AN ANALYSIS ON BIOMETRIC PRIVACY DATA REGULATION: A PIVOT TOWARDS LEGISLATION WHICH SUPPORTS THE INDIVIDUAL CONSUMER'S PRIVACY RIGHTS IN SPITE OF CORPORATE PROTECTIONS

*Carla Llaneza**

I. INTRODUCTION

The ways in which the silhouette of an individual's face grants access to a cell phone, or the simple touch of a fingerprint, allow citizens to clear airport security customs, are examples of the power of biometric data and the impact it continues to have on daily American life.[1] Although there are several advantages that this budding technological advancement has brought to individuals, business corporations, and government agencies, the individualized consumer is not aware of the ways in which this data is used and disseminated.[2] Data privacy is one of the most pressing

* Carla Llaneza, *Juris Doctor* Candidate, May 2021, St. Thomas University School of Law, ST. THOMAS LAW REVIEW, Member; B.A. Public Communication, American University, 2016. I dedicate this publication to my family: my father Dr. Pedro Llaneza; my mother Esperanza Llaneza; and my sisters Sofia Kelly, Paola Llaneza, and Bianca Nicastri. This would not have been made possible without their constant love and support. I also want to thank the St. Thomas Law Review Executive Board for their mentorship throughout the writing process.

[1] *See Safety & Security of U.S. Borders: Biometrics*, U.S. DEP'T OF STATE–BUREAU OF CONSULAR AFFAIRS, https://travel.state.gov/content/travel/en/us-visas/other-visa-categories/safety.html (last visited on May 27, 2020) (defining the ways in which national security relies on the use of biometric identifiers, namely facial recognition technology and finger print scans, as it has reduced the use of stolen visas, protected the ports from threats of terrorism, and all around improved safety for Americans); *see also* Kim Porter, *Biometrics and Biometric Data: What is it and is it secure,* NORTON, https://us.norton.com/internetsecurity-iot-biometrics-how-do-they-work-are-they-safe.html (last visited May 27, 2020) (finding how the use of fingerprints and facial recognition technology has become common on smart phones, such as on the Apple iPhone and Android devices, as a way for consumers to authenticate their identity to gain access to their phones).

[2] *See* Lior Jacob Strahilevitz & Matthew B. Kugler, *Is Privacy Policy Language Irrelevant to Consumers,* COASE-SANDO INST. FOR L. & ECON. (Sept. 2016), https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?referer=https://scholar.google.com/&httpsredir=1&article=2465&context=law_and_economics (concluding that even though consumers found that Facebook's use of facial recognition software and Google and Yahoo's content analysis was "highly intrusive" they assented to the companies' privacy policies); *see also* Sharon Nakar & Dov Greenbam, *Now You See Me. Now You Still Do: Facial Recognition Technology and The Growing Lack of Privacy,* 23 B.U. J. SCI. & TECH L. 88, 90–91 (2018) (finding that government agencies need to

societal issues today, with American consumers calling on business corporations and lawmakers to address the issue.[3] It can be determined that this desire for more protection over personal private data will only continue to grow stronger as private companies further garner strategies in retrieval of sensitive information for profit.[4] Over the last sixteen years, private entities in the United States have gained access to a wealth of consumers' sensitive behavioral and physical information through the use of biometric data.[5] Biometrics data is "the measurement and statistical analysis of people's unique physical and behavioral characteristics."[6] Examples of biometric measures include fingerprints, facial recognition, iris recognition, and DNA matching.[7] Statistics show that the use of these biometric measures such as fingerprints, iris detection,

be careful when implementing facial recognition technology ("RFT") as it can lead to violations of privacy and other legal issues).

[3] *See The Societal ROI Index: A Measure for the Times We Find Ourselves In*, THE HARRIS POLL, 10 (2018), https://theharrispoll.com/wp-content/uploads/2018/11/Societal-ROI-Media-Deck-FINAL_FNL_High-Res.pdf (explaining the results of the Harris Poll survey which found that sixty-five percent of American survey participants believe that the most important social issue they want private sector companies to address is data privacy)*; see also* Lee Rainie, Sara Kiesler, et. al, *Anonymity, Privacy, and Security Online,* PEW RES. CTR. (Sept. 5, 2013), https://www.pewinternet.org/wp-content/uploads/sites/9/media/Files/Reports/2013/PIP_AnonymityOnline_090513.pdf (finding that "some 68% of internet users believe current laws are not good enough in protecting people's privacy online").

[4] *See* Gabriel J.X. Dance et al., *As Facebook Raised a Privacy Wall, It Carved a Wall for Tech Giants,* THE N. Y. TIMES (Dec. 18, 2018), https://www.nytimes.com/2018/12/18/technology/facebook-privacy.html (finding that "personal data has been the most prized commodity of the digital age by some of the most powerful companies in Silicon Valley and beyond"); *see also* Sarah Meyer, *Biometric Information – Knowing Who (and Where) You Are,* CPO MAG. (Dec. 24, 2018), https://www.cpomagazine.com/data-privacy/biometric-identification-knowing-who-and-where-you-are/ (concluding that multi-model data collection that lacks regulation may lead to breach and ultimate profit from companies).

