer data breach victims can typically only hold the private entity with which they entrusted their data accountable for the breach. In most situations, impacted victims have one of four options: (1) a private lawsuit, (2) a class action suit, (3) private arbitration, or (4) state attorneys general action.[57]

A. Private Lawsuits

Bringing a private suit for a data breach can be a complicated process depending on which state a victim finds herself in. Few states have statutes that address the possibility of a private right of action in the event of a data breach and, of those that do, some specific restrictions may apply.[58] Data breach notification statutes in California or Louisiana, for example, allow for a private right of action only when a compromised entity fails to notify users of the breach.[59] Further, both of these statutes require a victim suffer "actual harm," sometimes referred to as "tangible" or "cognizable harm," as a result of the breach, something that can be difficult to prove due to the at times complex and abstract nature of the data stolen.[60] Other states, such as Alaska or Massachusetts, have statutes that enable data breach victims to sue for deceptive or unfair business practices instead of directly addressing data breaches.[61] If a state does not have a statute that might provide a private right of action for data breach, the risk involved in privately suing a compromised entity increases as the suit would have to rely

---

57 *See* Ian Salisbury, *Wanna Sue Equifax? Here Are All Your Options*, TIME (Sep. 22, 2017), http://time.com/money/4949869/equifax-data-breach-lawsuits/ [https://perma.cc/G5WS-9T5X].

58 *See* BAKER & HOSTETLER LLP, DATA BREACH CHARTS: JULY 2018 26, https://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/Data_Breach_Charts.pdf [https://perma.cc/BUD4-USAT] (last visited Mar. 7, 2019).

59 *See id.*

60 *See id.*

61 *See id.*

on legal theories independent of specific laws.[62] Ultimately, any private suit against a compromised entity may present an unbearably high level of risk depending on the amount of financial and legal resources available.[63]

B. Class Action Lawsuits

Class action suits may provide a more economical option to victims of data breaches, however, such suits can present a different host of challenges. First, few class action complaints are ever filed against breached entities relative to the amount of breaches that occur.[64] While 806 data breaches were made public in 2016, only seventy-six class action complaints were filed throughout the year.[65] Of those seventy-six complaints, only twenty-seven unique defendants were named resulting in only 3.3% of publicly reported breaches leading to class action litigation.[66] Class action suits against breached entities can also have difficulties with the predominance requirement of class certification due to difficulty proving that losses resulting from fraudulent transactions are consistent amongst the class.[67] The challenge of proving actual harm can also impact class action suits. In a 2015 case involving a class action suit against eBay for a data breach resulting in the exposure of users' "personally identifiable information" ("PII"),[68] a federal judge dismissed the suit finding

---

62 *See* Matt Garry, *My Data Has Been Breached—Can I Sue?*, MICH. TECH. L. REV., https://mttlr.org/2018/10/my-data/ [https://perma.cc/7XYM-TDAD] (last visited Mar. 7, 2019).

63 *See* Richard Cordray, *Let Consumers Sue Companies*, N. Y. TIMES (Aug. 22, 2017), https://www.nytimes.com/2017/08/22/opinion/let-consumers-sue-companies.html [https://perma.cc/JX87-6S8G]; Salisbury, *supra* note 57.

64 *See* David Zetoony et al., *2017 Data Breach Litigation Report*, BRYAN CAVE LLP, https://d11m3yrngt251b.cloudfront.net/images/content/9/6/v2/96690/Bryan-Cave-Data-Breach-Litigation-Report-2017-edition.pdf [https://perma.cc/Q5EA-BC8K] (last visited Mar. 7, 2019).

65 *See id*. at 3.

66 *See id.* at 1.

67 *See generally* Green v. eBay Inc., No. 14-1688, 2015 U.S. Dist. LEXIS 58047 (E.D. La. May 4, 2015); Mathew J. Schwartz, *Why So Many Data Breach Lawsuits Fail*, BANK INFO. SEC. (May 11, 2015), https://www.bankinfosecurity.com/data-breach-lawsuits-fail-a-8213 [https://perma.cc/BM8F-Q7JF].

68 Personally identifiable information, generally, is data that can be used to identify or de-anonymize a particular person. *See What Is Personally Identifiable Information (PII)?*,

that the plaintiffs had no Article III standing as they did not suffer actual harm from the breach.[69] There, the court stated that an increased risk of identity theft resulting from the breach did not constitute actual harm.[70] In 2016, the Supreme Court held in *Robins v. Spokeo* that "intangible harm," including risk of harm, could be considered "concrete" for the purposes of Article III standing, giving courts some guidance in addressing data breach harms.[71] However, there has since been little guidance as to when a particular harm is "concrete."[72] Now, while not all courts agree that future risk of harm resulting from data breaches does not constitute harm, the risk of being dismissed remains.[73] Further, class action suits can generally be very risky with some studies finding that few end with a final judgment on the merits for the plaintiffs and even fewer produce any benefit to the plaintiffs.[74]

C. Arbitration

While private arbitration is occasionally a data breach victim's choice, it is often the only means available to compromised consumers.[75] Mandatory arbitration clauses are written into many contracts and agreements between consumers and private entities,

---

LIFELOCK, https://www.lifelock.com/learn-identity-theft-resources-what-is-personally-identifiable-information.html [https://perma.cc/5VHQ-BAFV] (last visited Mar. 7, 2019); *see also* PII, *Anonymized Data, and Big Data Privacy*, SMARTDATA COLLECTIVE (Feb. 12, 2015), https://www.smartdatacollective.com/pii-anonymized-data-and-big-data-privacy/ [https://perma.cc/A29K-3ENT]. The PII exposed in *Green* included users' names, mailing addresses, birthdates, and more. *See Green*, 2015 U.S. Dist. LEXIS, at *2–4, *15–16.

69 *See Green*, 2015 U.S. Dist. LEXIS, at *2–4, *15–16.

70 *See id.* at *15–16.

71 *See* Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1549 (2016).

72 *See* Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data Breach Harms*, 96 TEX. L. REV. 737, 744 (2018).

73 *See generally* In re Adobe Sys. Privacy Litig., 66 F. Supp. 3d 1197, 1216 (N.D. Cal. 2014); In re Sony Gaming Networks & Customer Data Sec. Breach Litig., 996 F. Supp. 2d 942, 963 (S.D. Cal. 2014).

74 *See* MAYER BROWN LLP, *Do Class Actions Benefit Class Members? An Empirical Analysis of Class Actions*, INST. FOR LEGAL REFORM, http://www.instituteforlegalreform.com/uploads/sites/1/Class_Action_Study.pdf [https://perma.cc/7WTR-LPM2] (last visited Mar. 7, 2019).