[5] *See* Alan S. Wernick, *Biometric Information – Permanent Personally Identifiable Information Risk*, A.B.A. (Feb. 14, 2019), https://www.americanbar.org/groups/business_law/publications/committee_newsletters/bcl/2019/201902/fa_8/ (explaining how the use of biometric information technology to retrieve a consumer's personal information for company use has grown substantially); *see also* Quinn Emanuel Urquhart & Sullivan, LLP, *June 2019: The Rise of Biometrics Laws and Litigation*, J.D. SUPRA (June 28, 2019), https://www.jdsupra.com/legalnews/june-2019-the-rise-of-biometrics-laws-82168/ (finding that there has been a notable increase in litigation and legislation surrounding the use and collection of biometric data).

[6] Margaret Rouse, *Biometrics,* TECH TARGET (May 2019), https://searchsecurity.techtarget.com/definition/biometrics (defining biometrics as a measure of people's physical and behavioral characteristics which are used for identification of individuals); *see also* Wernick, *supra* note 5 (finding that biometrics analyze an individual's biologically unique physical and behavioral characteristics to access their identification).

[7] *See* Molly K. McGinley, *The Biometric Bandwagon Rolls On: Biometric Legislation Proposed Across the United States,* NAT'L L. REV. (Mar. 25, 2019), https://www.natlawreview.com/article/biometric-bandwagon-rolls-biometric-legislation-proposed-across-united-states (analyzing how the definition of biometric information has been defined both in a broad sense to include "physiological, biological and behavioral characteristics" and in a more narrow sense to include only specific types of information such as "fingerprints" depending on the state); *see also* Rouse, *supra* note 6 (distinguishing between the two types of biometric identifiers and how they depend on either physiological or behavioral characteristics).

and facial recognition software has gained significant traction for identification purposes in several different fields.[8] This type of information is used by government agencies, businesses, hospitals, banks, and even retail services to gain access to a person's identity; in addition, these companies use the identifiers to improve business functionality and efficiency.[9] However, because biometric identifiers are unique to each individual, this means that unlike a username and password combination, if a person's biometric identifiers are compromised, they cannot be changed.[10]

Although biometric information serves as a crucial tool for both businesses and individuals alike, legislation that would protect the consumer from potential abuse by corporations, in the form of a data breach, has yet to be decided on a federal level.[11] There have been a few pieces of state legislature which have been passed in recent years which overwhelmingly seem to provide consumers with the ability to have power over their private data. However, the majority of those laws seem to favor the rights of the business corporation and not of the consumer.[12] But

---

[8] *See* Peter Tsai, *Data Snapshot: Biometrics in the Workplace Commonplace, But Are They Secure?,* SPICEWORKS (Mar. 12, 2018), https://community.spiceworks.com/security/articles/2952-data-snapshot-biometrics-in-the-workplace-commonplace-but-are-they-secure (finding that based off a survey of five-hundred IT companies, biometric authentication technology is used by sixty-two percent of companies with an additional twenty-four percent of whom plan to use the technology within two years); *see also* Meyer, *supra* note 4 (finding that biometric identification, initially used by government agencies to ensure national security has now become part of lucrative consumer brands such as *Apple*, *Dell* and *Lenovo*).

[9] *See* U.S. Dep't of State, *supra* note 1 (explaining the ways in which the use of biometric identifiers has proven to be an important method in protecting the country's national security); *see also* Wernick, *supra* note 5 (detailing how workforce managements, hospitals, banks, and retail stores use biometric measures by having their employees clock into work with their fingerprints, access patient files, and even enter into a business facility without the use of a key).

[10] *See* Quinn, *supra* note 5 (noting how the collection of biometric identifiers specifically raises privacy concerns because of the inability for them to change, unlike identity cards and passwords, should there be a compromise); *see also* Rouse, *supra* note 6 (finding how the physical qualities of some biometric measures are static and cannot be replaced as was noted in the breach that the U.S. Office for Personal Management experienced in 2014 when 20 million individuals fingerprints were compromised).

[11] *See* McGinley, *supra* note 7 (finding that federal legislation to support biometric privacy data on a national level has yet to be established although state legislatures have created their own); *see also* Wernick, *supra* note 5 (finding that Biometric Information Privacy is "under review by state and federal legislators and regulators in the United States and other governments and regulators in the international community").