75 *See Arbitration*, NAT'L ASS'N CONSUMER ADVOCATES, https://www.consumeradvocates.org/for-consumers/arbitration [https://perma.cc/43C4-ZL6L] (last visited Mar. 7, 2019).

especially in matters related to finances.[76] Such clauses, should private entities choose to enforce them, can effectively bar a consumer's right to sue entirely.[77] In many contracts and agreements, mandatory arbitration clauses can be difficult to catch in the fine print and, in the past, private entities have attempted to enforce such arrangements on consumers even without formal agreements.[78] Arbitration can also be costly for an aggrieved individual and prevent her from having an opportunity to present her case to a judge.[79] A 2015 Consumer Financial Protection Bureau ("CFPB") study found that, on average, group lawsuits were more effective in getting plaintiffs money than arbitration.[80] Further, a study of one particular arbitration firm found that businesses prevailed ninety-four percent of the time.[81] Although

---

[76] *See generally* CONSUMER FIN. PROT. BUREAU, ARBITRATION STUDY: REPORT TO CONGRESS, PURSUANT TO DODD-FRANK WALL STREET REFORM AND CONSUMER PROTECTION ACT § 1028(A) (2015).

[77] *See* NAT'L ASS'N CONSUMER ADVOCATES, *supra* note 75.

[78] *See Mandatory Arbitration Clauses: Undermining the Rights of Consumers, Employees, and Small Businesses*, PUB. CITIZEN, https://www.citizen.org/article/mandatory-arbitration-clausesundermining-rights-consumers-employees-and-small-businesses [https://perma.cc/5NUE-9MJ3] (last visited Mar. 7, 2019). The proliferation of mandatory arbitration clauses should be of little surprise given how few Americans read terms of service or privacy policies, and how long it would take to do so each year. *See* David Berreby, *Click to Agree with What? No One Reads Terms of Service, Studies Confirm*, THE GUARDIAN (Mar. 3, 2017, 8:38 AM), https://www.theguardian.com/technology/2017/mar/03/terms-of-service-online-contracts-fine-print [https://perma.cc/8PH2-MPCS]; Keith Wagstaff, *You'd Need 76 Work Days to Read All Your Privacy Policies Each Year*, TIME (Mar. 6, 2012), http://techland.time.com/2012/03/06/youd-need-76-work-days-to-read-all-your-privacy-policies-each-year/ [https://perma.cc/PGQ6-WFF9]. Some arbitration clauses attempt to forego formal agreements entirely; in one instance, General Mills attempted to bind any consumer who "liked" its Facebook page to mandatory arbitration. *See* Ricardo Lopez, *General Mills Abandons Mandatory Arbitration after Consumer Outcry*, L.A. TIMES (Apr. 21, 2014, 10:44 AM), http://www.latimes.com/business/la-fi-mo-general-mills-legal-policy-reversal-20140421-story.html [https://perma.cc/NNP7-ADQ4].

[79] *See Arbitration: Not Necessarily a Better Option Than Litigation*, BTLG ATTORNEYS AT LAW, http://www.btlg.us/News_and_Press/articles/arbitration.html [https://perma.cc/HK72-PD56] (last visited Mar. 7, 2019); Gary Benton, *Arbitrators Are Not Judges*, SILICON VALLEY ARBITRATION & MEDIATION CENTER, https://svamc.org/arbitrators-are-not-judges [https://perma.cc/A8GX-RW4F] (last visited Mar. 7, 2019).

[80] *See* CONSUMER FIN. PROT. BUREAU, *supra* note 76; Cordray, *supra* note 63.

[81] *See* John O'Donnell, *The Arbitration Trap: How Credit Card Companies Ensnare Consumers*, PUB. CITIZEN 4 (2007),

the CFPB added a rule to the Federal Register in July 2017 forbidding financial firms under the Bureau's jurisdiction from blocking consumers from joining class action suits, the rule was repealed just four months later.[82]

D. State Attorneys General Actions

In the 1960s and 1970s, state attorneys general ("AG") established consumer protection divisions in their offices, as states, with the FTC's encouragement, began to adopt Unfair and Deceptive Practices ("UDAP") statutes.[83] By the 1990s, state AG offices started using UDAP laws to "protect consumers from privacy-invasive business practices."[84] Since then, as Danielle Citron notes in *The Privacy Policymaking of State Attorneys General*, state AGs have used their tools to shape and change legal norms surrounding data privacy violations. Despite these gains, however, AG action gives data breach victims little control over their recourse as AGs have ultimate discretion over what lawsuits they file.[85] Further, because AGs are elected officials, they remain susceptible to political capture through special interest lobbying.[86]

---

https://www.citizen.org/sites/default/files/final_wcover.pdf [https://perma.cc/AV2B-L5XN].

82 *See* Sylvan Lane, *Trump Repeals Consumer Arbitration Rule, Wins Bankers Praise*, THE HILL (Nov. 1, 2017, 4:43 PM), http://thehill.com/policy/finance/358297-trump-repeals-consumer-bureau-arbitration-rule-joined-by-heads-of-banking [https://perma.cc/4L23-CYY7].

83 *See* Danielle K. Citron, *The Privacy Policymaking of State Attorneys General*, 92 NOTRE DAME L. REV. 747, 753–54 (2017).

84 *Id.* at 754.

85 *See* Emily Myers & Ayeisha Cox, *The Authority of State Attorneys General and Their Efforts on 21st Century Policing*, THE BOOK OF THE STATES 202 (2016), http://knowledgecenter.csg.org/kc/system/files/Myers%20Cox%202016.pdf [https://perma.cc/QED9-U4N2].

86 *See* Citron, *supra* note 83.

III. THE MECHANISMS OF TODAY'S STATE BIOMETRIC DATA PRIVACY STATUTES

A. What is a Biometric Identifier?

BIPA defined the unique biological traits and characteristics used for biometric authentication as "biometric identifiers":

> Section 10. Definitions. In this Act:
> "Biometric identifier" means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry. Biometric identifiers do not include writing samples, written signatures, photographs, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, or physical descriptions such as height, weight, hair color, or eye color.[87]

The use of the term "biometric identifier" as the subject of the type of information being regulated is universal across all three state statutes however, each law has its own unique definition of a biometric identifier.[88] For example, Texas's Capture or Use Biometric Identifier Act distinguishes itself from BIPA by defining a biometric identifier as "a retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry."[89] Unlike BIPA, CUBI's definition offers no specific exemptions for what is not considered a biometric identifier.[90] The Washington Biometric Privacy Act similarly distinguishes itself from its predecessors by instead giving a general definition for a biometric identifier followed by examples of what is or is not included by the definition:

> (1) "Biometric identifier" means data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint,

---

87 740 ILL. COMP. STAT. 14/10 (2008).

88 *Compare* WASH. REV. CODE § 19.375 (2017), *with* TEX. BUS. & COM. CODE § 503.001 (2009), *and* 740 ILL. COMP. STAT. 14/1 (2008).

89 Capture or Use Biometric Identifier Act, TEX. BUS. & COM. CODE § 503.001 (2009).

90 *See, e.g.*, TEX. BUS. & COM. CODE § 503.001(a) (2009) ("In this section, "biometric identifier" means a retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry.").

> voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify a specific individual. "Biometric identifier" does not include a physical or digital photograph, video or audio recording or data generated therefrom, or information collected, used, or stored for health care treatment, payment, or operations under the federal health insurance portability and accountability act of 1996.[91]

B. Collectors of Biometric Information

All three statutes address the protection of biometric identifiers in the possession of private corporations, although each statute uses different language in referring to such entities.[92] BIPA defines such parties as "private entities" meaning "any individual, partnership, corporation, limited liability company, association, or other group, however organized" and specifically excludes a "State or local government agency" or "any court of Illinois, a clerk of the court, or a judge or justice thereof."[93] Conversely, WPBA and CUBI refer to such parties as a "person."[94] According to WPBA, a person is "an individual, partnership, corporation, limited liability company, organization, association, or any other legal or commercial entity, but does not include a government agency."[95] For the purposes of this discussion, "private entity" will be used to refer to the subjects of all three statutes.

C. Retention

Each statute addresses the retention of biometric data with different levels of specificity. The WBPA states:

> (4) A person who knowingly possesses a biometric identifier of an individual that has been enrolled for

---

91 WASH. REV. CODE § 19.375.010 (2017).

92 *Compare* WASH. REV. CODE § 19.375 (2017), *with* TEX. BUS. & COM. CODE § 503.001 (2009), *and* 740 ILL. COMP. STAT. 14/1 (2008).

93 740 ILL. COMP. STAT. 14/10 (2008).

94 *Compare* WASH. REV. CODE § 19.375 (2017), *with* TEX. BUS. & COM. CODE § 503.001 (2009), *and* 740 ILL. COMP. STAT. 14/1 (2008).

95 WASH. REV. CODE § 19.375.010 (2017).

> a commercial purpose: (b) May retain the biometric identifier no longer than is reasonably necessary to (i) Comply with a court order, statute, or public records retention schedule specified under federal, state, or local law; (ii) Protect against or prevent actual or potential fraud, criminal activity, claims, security threats, or liability; and (iii) Provide the services for which the biometric identifier was enrolled.[96]

The WBPA makes no mention of a deletion timeline for biometric data collected. CUBI and BIPA, by contrast, both address this possibility in their text. CUBI states "(c) A person who possesses a biometric identifier of an individual that is captured for a commercial purpose: (3) shall destroy the biometric identifier within a reasonable time, but not later than the first anniversary of the date the purpose for collecting the identifier expires . . . ."[97] BIPA's retention requirements are the most comprehensive, stating:

> Section 15. Retention; collection; disclosure, destruction.
> (a) A private entity in possession of biometric identifiers or biometric information must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first. Absent a valid warrant or subpoena issued by a court of competent jurisdiction, a private entity in possession of biometric identifiers or biometric information must

---

96 WASH. REV. CODE § 19.375.020 (2017).

97 TEX. BUS. & COM. CODE § 503.001(c)(3) (2009).

> comply with its established retention schedule and destruction guidelines.[98]

D. Reasonable Care

The three state laws also all rely on some version of a "reasonable care" objectivity standard when addressing how biometric data in the employ of a private entity or person should be protected, with each statute producing a different outcome.[99] Illinois's BIPA includes the most detailed description of how biometric data is to be protected:

> Section 15. Retention; collection; disclosure, destruction.
> (e) A private entity in possession of a biometric identifier or biometric information shall: (1) store, transmit, and protect from disclosure all biometric identifiers and biometric information using the reasonable standard of care within the private entity's industry; and (2) store, transmit, and protect from disclosure all biometric identifiers and biometric information in a manner that is the same as or more protective than the manner in which the private entity stores, transmits, and protects other confidential and sensitive information.[100]

Illinois's standard for biometric data protection can be boiled down to two main attributes: using reasonable care as defined within a private entity's industry and treating it similarly to how the individual entity treats other confidential and sensitive information.[101] The first requirement is effectively an objectivity standard focused on market custom by measuring a private entity's protection against other similar entities in the market or industry.[102] The second measures an entity's protection of biometric data

---

98 740 ILL. COMP. STAT. 14/15 (2008).

99 *Compare* WASH. REV. CODE § 19.375 (2017), *with* TEX. BUS. & COM. CODE § 503.001 (2009), *and* 740 ILL. COMP. STAT. 14/15 (2008).

100 740 ILL. COMP. STAT. 14/15 (2008).

101 *See* 740 ILL. COMP. STAT. 14/15(e) (2008).

102 *See* 740 ILL. COMP. STAT. 14/15(e)(1) (2008).

against its protection of other sensitive data.[103] Similarly, Texas's CUBI has two primary requirements:

> (c) A person who possesses a biometric identifier of an individual that is captured for a commercial purpose: (2) shall store, transmit, and protect from disclosure the biometric identifier using reasonable care and in a manner that is the same as or more protective than the manner in which the person stores, transmits, and protects any other confidential information the person possesses . . . [104]

Unlike BIPA's first requirement, CUBI's reasonable care standard is a regular objectivity standard.[105] CUBI's second requirement, however, is effectively the same as BIPA's second, tasking private entities in possession of biometric data to protect it as it would other confidential information.[106] WBPA has only one primary requirement for protecting biometric data, merely tasking persons who knowingly possesses commercially-purposed biometric data that has been enrolled to "take reasonable care to guard against unauthorized access to and acquisition of biometric identifiers that are in possession or under the control of the person . . ."[107] WBPA's requirement is, like CUBI's first requirement, a reasonable care objectivity standard.[108]

E. The Sale and Release of Biometric Data

Each statute broadly prevents private entities in possession of biometric data from selling, leasing, trading, or otherwise profiting that data.[109] Notably, BIPA is the only statute of the three to distinguish between sale and disclosure of biometric data.

---

103 *See* 740 ILL. COMP. STAT. 14/15(e)(2) (2008).

104 TEX. BUS. & COM. CODE § 503.001 (2009).

105 *Compare* TEX. BUS. & COM. CODE § 503.001(c)(2) (2009), *with* 740 ILL. COMP. STAT. 14/15(e) (2008).

106 *Compare* TEX. BUS. & COM. CODE § 503.001(c)(2) (2009), *with* 740 ILL. COMP. STAT. 14/15(e) (2008).

107 WASH. REV. CODE § 19.375.020 (2017).

108 *Compare* WASH. REV. CODE § 19.375.020 (2017), *with* TEX. BUS. & COM. CODE § 503.001(c)(2) (2009).

109 *Compare* WASH. REV. CODE § 19.375 (2017), *with* TEX. BUS. & COM. CODE § 503.001 (2009), *and* 740 ILL. COMP. STAT. 14/15 (2008).