[12] *See* WASH. REV. CODE § 19.375.030 (2020) (showing Washington State's slight change to the standards set out by Illinois' BIPA by granting no private right of action and only allowing Washington's attorney general the ability to enforce that right); *see also* Kimberly Gold et al., *The Facial Scan that Launched a Thousand Laws: Biometric Privacy Legislation Trend Continues to Grow Nationwide,* TECH. L. DISPATCH, https://www.technologylawdispatch.com/2019/08/privacy-data-protection/the-facial-scan-that-launched-a-thousand-laws-biometric-privacy-legislation-trend-continues-to-grow-nationwide/ (last visited May 27, 2020) (quoting the Washington session laws which state how the use of biometrics without consent is prohibited however there is no direct private right of action established and it would need to ultimately be the decision of the State Attorney to enforce

there should be regulation available to consumers in the United States emulating the European Union's leading law on internet privacy known as the General Data Protection Regulation (the "GDPR"), and more specifically focusing on the "Right to be Forgotten."[13]

This Comment will address the different ways in which biometric data has become an integral part of everyday American life, whether it be through the use of facial recognition for national security or the use of fingerprinting to access an individual's smartphone.[14] Part II will further discuss how biometric data privacy legislation, specifically as set out in the Biometric Illinois Privacy Act ("BIPA"), has become prominent and will analyze its effects on the legal rights of consumers to bring suit against private entities.[15] Part III will discuss the present solutions available to consumers who fall victim to companies who distribute consumer's information.[16] Further, Part IV will compare these solutions to the European Union's regulation known as the "Right to be Forgotten".[17]

---

it).

[13] *See Biometric Data and Data Protection Regulations (GDPR and CCPA),* GEMALTO (Feb. 27, 2020), https://www.gemalto.com/govt/biometrics/biometric-data (explaining the regulation adopted in the European Union which states that "consent must be explicit before the collection of the data" as well as that the person who's data has been collected has a right to "withdraw his or her consent at any time"); *see also* Andrew K. Woods, *Three Things to Remember from Europe's 'Right to Be Forgotten' Decisions*, LAWFARE BLOG (Oct. 1, 2019, 10:11 AM), https://www.lawfareblog.com/three-things-remember-europes-right-be-forgotten-decisions (finding that recent court rulings over the EU's "Right to be Forgotten Regulations," which concluded that Google would agree to remove certain search results at the request of each individual, would only allow this data removal for participants that are located in the European Union).

[14] *See* Porter, *supra* note 1 (discussing how although biometric data creates "convenience to commercial users" it also aids governmental agencies such as the FBI and Homeland Security to gather information for public safety); *see also* Wernick, *supra* note 5 (discussing the role that biometric identifiers play in the landscape between businesses and consumers today).

[15] *See* Quinn, *supra* note 5 (finding that the BIPA creates a private cause of action for anyone who has been deemed an aggrieved party to "seek $1000 for each negligent violation of the act"); *see also* McGinley, *supra* note 7 (stating that the state laws passed in Illinois, Texas, and Washington differ in significant ways as the states attempt to "keep up" with the changes in technology and business policy).

[16] *See* Gold, *supra* note 12 (finding that under BIPA consumers who have been aggrieved by a breach can recover between $1000 to $5000 in damages); *see also* Annemaria Duran, *Learn How Washington's New Biometric Privacy Law Affects Businesses,* SWIPECLOCK (Jan. 3, 2018), https://www3.swipeclock.com/blog/learn-washingtons-new-biometric-privacy-law-affects-businesses/ (stating that the Washington State Biometric Privacy Act does not apply to corporations or employers who "use biometric information in a noncommercial use").

[17] *See* Steven C. Bennett, *The "Right to be Forgotten": Reconciling EU and US Perspectives,* BERKLEY J. INT'L (May 2012), https://pdfs.semanticscholar.org/5e38/d17d678ed5c3dc94cfb8288ed305a3dfe942.pdf (elaborating on how the EU created the right to be forgotten which granted citizens the right to extinguish their data from the internet when it was used for the purposes for which it was collected); *see also* Alessandra Mantelero, *The EU Proposal for a General Data Protection Regulation and the Roots of the 'Right to be Forgotten',* COMPUTER L. & SECURITY REV. (June 2013), https://www.sciencedirect.com/science/article/pii/S0267364913000654 (explaining how the EU's Right to be Forgotten Regulation allows the individual to have autonomy over sensitive information).