Regarding the sale of biometric data, BIPA's requirements prohibit such practices absolutely, stating: "No private entity in possession of a biometric identifier or biometric information may sell, lease, trade, or otherwise profit from a person's or a customer's biometric identifier or biometric information."[110] For disclosure or release of biometric data, BIPA states:

> (d) No private entity in possession of a biometric identifier or biometric information may disclose, redisclose, or otherwise disseminate a person's or a customer's biometric identifier or biometric information unless: (1) the subject of the biometric identifier or biometric information or the subject's legally authorized representative consents to the disclosure or redisclosure; (2) the disclosure or redisclosure completes a financial transaction requested or authorized by the subject of the biometric identifier or the biometric information or the subject's legally authorized representative; (3) the disclosure or redisclosure is required by State or federal law or municipal ordinance; or (4) the disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.

Both CUBI and WBPA take a different approach, addressing the sale and disclosure of biometric data simultaneously. Such an approach allows for scenarios in which the sale of biometric data is allowed, unlike BIPA. CUBI provides:

> (c) A person who possesses a biometric identifier of an individual that is captured for a commercial purpose: (1) may not sell, lease, or otherwise disclose the biometric identifier to another person unless: (A) the individual consents to the disclosure for identification purposes in the event of the individual's disappearance or death; (B) the disclosure completes a financial transaction that the individual requested or authorized; (C) the

---

110 740 ILL. COMP. STAT. 14/15(c) (2008).

> disclosure is required or permitted by a federal statute or by a state statute other than Chapter 552, Government Code; or (D) the disclosure is made by or to a law enforcement agency for a law enforcement purpose in response to a warrant . . . .[111]

The WBPA, meanwhile, has an even broader list of exemptions than CUBI.[112] Most notably, the WBPA includes an exemption for disclosure and sale to any third party who contractually promises not to disclose the data or enroll it for use inconsistent with the original businesses uses.

F. Purpose of Law

Another provision shared by only two statutes is the explicit mention of a purpose for the law, included in Illinois's BIPA and the WBPA. Likely due to the real-world circumstances that lead to the drafting of BIPA, the Illinois statute's purpose is comprehensive and detailed:

> Section 5. Legislative findings; intent. The General Assembly finds all of the following:
> (a) The use of biometrics is growing in the business and security screening sectors and appears to

---

111 TEX. BUS. & COM. CODE § 503.001 (2009).

112 Here, the WBPA provides:

> (3) Unless consent has been obtained from the individual, a person who has enrolled an individual's biometric identifier may not sell, lease, or otherwise disclose the biometric identifier to another person for a commercial purpose unless the disclosure: (a) Is consistent with subsections (1), (2), and (4) of this section; (b) Is necessary to provide a product or service subscribed to, requested, or expressly authorized by the individual; (c) Is necessary to effect, administer, enforce, or complete a financial transaction that the individual requested, initiated, or authorized, and the third party to whom the biometric identifier is disclosed maintains confidentiality of the biometric identifier and does not further disclose the biometric identifier except as otherwise permitted under this subsection (3); (d) Is required or expressly authorized by a federal or state statute, or court order; (e) Is made to a third party who contractually promises that the biometric identifier will not be further disclosed and will not be enrolled in a database for a commercial purpose inconsistent with the notice and consent described in this subsection (3) and subsections (1) and (2) of this section; or (f) Is made to prepare for litigation or to respond to or participate in judicial process.

WASH. REV. CODE § 19.375.020 (2017).

> promise streamlined financial transactions and security screenings. (b) Major national corporations have selected the City of Chicago and other locations in this State as pilot testing sites for new applications of biometric-facilitated financial transaction, including finger-scan technologies at grocery stores, gas stations, and school cafeterias. (c) Biometrics are unlike other unique identifiers that are used to access finances or other sensitive information. For example, social security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at the heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions. (d) An overwhelming majority of members of the public are weary of the use of biometrics when such information is tired to finances and other person information. (e) Despite limited State law regulating the collection, use, safeguarding, and storage of biometrics, many members of the public are deterred from partaking in biometric identifier-facilitated transactions. (f) The full ramifications of biometric technology are not fully known. (g) The public welfare, security, and safety will be served by regulating the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information.[113]

Particularly of note in this statement of purpose is reference to both public weariness of biometric technology and the acknowledgment of unknown dangers that biometric data might present.[114] This motivation suggests that Illinois lawmakers were likely particularly worried about the danger of biometric data breaches and that BIPA, as a result, was cautiously drafted with

---

113 740 ILL. COMP. STAT. 14/5 (2008).

114 *See* 740 ILL. COMP. STAT. 14/5(d)–(f) (2008).

these concerns in mind. The WBPA's statement of intent is more concise and straightforward:

> The legislature finds that citizens of Washington are increasingly asked to disclose sensitive biological information that uniquely identifies them for commerce, security, and convenience. The collection and marketing of biometric information about individuals, without consent or knowledge of the individual whose data is collected, is of increasing concern. The legislature intends to require a business that collects and can attribute biometric data to a specific uniquely identified individual to disclose how it uses that biometric data, and provide notice to and obtain consent from an individual before enrolling or changing the use of that individual's biometric identifiers in a database.[115]

Texas's CUBI lacks any specific mention of the Texas legislatures intent or purpose behind passing the Act.[116]

G. Remedies

Each of these statutes offers mechanisms by which a private entity in violation of the law can be held accountable.

1. The Private Right of Action

The most direct approach is a private right of action provided by the first law to address biometric authentication, BIPA:

> Section 20.
> Right of action. Any person aggrieved by a violation of this Act shall have a right of action in a State circuit court or as a supplemental claim in federal district court against an offending party. A prevailing party may recover for each violation: (1) against a private entity that negligently violates a

---

115 WASH. REV. CODE § 19.375.900 (2017).

116 *See* TEX. BUS. & COM. CODE § 503.001 (2009).

> provision of this Act, liquidated damages of $1,000 of actual damages, whichever is greater; (2) against a private entity that intentionally or recklessly violates a provision of this Act, liquidated damages of $5,000 or actual damages, whichever is greater; (3) reasonable attorneys' fees and costs, including expert witness fees and other litigation expenses; and (4) other relief, including an injunction, as the State or federal court may deem appropriate.[117]

BIPA is the only statute of the three to offer a private right of action.[118]

2. State Attorneys General Enforcement

CUBI provides its own civil action through the state attorney general, stating that "[a] person who violates this section is subject to a civil penalty of not more than $25,000 for each violation. The attorney general may bring an action to recover the civil penalty."[119] Similarly to CUBI, WBPA may only be enforce through the state attorney general.[120] Unlike CUBI, however, this enforcement mechanism is not provided in the text of the statute but through the Washington Consumer Protection Act.[121] Violations of the WBPA are considered unfair or deceptive acts or methods of competition and carry a maximum civil penalty of two-thousand dollars.[122]

H. Additional Provisions

Uniquely, the WBPA is the only biometric privacy statute to date that includes something called the "security purpose"

---

117 740 ILL. COMP. STAT. 14/20 (2008).

118 *See id.*

119 TEX. BUS. & COM. CODE § 503.001(d) (2009).

120 *Compare* WASH. REV. CODE § 19.375.030(2) (2017), *with* TEX. BUS. & COM. CODE § 503.001(d) (2009).