Finally, Part V will discuss the solutions to biometric privacy data breaches by proposing federal legislation similar to the already established state law private causes of action for the aggrieved, as well as giving the individual the option to participate in complete data wiping, similar to that which is done in the European Union.[18]

II. BACKGROUND

A. THE BIOMETRIC ILLINOIS PRIVACY DATA ACT

In October 2008, BIPA was passed by the State of Illinois and since then has created a platform for the future of data privacy litigation and legislation.[19] BIPA became the first law in the United States to protect individual privacy data and since its inception, has given rise to hundreds of class action law suits.[20] The Act prohibits any private entity in possession of biometric identifier or biometric information to "sell, lease, trade[,] or otherwise profit from a person's or customer's biometric identifier or biometric information."[21]

It can be argued that the most notable protection BIPA provides is the protection of the individual consumer from corporations who benefit from the collection of their biometric identifiers.[22] Although there are other state laws that have followed in BIPA's footsteps, BIPA is the only act which provides individual consumers with a private right of action by allowing any person who has been aggrieved by either a private entity or

---

[18] *See* Wernick, *supra* note 5 (examining how Federal legislation has not yet been established and how three states: Washington, Texas, and Illinois, have been the only ones to employ action on biometric data privacy); *see also* Woods, *supra* note 13 (finding that the European Union's regulation known as the "Right to be Forgotten" does not allow for a global relinquishment of data, it only has control over the member states of the EU).

[19] *See* 740 ILCS 14/15 (outlining BIPA legislation for biometric privacy data); *see also* Wernick, *supra* note 5 (describing the BIPA regulation and how, since its inception, it has given rise to multiple private and class action lawsuits between individuals and breaching companies).

[20] *See* Timothy J. Pastore, *Legal Brief: Biometrics, the Law, and Your Company,* SECURITY INFO WATCH (Sept. 19, 2019), https://www.securityinfowatch.com/access-identity/biometrics/article/21094070/biometrics-the-law-and-your-company (stating that BIPA became the first law in the United States to protect biometric information and that although other states have enacted similar legislation, "none rise to the level of protections afforded by BIPA"); *see also* Quinn, *supra* note 5 (concluding that BIPA was the first comprehensive biometric privacy law set in place in the United States and since then over two hundred class action suits have been filed under it).

[21] 740 ILCS 14/15 (quoting text from the BIPA legislation); *see also* Nakar, *supra* note 2 (stating that no company or private entity will be allowed to buy, sell, lease, or distribute personal biometric identifiers without consent of the individual whose biometric identifiers were captured in the first place).

[22] *See* Julie Carter, Alexandra Dugan & Erin Illman, *First Federal Legislation Proposed Relating to Protection of Biometrics,* J.D. SUPRA (Apr. 5, 2019), https://www.jdsupra.com/legalnews/first-federal-legislation-proposed-15673/ (noting that BIPA has been considered to be the "gold standard" for Biometric Privacy Data legislation); *see also* McGinley, *supra* note 7 (addressing how BIPA created a new trend known as the "biometric bandwagon" as other states seek to create legislation in order to protect consumers from similar data breaches).

an individual to sue for up to "$1000 for each negligent violation of the act and $5000 for each intentional or reckless violation."[23] In addition, companies or private entities who violate BIPA are liable for attorneys' fees and costs as well as any experts' fees and injunctive relief.[24]

Although BIPA does not define who would be considered an "aggrieved party," in the seminal case of *Rosenbach v. Six Flags Entertainment Corp*., the Supreme Court of Illinois settled this uncertainty by holding that once a company fails to comply with any of the requirements as outlined under the Act, the individual would have standing to sue under a BIPA violation.[25] In that case, Six Flags Theme Park in Illinois used a minor's fingerprint to grant him access to the theme park without providing him with information on how long the biometric information would be retained, nor for what purpose the fingerprint would serve now that it was collected by the park.[26] It was thus established that the plaintiffs could recover damages because they were considered "aggrieved parties" once the theme park did not provide them with information on what they had just consented to when they allowed the park to use their fingerprints.[27] Consequently, it was decided on precedence that a person

---

[23] 740 ILCS 14/20 (quoting BIPA); *see also* Quinn, *supra* note 5 (finding that the Act itself does not define what an "aggrieved" party actually means and therefore leaves it to the courts to determine "what level of harm a plaintiff must experience to have statutory standing"); *see also* Wernick, *supra* note 5 (explaining further that BIPA provides that "a prevailing plaintiff may recover liquidated damages of $1000 or actual damages, whichever is greater, in addition to obtaining other relief such as an injunction" and in addition a plaintiff may also recover reasonable attorney's fees and costs included in their damages).

[24] *See* 740 ILCS 14/20 (quoting Section 20 of BIPA which states that a prevailing party may recover for each violation against another who negligently or recklessly violates a provision of the act, reasonable attorneys' fees and costs, and injunctive relief if the court deems appropriate); *see also* Ryan S. Higgins, Daniel Campbell & Matthew R. Cin, *Biometric Privacy Update- Actual Harm Not Required,* NAT'L L. REV. (Feb. 07, 2019), https://www.natlawreview.com/article/biometric-privacy-update-actual-harm-not-required (finding that the cost of non-compliance of BIPA can have a large impact on private entities who do not conform finding companies liable for $1000 per violation in liquidated damages).