121 *See* Civil Penalties, WASH. REV. CODE § 19.86.140 (1983); Lara Tumeh, *Washington's New Biometric Privacy Statute and How It Compares to Illinois and Texas Law*, BLOOMBERG LAW: PRIVACY LAW WATCH (Oct. 16, 2017), https://www.alston.com/-/media/files/insights/publications/2017/10/tumehbiometriclaws-privacylawwatch.pdf [https://perma.cc/CQ9K-PVWV].

122 *See* WASH. REV. CODE § 19.86.140 (1983).

exemption.[123] The statute gives a list of general requirements that private entities are expected to meet to remain in compliance with the WBPA.[124] The seventh provision of this section provides that "[n]othing in this section requires an entity to provide notice and obtain consent to collect, capture, or enroll a biometric identifier and store it in a biometric system, or otherwise, in furtherance of a security purpose."[125] This purpose, as defined in the statute's definitions section, means "the purpose of preventing shoplifting, fraud, or any other misappropriation or theft of a thing of value, including tangible and intangible goods, services, and other purposes in furtherance of protecting the security or integrity of software, accounts, applications, online services, or any person."[126]

CUBI also contains a unique provision regarding retention of employee biometrics: "If a biometric identifier captured for a commercial purpose has been collected for security purposes by an employer, the purpose for collecting the identifier under Subsection (c)(3) is presumed to expire on termination of the employment relationship."[127]

IV. THE BENEFITS OF A PRIVATE RIGHT OF ACTION AND OTHER POSSIBLE IMPROVEMENTS

This Part will address the strengths and weaknesses of the current enacted biometric data privacy statutes, discuss how the Illinois Biometric Information Privacy Act's private right of action can provide a model for future biometric privacy laws, and explore novel provisions future statutes might incorporate. Section IV.A will discuss how BIPA's provisions might provide the best protection for consumers concerned about their biometric security over CUBI and the WBPA. Section IV.B will examine the insufficiencies of the Washington Biometric Privacy Act and the Capture or Use Biometric Identifier Act. Section IV.C will address the ways in which the Washington Biometric Act and the Texas

---

123 *See* WASH. REV. CODE § 19.375.020 (2017).
124 *See id.*
125 *Id.*
126 WASH. REV. CODE § 19.375.010 (2017).
127 TEX. BUS. & COM. CODE § 503.001(c)(2) (2009).

Capture or Use Biometric Identifier Act can also contribute to the future development of biometric privacy statutes. Finally, Section IV.D will discuss novel ways in which future biometric privacy statutes can be improved.

A. The Biometric Information Privacy Act's Supremacy

1. The Strength of the Private Right of Action

Illinois's Biometric Information Privacy Act was created in the aftermath of a private entity dissolving, leaving questions for consumers about what would become of their sensitive financial and biometric data.[128] The act's purpose, in many ways, reflects modern anxieties surrounding data insecurity with mentions of public wariness of novel technology and the potential unknown risks involved. While biometric authentication technology is used more often by the average adult today,[129] many Americans believe they have lost control of their data and are unsure of how to regain it.[130] This sentiment could hardly be considered surprising considering how few data breach victims are able to successfully hold compromised private entities legally accountable for their failure to protect sensitive information.[131] To that end, the inclusion of BIPA's private right of action is perhaps one of the most unique and vital aspects of the statute. The right to hold compromised private entities personally accountable for their failure to adequately secure sensitive biometric data is rarely enshrined so explicitly for data breach victims. The right of action provides a mechanism through which compromised consumers can avoid the class certification challenges present in already rare data breach class action suits. The private right can also provide an alternate means to bring suit against private entities with forced arbitration clauses that specifically prohibit class action suits.

---

128 *See* Kay, *supra* note 51, at 1.

129 *See* Koma, *supra* note 17.

130 *See* Mary Louise Kelly, *Most Americans Feel They've Lost Control of Their Online Data*, NPR (Apr. 10, 2018), https://www.npr.org/2018/04/10/601148172/most-americans-feel-theyve-lost-control-control-of-their-online-data [https://perma.cc/SDB7-EUJJ].

131 *See* discussion *supra* Sections I–II.

The damages floors enshrined in BIPA's right of action are also worth noting. A prevailing party can recover $1,000 or actual damages, whichever is greater, should a private entity negligently violate BIPA.[132] That damage floor rises to $5,000 if it is found that the private entity intentionally or recklessly violated the statute.[133] The right of action also provides for attorney's fees and costs.[134] While BIPA's critics have argued the statute's right of action may lead to frivolous lawsuits,[135] there is little to suggest that BIPA suits have become unduly burdensome on Illinois businesses. Given the surge in BIPA related class action suits, it is possible that the inclusion of damage floors might make BIPA unduly burdensome on smaller businesses that may be subject to BIPA suits.[136] Such disincentivizing, however, is likely in the best interest of data security as small businesses are often at greater risk of cyberattacks and small to medium sized businesses account for over half of all data breaches that occur daily.[137] Further, the inclusion of damage floors in BIPA likely help incentivize larger businesses to make sure they remain compliant with the statute's conditions.

Similar to broader data breach suits, questions have arisen as to whether actual injury must be proven to proceed with BIPA's right of action. In *McCollough v. Smarte Carte, Inc.*, the plaintiff brought suit against Smart Carte, Inc. for its failure to obtain her written consent for her biometric identifier or to inform her of their data retention policy after she used one of their fingerprint enabled

---

132 *See* 740 ILL. COMP. STAT. 14/20 (2008).

133 *See id*.

134 *See id*.

135 *See* Karla Grossenbacher & Christopher W. Kelleher, *Hazards Ahead: Uptick In Biometric Privacy Laws Can Put Employees In Hot Seat*, SEYFARTH SHAW LLP (Oct. 3, 2017), https://www.laborandemploymentlawcounsel.com/2017/10/hazards-ahead-uptick-in-biometric-privacy-laws-can-put-employers-in-hot-seat/ [https://perma.cc/P2G3-HKL7].

136 *See id*; Steven Pearlman, Eddie Young & Alex Weinstein, *The New Wave OF Employee Biometrics Class Actions*, LAW360 (Oct. 13, 2017, 11:24 AM), https://www.law360.com/cybersecurity-privacy/articles/972212/the-new-wave-of-employee-biometrics-class-actions?nl_pk=d5154baa-3c0f-408d-8f5e-e2a35a0f4b2c&utm_source=newsletter&utm_medium=email&utm_campaign=cybersecurity-privacy&read_more=1 [https://perma.cc/YC5R-WSQP].

137 *See* INSUREON, *supra* note 12.

lockers.[138] The court in *McCollough* found the plaintiff lacked Article III standing as Smart Carte's violation of BIPA was merely technical and created no concrete injury.[139] Unlike some data breach suits however, economic harm is not necessarily required by courts to bring a successful BIPA suit.[140] In *Monroy v. Shutterfly, Inc.*, Shutterfly automatically collected the facial geometry of the plaintiff without his consent when a third party uploaded a picture of his face and tagged it with his name.[141] Although the plaintiff's information was not compromised, the court recognized a violation of his privacy as concrete harm.[142]

This matter was most recently addressed in *Rosenbach v. Six Flags*. In *Rosenbach*, Six Flags, an amusement park, collected the plaintiff's fingerprint identifier in exchange for entering the park using a "season pass."[143] When doing so, however, Six Flags gave the plaintiff no notice and did not obtain written consent from him.[144] Consequently, the plaintiff's mother, Stacy Rosenbach, brought suit on his behalf. The Court, which did not cite *Spokeo* in its holding,[145] paid special attention to the Illinois General Assembly's stated purpose of BIPA, stating:

> It is clear that the legislature intended for this provision to have substantial force. When private entities face liability for failure to comply with the law's requirements without requiring affected individuals or customers to show some injury beyond violation of their statutory rights, those entities have the strongest possible incentive to conform to the law and prevent problems before the

---

138 2016 U.S. Dist. LEXIS 100404, at *1–3 (N.D. Ill. Aug. 1, 2016).

139 *See id*. at *5.

140 *See generally* Rosenbach v. Six Flags Entm't Corp., 2017 IL App (2d) 170317; Monroy v. Shutterfly, Inc., No. 16-C-10984, 2017 U.S. Dist. LEXIS 149604, at *27 (N.D. Ill. Sep. 15, 2017).

141 *See Monroy*, 2017 U.S. Dist. LEXIS 149604, at *1–3.

142 *See id*. at *26–27.

143 Rosenbach v. Six Flags Entm't Corp., 2019 IL 123186, at ¶¶ 4–9.

144 *See id.*; *Season Passes & Memberships*, SIX FLAGS (July 2014), https://web.archive.org/web/20140706110138/https://www.sixflags.com/greatamerica/store/season-passes [https://perma.cc/FCG8-CSJX].

145 *See Rosenbach*, 2019 IL.

> occur and cannot be undone. Compliance should not be difficult; whatever expenses a business might incur to meet the law's requirements are likely to be insignificant compared to the substantial and irreversible harm that could result if biometric identifiers and information are not properly safeguarded; and the public welfare, security, and safety will be advanced. That is the point of the law. To require individuals to wait until they have sustained some compensable injury beyond violation of their statutory rights before they may seek recourse, as defendants urge, would be completely antithetical to the Act's preventative and deterrent purposes.[146]

The Court makes it clear that the actual harm question befuddling other courts dealing with data breach victims is simply not a relevant consideration when the legislature is explicit and the potential for harm is this high:

> When a private entity fails to adhere to the statutory procedures, as defendants are alleged to have done here, "the right of the individual to maintain [his or] her biometric privacy vanishes into thin air. The precise harm the Illinois legislature sought to prevent is then realized." This is no mere "technicality." The injury is real and significant.[147]

Rosenbach's language is not insignificant. The Illinois State Supreme Court's declaration that a per se violation of BIPA is

---

[146] *Rosenbach*, 2019 IL 123186, at ¶ 37. Curiously, but for the Illinois General Assembly's inclusion of BIPA's purpose, tension might exist between the holdings in *Spokeo* and *Rosenbach*. The Court's opinion in *Spokeo*, while recognizing intangible harms as concrete, explicitly clarified that a plaintiff must allege more than a "bare procedural violation" of the statute that is "divorced from" the real harms that FCRA is designed to prevent. Spokeo, Inc., v. Robins, 136 S. Ct. 1540, 1549 (2016). The Court's opinion in *Rosenbach* makes clear that Six Flags' violation of BIPA is concrete because, according to statute's purpose, it is the exact kind of privacy harm BIPA was created to prevent. *See Rosenbach*, 2019 IL 123186, at ¶ 34 (citing Patel v. Facebook Inc., 290 F. Supp. 948, 954 (N.D. Cal. 2018)).

[147] *See Rosenbach*, 2019 IL 123186, at ¶ 34 (citing Patel v. Facebook Inc., 290 F. Supp. 948, 954 (N.D. Cal. 2018)).

harm sufficient to form a cause of action is exceptionally pro-consumer, holding irresponsible data firms accountable for failing to take even basic statutory measures to protect biometric privacy.[148] This holding represents a forward-thinking judicial perspective in addressing statutorily protected privacy harms. For these reasons, BIPA's private right of action, along with a comprehensive statement of purpose on behalf of the drafting legislatures, should be incorporated in future biometric privacy statutes serious about protecting privacy rights.

2. A Prohibition on Selling Biometric Data

BIPA's restrictions against private entities selling consumer biometric data is also exemplary compared to its successors. Although all three statutes contain provisions allowing for the disclosure of biometric data should the completion of a financial transaction or federal law require,[149] BIPA strictly forbids private entities from selling, leasing, trading, or otherwise profiting from a consumer's biometric data with no exceptions.[150] While both CUBI and WBPA generally disallow the selling of user biometric data, both statutes have a host of exemptions to this requirement, some questionable.[151] In Texas, a private entity may sell biometric data in the event of a user's "disappearance or death."[152] While a deceased consumer might not have any need for their biometric information, there does not seem to be a compelling reason why that data could be sold as opposed to destroyed. The WBPA offers an even larger list of exemptions, going as far as to allow a private entity to sell biometric data to third parties so long as the third party "contractually promises" not to further disclose or enroll the information.[153] Such a disclosure appears to have a very low threshold for a private entity and could potentially raise further questions as to the statute's ability to adequately protect data. By

---

148 *See id.*

149 *Compare* WASH. REV. CODE § 19.375.020 (2017), *with* TEX. BUS. & COM. CODE § 503.001 (2009), *and* 740 ILL. COMP. STAT. 14/15 (2008).

150 *See* 740 ILL. COMP. STAT. 14/15(c) (2008).

151 *Compare* WASH. REV. CODE § 19.375.020 (2017), *with* TEX. BUS. & COM. CODE § 503.001 (2009).

152 TEX. BUS. & COM. CODE § 503.001 (2009).

153 WASH. REV. CODE § 19.375.020 (2017).

outright disallowing the sale of user biometric data, BIPA requires a higher level of security from private entities and disincentivizes the sale of consumer data.

3. The Written Retention & Deletion Policy

Finally, BIPA's requirement of a written policy surrounding biometric collection that must be public to consumers and enforced by a private entity is a strong policy. Such a provision helps to incentivize private entities to incorporate a compliance aspect in their collection of biometric data which, ideally, can help to prevent future litigation under BIPA. Further, a public biometrics policy can help consumers make more informed choices about who they choose to store their sensitive data with, allowing them to feel more in control of their own data.