[25] *See* Rosenbach v. Six Flags Entm't Corp., N.E. 3d 1199, 1206 (2019) (holding that a person does not need to "allege some actual injury or adverse effect, beyond violation of his or her rights under the Act" to be considered an "aggrieved" person); *see also* Quinn, *supra* note 5 (discussing how the plaintiff, Rosenbach, was considered aggrieved when the amusement park, Six Flags, collected her fourteen year old son's fingerprints without consent).

[26] *See Rosenbach,* N.E. 3d at 1201 (finding that Stacy Rosenbach and her son provided Six Flags with their fingerprints to gain access to the park and neither was given information in writing about the "specific purpose and length of term for which his fingerprint had been collected"); *see also* Tae Kim, *Rosenbach v. Six Flags: Illinois Supreme Court Interprets Illinois Biometric Privacy Law*, JOLT DIG. (Feb. 18, 2019), http://jolt.law.harvard.edu/digest/rosenbach-v-six-flags-illinois-supreme-court-interprets-illinois-biometric-privacy-law (finding that the *Rosenbach* case established that a plaintiff who sues under BIPA does not need to show they suffered injury to be awarded monetary damages).

[27] *See* Wernick, *supra* note 5 (finding that the Rosenbach plaintiffs did not need to allege that they had an actual injury beyond their rights being violated under the Act to qualify as aggrieved parties); *see also* Gold*, supra* note 12 (finding that the Illinois Supreme Court established that a plaintiff "need only plead a violation of BIPA" to be considered an aggrieved party as expressed in the

who is "aggrieved" need not suffer actual harm but just needs to find that the company violated the requirements of the Act to be able to recover damages under BIPA.[28]

BIPA establishes that if private entities or individuals collect biometric identifiers or similar types of information through the use of fingerprints, facial recognition technology, or iris scans, the entities are to provide notice to the individual consumers whose information has been or is about to be used, distributed, or sold.[29] It also requires for the company or private entity that has collected the information to inform the consumer in writing about what they will do with the information that has been collected and for what length of time the information will remain collected before they destroy it, sell it, or otherwise handle the biometrics.[30] Employers who have retained information from their employees using biometric identifiers must provide them with a written policy outlining the ways in which they will dispose of the identifiers no later than three years after the purpose of their collection was met or the person's last interaction with the employer.[31]

---

statute).

[28] *See* Higgins, *supra* note 24 (elaborating on how the court has reached the conclusion that one need not be actually injured to recover because when someone's biometric information is risked it is an actual breach); *see also Patel v. Facebook Inc.,* 290 F. Supp. 3d 948, 954 (N.D. Cal. 2018) (finding that because biometric identifiers are unique to each person and cannot be changed, "procedural protections" are especially pertinent).

[29] *See* Quinn, *supra* note 5 (finding that before a corporation collects or stores biometric information, they must "provide written notice to individuals that the collection will occur as well as the purpose and length of the collection"); *see also* Thomas F. Zych, Steven G. Stransky & Brian Doyle-Wenger, *State Biometric Privacy Legislation: What You Need to Know*, LEXOLOGY.COM (Sept. 5, 2019), https://www.lexology.com/library/detail.aspx?g=ebc0e01c-45cc-4d50-959e-75434b93b250 (finding that the private entities that possess biometric information need to "make available a written policy that includes a retention schedule and guidelines for permanently destroying the information").

[30] *See Landmark Ruling on the Illinois Biometric Information Privacy Act*, WINSTON & STRAWN, LLP (Jan. 30, 2019), https://www.winston.com/en/thought-leadership/landmark-ruling-on-the-illinois-biometric-information-privacy-act.html (explaining how the Biometric Privacy Act requires that any company that collects this information must indicate to the consumer what they will be doing with the information); *see also* Stuart D. Levi, et al., *Illinois Supreme Court Holds that Biometric Privacy Law Does Not Require Actual Harm for Private Suits,* SKADDEN (Jan. 29, 2019), https://www.skadden.com/insights/publications/2019/01/illinois-supreme-court (establishing that companies who collect biometric information must disclose their "policies for usage and retention").

[31] *See* Phillip M. Schreiber & Andrew N. Fiske, *Illinois Supreme Court Expands Potential Liability Under Biometric Information Privacy Act,* HOLLAND & KNIGHT (Jan. 25, 2019), https://www.hklaw.com/en/insights/publications/2019/01/illinois-supreme-court-expands-potential-liability (explaining how BIPA law requires companies to destroy the biometric identifiers after three years of storage); *see also* Niya T. McCray, *Sensitive to the Touch: The Evolution of U.S. Biometric Privacy Law,* BRADLEY (May 2018), https://www.bradley.com/insights/publications/2018/05/the-evolution-of-us-biometric-privacy-law (claiming that BIPA requires companies to adhere to "strict guidelines" when it comes to written policies on how they will destroy the biometric identifier information).