B. The Washington Biometric Act and Capture or Use Biometric Identifier Act Information Act's Insufficiency

1. The Security Purpose Exception

While each of the three state biometric privacy statutes have flaws in how they regulate the protection of user data, the Washington Biometric Privacy Act's shortcomings are particularly troubling. Despite being the most recent of the three statutes, several provisions of the WBPA raise serious questions about its effectiveness in regulating private entities, none more so than the "security purpose" exception. While biometric authentication is not exclusively used as a means of security, it does account for the overwhelming majority of its use.[154] Should this exception have only applied to tangible goods or services, it is possible that the purpose of the WBPA could remain intact, although unduly burdened. However, the broadness of this exception's language, and the vagueness of the term "other purposes," are difficult to overstate. Given that one of the main purposes of biometric technology is to secure physical and digital spaces from unverified

---

[154] *See* Alexandro Pando, *Beyond Security: Biometrics Integration into Everyday Life*, FORBES (Aug. 4, 2017, 8:00 AM), https://www.forbes.com/sites/forbestechcouncil/2017/08/04/beyond-security-biometrics-integration-into-everyday-life/#38724d81431f [https://perma.cc/27N3-TLN7].

users, this exception effectively undermines the WBPA's effectiveness.

Beyond the security purpose, there are also concerns about the WBPA's definition of "biometric identifiers." The statute lists a general definition for a biometric identifier before listing examples, however, facial recognition is notably absent from the types of identifiers listed.[155] Although Representative Jeff Morris, the WBPA's prime sponsor, has argued that the exclusion of facial recognition from the definition does not necessarily preclude its inclusion, some attorneys worry that courts will exclude that particular biometric identifier when assessing the WBPA opening citizens up to the danger of having their faces catalogued without their knowledge or consent.[156]

2. State Attorneys General Action

While it is possible to enforce both CUBI and WBPA through their respective state attorney generals, this option does not offer victims of data breaches the opportunity to be compensated for a private entity's failure to protect their data.[157] As noted in Section II.D, AGs, while perhaps instrumental in shaping data privacy norms, have the ultimate discretion in choosing what lawsuits to file and are susceptible to political capture.[158] While scholars have noted that it is unlikely that all fifty state AGs would be politically captured by anti-consumer interests,[159] this is a small comfort to consumers in captured states.[160]

---

155 *See* WASH. REV. CODE § 19.375.010 (2017).

156 *See* Paul Shukovsky, *Washington Biometric Privacy Law Lacks Teeth of Illinois Cousin*, BLOOMBERG (July 18, 2017), https://www.bna.com/washington-biometric-privacy-n73014461920/ [https://perma.cc/994F-CZZ5].

157 *See supra* notes 120–22 and accompanying text.

158 *See supra* Section II.D.

159 *See* Citron, *supra* note 83, at 803–04.

160 Further, the author of this Note was unable to find any Texas suits brought under CUBI through Westlaw, Westlaw Litigation Analytics, or Lexis as of February 27, 2019. While the absence of evidence is not evidence of absence, the dearth of information surrounding CUBI AG suits is likely the result of few, if any, CUBI suits ever being filed. *See* Fred Shapiro, *The Absence of Proof*, FREAKONOMICS (Sept. 29, 2011, 2:32 PM), http://freakonomics.com/2011/09/29/the-absence-of-proof/ [https://perma.cc/9SCW-3ZS4]. On March 22, 2019, the author submitted a Public Information Act Request to the Texas Attorney General requesting information or documentation relating to any actions

C. What the Other Biometric Statutes Have to Offer

1. The Washington Biometric Privacy Act

Although the WBPA might largely be ineffective at protecting data, the statute's novel focus on the regulation of the enrollment of biometric data as opposed to its collection might be a beneficial element to incorporate into future biometric privacy laws. Both BIPA and CUBI primarily regulate the ways in which private entities can collect and capture biometric data.[161] CUBI states that "a person may not capture a biometric identifier of an individual for a commercial purpose unless the person: (1) informs the individual before capturing the biometric identifier; and (2) receives the individual's consent to capture the biometric identifier."[162] Similarly, BIPA states:

> (b) No private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information, unless it first: (1) informs the subject or the subject's legally authorized representative in writing that the biometric identifier or biometric information is being collected or stored; (2) informs the subject or the subject's legally authorized representative in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and (3) receives a written release executed by the subject of the

---

or litigation brought under the Capture or Use Biometric Identifier Act from the statute's inception through February 27, 2019, including matters ending in settlements. On April 5, 2019, the Office of the Attorney General of Texas responded to Public Information Request No. R000722 stating that "the OAG has reviewed its files and has no information responsive to your request." Letter from June B. Harden, Assistant Attorney General, Office of the Attorney General of Texas, to Maya Rivera, Managing Editor, Fordham Intellectual Property, Media & Entertainment Law Journal (Apr. 5, 2019) (on file with author). Consequently, it is reasonable to conclude that the Office of the Attorney General of Texas has never brought a CUBI action since the statute's inception, highlighting the potential inefficiency of State AG enforcement.

[161] *Compare* TEX. BUS. & COM. CODE § 503.001 (2009), *with* 740 ILL. COMP. STAT. 14/15 (2008).

[162] TEX. BUS. & COM. CODE § 503.001 (2009).

> biometric identifier or biometric information or the subject's legally authorized representative.[163]

Conversely, the WBPA states that "a person may not enroll a biometric identifier in a database for a commercial purpose, without first providing notice, obtaining consent, or providing a mechanism to prevent the subsequent use of a biometric identifier for a commercial purpose."[164] According to the statute "'enroll' means to capture a biometric identifier of an individual, convert it into a reference template that cannot be reconstructed into the original output image, and store it in a database that matches the biometric identifier to a specific individual."[165]

The divergence from BIPA and CUBI is significant as it places a greater emphasis on how private entities use the biometric data they collect by only regulating data that is being stored in a database to be used again in the future. Such an approach can prevent private entities who may be collecting biometric data for a very limited period of time from being subject to the various conditions of the WBPA. Further, the definition of "enroll" appears to prescribe a specific format in which biometric data should be stored that prevents the identifier from being reconstructed from the data to the original image. This templating can make biometric identifiers more difficult to steal as hackers who steal biometric data will not be able to easily reconstruct the original identifier. Finally, while BIPA and CUBI both require private entities to inform consumers and receive their express consent before capturing biometric data, the WBPA requires only one of three conditions: notice, consent, or a mechanism to unenroll one's data.[166] These requirements appear to be less burdensome and more adaptable then the requirements for capturing such data under BIPA or CUBI allowing for data enrollment on a flexible, individualized basis. Overall, these enrollment requirements combined with the positive elements of

---

163 740 ILL. COMP. STAT. 14/15 (2008).
164 WASH. REV. CODE § 19.375.020 (2017).
165 WASH. REV. CODE § 19.375.010 (2017).
166 *See* WASH. REV. CODE § 19.375.020 (2017).

BIPA could make for stronger biometric privacy statutes in the future.

2. The Capture or Use Biometric Identifier Act

CUBI is notably the only state biometric privacy statute to date that contains a provision addressing the retention and deletion of employee biometric data, specifically requiring that employers delete such data shortly after an employee's termination.[167] With recent surveys suggesting that upwards of 64% of workplaces now incorporate biometrics for security and business purposes, this prescient CUBI provision would make for a wise addition to future biometric privacy legislation.[168]

D. Other Considerations for Future Biometric Privacy Statutes

There are several additional measures that future biometric privacy statutes can incorporate to best protect privacy rights and ensure an informed judiciary.