III. BIPA'S EFFECT ON INDIVIDUAL STATE LEGISLATURE

A. BIPA LEADS BIOMETRIC PRIVACY INFORMATION LEGISLATION

The effect of the BIPA legislation was not seen until a few years after its enactment when several class action lawsuits were filed, namely from employees against employers for using their fingerprints for timekeeping purposes.[32] This legislation has not only put businesses in Illinois who use biometric identifiers to collect information from their employers or other consumers on notice, but has also done the same for private corporations not localized in the state in preparation of the legislation that is being considered across the United States.[33]

Although Illinois has set the stage for other state legislatures to restrict the use and dissemination of biometric data collected by private corporations, several of the other state's approach to the drafting of their own privacy data acts have lacked the sole component which would provide the ultimate layer of protection for the individual consumer which is creating a private cause of action to sue the companies who tamper with the biometric identifiers.[34]

B. TEXAS STATUTE ON THE CAPTURE OR USE OF BIOMETRIC IDENTIFIERS

Texas was the second state to develop its own biometric identifier data privacy act after Illinois and Washington set the stage for consumer protection.[35] The Texas Act, Capture or Use of Biometric Identifiers

---

[32] *See* Higgins, *supra* note 24 (explaining how BIPA has opened the door to hundreds of lawsuits in Illinois for companies who have been non-compliant with the Act, namely suits between employees and employers for use of biometrics for timekeeping purposes); *see also* Robert Fallah, *Illinois Supreme Court Ruling: Biometric Privacy Law Only Requires Violation, Not Actual Harm,* EMP. PRIVACY BLOG (Feb. 6, 2019), https://www.fisherphillips.com/Employment-Privacy-Blog/illinois-supreme-court-ruling-biometric-privacy-law (finding how different companies, such as retail stores and fast food chains, have former employees who are filing lawsuits under BIPA for violations when using the biometric fingerprints to "punch clock" at their workplaces).

[33] *See* Quinn, *supra* note 5 (finding that businesses that collect this type of information should "closely examine how information is collected, used, shared, and evaluate compliance with BIPA"); *see also* Wernick, *supra* note 5 (explaining several points which businesses should employ in order to be compliant with BIPA's regulation and avoid potential breach such as developing policies which would outline how the business would use the information, and inform consumers and employees of the ways in which their information will be used).

[34] *See* Fallah, *supra* note 32 (finding how Illinois is the only state to allow for consumers or those who are aggrieved to have a private cause of action and recovery of damages); *see also* Wernick, *supra* note 5 (elaborating on how although other states have begun to adopt similar legislation, Illinois has been the only state to allow for a private cause of action).

[35] *See* Jerri Lynn Ward, *Texas Biometric Privacy Law Restricts Certain "Biometric Identifiers." Only Three States Have Laws Regulating the Collection and Storage of Biometric Data,* GARLOWARD (Mar. 26, 2018), https://www.garloward.com/2018/03/26/texas-biometric-privacy-law-restricts-certain-biometric-identifiers-three-states-laws-regulating-collection-storage-biometric-data/ (explaining that Texas passed its own law on the capture of biometric information due

("CUBI"), differs from that of Washington and Illinois as it only covers personal information categorized as "biometric identifier."[36] The definition of what would be considered a biometric identifier under CUBI is more specifically targeted to include: "specific types of information including fingerprints, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics used to identify a specific individual."[37]

The Texas statute, similarly to BIPA, prohibits companies from capturing information for "commercial purposes" without notice and consent having been sent to the aggrieved party before the capture.[38] CUBI fails to define what would be considered a "commercial purpose," but an example of one would be collecting fingerprints in order to pay employer salaries.[39] Also, unlike BIPA, Texas does not require that there be a written release.[40] The guidelines that would direct employers who retain this information, for timekeeping purposes, for example, are not as defined

to the rising concern of individual's information having been compromised); *see also* Alfonso Kennard, *How Texas Employers Can (and can't) Use Your Biometric Data,* KENNARD L. (Feb. 21, 2018), https://www.kennardlaw.com/blog/2018/02/how-texas-employers-can-and-cant-use-your-biometric-data.shtml (explaining how the Texas law was passed in 2009 and is similar to that of what was passed in Illinois).

[36] *See* Ward, *supra* note 35 (finding that the Texas statute only provides consumers protection for their biometric identifiers and not a broader category of information); *see also* Zych, *supra* note 29 (finding that the Texas law "prohibits the capture of an individual's biometric identifiers for a commercial purpose").

[37] *See Tex. Bus. & Com. Code § 503.001. Capture or Use of Biometric Identifier*, FINDLAW, https://codes.findlaw.com/tx/business-and-commerce-code/bus-com-sect-503-001.html (last visited May 27, 2020) (quoting the language from the Texas statute outlining the guidelines for capture and use of biometric identifiers); *see also* John G. Browning, *The Battle Over Biometrics: A Look at the Law in Texas and Two Other States.,* 81 TEX. B.J., 674, 676 (Oct. 2018) , https://www.texasbar.com/AM/Template.cfm?ection=Content_Folders&ContentID=42128&Template=/CM/ContentDisplay.cfm (stating how the Texas statute does not include protection over data that is "converted into a code or template" and does not have a broad category for biometric information).

[38] *See* Browning, *supra* note 37, at 676 (finding that the Texas statute, similarly to Illinois' BIPA regulation, requires that employers receive notice and consent); *see also* Nicole O., *Biometrics Laws and Privacy Policies,* PRIVACY POLICIES, https://www.privacypolicies.com/blog/privacy-policy-biometrics-laws/ (last visited May 27, 2020) (stating that the law requires that consent be given prior to the collection of the personal biometric information).

[39] *See* Karun Ahuja, *No Harm, No Foul? Not So, Under Illinois Biometric Privacy Law,* THE LABOR DISH (June 24, 2019), https://www.labordish.com/2019/06/no-harm-no-foul-not-so-under-illinois-biometric-privacy-law/#page=1 (finding that CUBI does not define what would be considered "commercial purposes," but an example of one would be the employer using biometric identifiers to pay their employees); *see also* Duran, *supra* note 16 (finding that the Washington law is broader than Texas law and only applies to biometric indicator commercial use).

[40] *See* Jacob M. Monty, *Employers, Get Ready for Spike in Biometric Privacy Lawsuits,* HR DAILY ADVISOR (June 27, 2019) https://hrdailyadvisor.blr.com/2019/06/27/employers-get-ready-for-spike-in-biometric-privacy-lawsuits/ (explaining how the Texas law, Capture or Use of Biometric Information Act, does not "require an employee's consent to be in writing"); *see also* Browning, *supra* note 37, at 676 (finding that the Texas state law does not require a "written release" of consent unlike that which BIPA requires).

as those in BIPA because the statute allows for the entities to have a "reasonable time" to delete the information.[41]

Most notably, the Texas statute, unlike that of BIPA or any other state legislation that has been in effect, does not provide individuals with a private right of action to sue.[42] This means that the suits will be heard at the discretion of the Texas State Attorney General and disallow for an increase in class action suits.[43] However, those companies that are not in compliance with the Texas State statute may face large sums of penalties in damages to the aggrieved parties.[44] The statute states that a violation of its regulations could cost up to $25,000 in civil penalties, which is a much larger penalty than that originally outlined in BIPA.[45] This provides large incentives for the businesses who collect biometric identifiers from their employers to update their policies and stay in compliance with the consumer-focused law.[46]

---

[41] *See Tex. Bus. & Com. Code §503.001. Capture or Use of Biometric Identifier*, *supra* 37 (quoting the language from the Texas statue defining the "reasonable time" standard for disparaging of biometric identifier information); *see also* McCray, *supra* note 31 (finding that the Illinois law vaguely states that the employer has a "reasonable amount of time" to destroy the sensitive information before being held accountable for a breach).

[42] *See* Quinn Emanuel Urquhart & Sullivan, LLP, *supra* note 5 (stating how Texas' Biometric Privacy Data Act does not provide individuals with a private right of action to sue companies who have breached); *see also* McGinley, *supra* note 7 (finding that the Texas statute is similar to that of Washington's state law because there is no private cause of action to sue).

[43] *See* McCray*, supra* note 31 (stating that the Texas law only allows for the Attorney General to bring an action to recover for violations of the act)*; see also* Ward, *supra* note 35 (explaining how the Texas State Attorney General can bring suit against companies for biometric privacy violations).

[44] *See* McCray, *supra* note 31 (finding that the amount in civil penalties that a company could face if they were to breach the Texas regulation could be up to $25,000 for each violation of the statute for the company to provide the aggrieved); *see also* Lara Tumeh, *Washington's New Biometric Privacy Statute and How It Compares to Illinois and Texas Law,* BLOOMBERG L. (Oct. 17, 2017), https://www.jdsupra.com/legalnews/washington-s-new-biometric-privacy-70894/ (finding that Texas authorizes up to $25,000 in damages for breach of the biometric privacy data act).

[45] *See* McCray, *supra* note 31 (finding that the Texas law allows for aggrieved consumers to collect up to $25,000 worth of damages); *see also* Molly McGinley et.al, *Litigation Under Illinois Biometric Information Privacy Act Highlights Biometric Data Risks,* CASETEXT (Nov. 10, 2017), https://casetext.com/analysis/litigation-under-illinois-biometric-information-privacy-act-highlights-biometric-data-risks?pricing_page_group=c&ct_spg=c&pdf_download_group=p&pdf_download_landing_page_group=p&new_learn_more=c&phone_number_group=c&sort=relevance&resultsNav=false&q= (noting how BIPA allows for "statutory damages of $1000 for each negligent violation or actual damages (whichever is greater) for each violation of the act, and $5000 or actual damages (whichever is greater) for each intentional or reckless violation of the act," while the Texas BIS act allows for remedies of up to $25,000 per violation).