1. Meaningful Consent via Opt-out and Alternatives

As businesses increasingly adopt biometric measures for employees and consumers,[169] it is paramount that consumers be given real choices in determining who to entrust their data to and when. Key to this interest is an individual's right to opt-out of a service or aspects of a service whenever she feels a business can no longer be trusted. It is not sufficient that consent must only be given once for a firm to have potentially indefinite use of biometric data; the consent must be meaningful, meaning certain uses of the data should be optional and the consent can be revoked at any time. A meaningful consent provision, as enshrined in the Fair Information Practice Principles and, now, in the General Data Protection Regulations ("GDPR") in the European Union, would guarantee that an individual has ultimate control over their

---

167 TEX. BUS. & COM. CODE § 503.001(c)(2) (2009).

168 *See* Roy Maurer, *More Employers Are Using Biometric Authentication*, SOC. HUMAN RES. MGMT (Apr. 6, 2018), https://www.shrm.org/resourcesandtools/hr-topics/technology/pages/employers-using-biometric-authentication.aspx [https://perma.cc/4BRZ-QGUV].

169 *See* VISA, *supra* note 5.

biometric data, a type of control that the sensitivity of biometric information should warrant.[170] When a consumer triggers such a provision, the target business would be expected to offer an alternative means of authentication to the user and, once in place, delete the user's biometric identifier from its records. While some firms, now including Six Flags,[171] allow alternative means of authentication when biometrics are involved, enshrining a mandatory opt-out procedure that incorporates meaningful consent would better hold firms to account in recognizing the privacy rights of consumers. Failure to comply with such a provision could result in liability via the private right to action.

2. Appointment of Special Masters

Another suggestion for improving future biometric privacy statutes would be to incorporate a mechanism to allow judges to consult with neutral, third party experts familiar with best data security practices. While the statutes' reasonable care standards

---

[170] *See The Fair Information Principles*, PRIVACY FIRST, https://www.privacyfirst.nl/acties-3/item/154-the-fair-information-principles-canada.html [https://perma.cc/E5ND-DLS8] (last visited Mar. 12, 2019); Regulation 2016/679 on the Protection of Natural Persons With Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. L 119, art. 7. The GDPR explicitly defines "biometric data" under Article 4 as "personal data resulting from specific technical processing relating to the physical, physiological, or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data." Regulation 2016/679 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. L 119, ch. 1, art. 4. The GDPR's inclusion of "physical, physiological, [and] behavioural characteristics" as biometric identifiers appear to be an implicit acknowledgment of the potential for biometric technology to evolve beyond our current understanding. *See* Danny Ross, *"Processing Biometric Data? Be Careful, Under the GDPR,"* IAPP (Oct. 31, 2017), https://iapp.org/news/a/processing-biometric-data-be-careful-under-the-gdpr/ [https://perma.cc/T984-MUY4]. Businesses collecting biometric identifiers of European Union citizens should be especially wary of how such information is stored given the GDPR's harsh penalties. *See generally "GDPR Enforcement and Penalties,"* IT GOVERNANCE (last visited Mar. 13, 2019), https://www.itgovernance.co.uk/dpa-and-gdpr-penalties [https://perma.cc/7CVF-YYF7].

[171] *See Season Passes & Memberships*, SIX FLAGS (2019), https://web.archive.org/web/20190122020232/https://www.sixflags.com/greatamerica/store/season-passes [https://perma.cc/45DY-D529].

provide a general guideline as to how to appropriately store and protect biometric data, it can be difficult to say what exactly reasonable care entails with regards to data security. Conversely, it is unreasonable and likely impossible to prescribe specific methods of data security as technology often moves so quickly that legislators cannot be expected to regularly update statutes with the latest best security practices. Consequently, giving judges the ability to consult with data security experts, à la Federal Rule of Evidence 706, when the appropriate level of security is unclear might provide for more equitable outcomes in future biometric privacy suits, especially as methods for data security evolve over the years.[172]

Some courts currently allow the appointment of "special masters" at the behest of parties or judges which allow a judge to delegate certain trial processes to a subject-matter expert capable of verifying specialized information.[173] These special masters have been used to supervise discovery, oversee settlement negotiations, and, usefully here, make recommendations to attorneys regarding damages in cases with difficult fact patterns.[174] Including provisions recommending the use of such special masters might be beneficial in determining whether a privacy defendant employed appropriate encryption and security of biometric data when a breach occurs.

CONCLUSION

In "Privacy As Trust," Ari Waldman notes that "strong trust norms are what allow sharing and social interaction to occur."[175] When it comes to data as sensitive and irreplaceable as biometric identifiers, trust placed in private entities is especially strong.

---

172 *See* FED. R. EVID. 706.

173 *See* Shira Schiendlin, *The Use of Special Masters in Complex Cases*, LAW360 (Aug. 15, 2017), https://www.law360.com/articles/950395/the-use-of-special-masters-in-complex-cases [https://perma.cc/6YKM-Q5LK].

174 *See id.*

175 ARI EZRA WALDMAN, PRIVACY AS TRUST: INFORMATION PRIVACY FOR AN INFORMATION AGE 6 (2018).

Today, however, this trust is beginning to break down.[176] Many Americans worry that they have no control over their data and do not know how to reclaim it.[177] When a data breach occurs, victims can be anxious about the heightened risk of identity theft and fraud they find themselves in, even when the data stolen can be changed or otherwise rendered useless.[178] With biometric data, the risk a data breach poses is not temporary, but can last for as long as the victim may live. The Biometric Information Privacy Act was drafted at a time when legislators shared these concerns and were worried about the potential ramifications of a biometric data breach.[179] As it happens, this wariness was prescient. The strict restrictions on the sale of biometric data and the inclusion of a private right of action with high damage floors were, in a very real sense, experimental as a biometric privacy statute had never been created before. However, these elements both prioritize the safety of consumer biometric data and empower consumers to hold private entities accountable in a way that is almost unheard of in data privacy law today. Though newer biometric privacy laws with fresh ideas have been introduced in the years since BIPA was made law, the most significant principles of the original statute should ultimately remain a lodestar for new biometric privacy legislation to follow. Further, the incorporation of meaningful consent and the appointment of special masters can also improve future biometric privacy, giving consumers more control over their data.

---

176 *See, e.g.*, Kim Hart, *Americans Don't Trust Tech Companies on Data Privacy*, AXIOS (Apr. 23, 2018), https://www.axios.com/distrust-social-media-firms-to-protect-privacy-survey-8b95db51-f137-46e3-a239-a5f304f0ac1b.html [https://perma.cc/45CX-RAAX].

177 *See* Kelly, *supra* note 130.

178 *See generally* Solove & Citron, *supra* note 72.

179 *See supra* Section III.F.