[46] *See* Ahuja, *supra* note 39 (stating that Washington specifically defined "commercial purpose"); *see also* Nicole O., *supra* note 38 (explaining how the Washington law is similar to the law in Illinois in the way that it "regulates collecting, using, and retaining data").

C. WASHINGTON STATE BIOMETRIC PRIVACY DATA ACT

The biometric privacy data legislation passed in the State of Washington is commendable as it sets out much of the same language from the legislation as laid out in BIPA by setting forth requirements for businesses who decide to use biometric identifiers to collect employer's information.[47] However, the Washington State legislation removes the vital language from BIPA which grants the individual consumer a private right of action to sue companies who fail to comply with the legislation's requirements, weakening its effect on an individual's rights over their private data.[48] The Washington Privacy Data Act notably also removed facial recognition technology ("FRT"), voice and audio recordings, and physical or digital photographs from the definition of what is considered a biometric identifier.[49] However, the most significant change from that of BIPA is the type of notice and the ways that consent from an individual is obtained is "context-dependent" and is not as restrictive to a writing as that required in BIPA.[50] In order for the type of notice to be within compliance of the Act, the notice just needs to be delivered in a way that it is made readily available to any affected individual.[51]

---

[47] *See* WASH. REV. CODE § 19.375 (2017) (quoting from the Washington Biometric Privacy Data Act which sets requirements for private entities who collect information through biometric identifiers to follow); *see also Washington Becomes Third State to Enact Biometric Privacy Law*, HUNTON PRIVACY BLOG (June 1, 2017), https://www.huntonprivacyblog.com/2017/06/01/washington-becomes-third-state-enact-biometric-privacy-law/ (finding that the Washington House Bill 1493, now signed into law, establishes requirements for businesses who collect biometric identifiers such as "fingerprints, eye retinas, irises, and other unique biological patterns or characteristics used to identify a specific individual").

[48] *See* WASH. REV. CODE § 19.375.010(1) (2017) ("'Biometric identifier' does not include a physical or digital photograph, video or audio recording or data generated therefrom . . . ."); *see also* Quinn Emanuel Urquhart & Sullivan, LLP, *supra* note 5 (finding that the Washington State law as well as the Texas law, although based in BIPA legislation, removes the private right of action for individuals to sue).

[49] *See* WASH. REV. CODE § 19.375.010(1) (2017) ("'Biometric identifier' does not include a physical or digital photograph, video or audio recording or data generated therefrom . . . ."); *see also* Benjamin J. Byer, *Washington's New Biometric Privacy Law: What Businesses Need to Know,* DAVIS WRIGHT TREMAINE (July 24, 2017), https://www.dwt.com/insights/2017/07/washingtons-new-biometric-privacy-law-what-busines (concluding that the Washington State Law purposefully excludes the definition of facial recognition technology under biometric identifier, which would be used in social networks and other photo storage websites).

[50] *See* WASH. REV. CODE § 19.375.020 (2017) (setting forth consent requirements without expressing that such consent must be in writing); *see also* Jim Halpert, *Washington Becomes the Third State With a Biometric Privacy Law: Five Key Differences*, DLA PIPER (June 21, 2017), https://www.dlapiper.com/en/us/insights/publications/2017/06/washington-third-state-with-biometric-privacy-law/ (concluding that the Washington law does not distinctly outline the type of notice that needs to be given to consumers unlike that of BIPA).

[51] *See* WASH. REV. CODE § 19.375.020(2) (2017) ("Notice is a disclosure, that is not considered affirmative consent, that is given through a procedure reasonably designed to be readily available to affected individuals . . . ."); *see also* Byer, *supra* note 49 (finding that the Washington State law which does not require consent of biometric information to be given in writing allows for the potential of some retail stores to gain consent to biometric information use given orally over the

The Washington State Biometric Privacy Law also differentiates itself from that of BIPA because, similarly to CUBI, it is enforceable at the discretion of the State Attorney which could allow for the potential of consumers who have been affected by data breaches to not receive compensation or seek other types of court ordered remedies.[52] Therefore, individuals who seek a remedy for breach in Washington State do not have the private right of action that the Illinois residents who are protected under BIPA as aggrieved parties receive; it is up to the discretion of the Attorney General instead.[53] As multiple states join in on the adoption of stronger Biometric Privacy Data protection, the important clauses which protect the individual consumer from the exploitation of the larger private corporations should be preserved.[54]

D. THE CALIFORNIA CONSUMER PRIVACY ACT

Perhaps BIPA's greatest influence of all state legislation is the new data privacy law that will become effective on January 1, 2020, in the State of California known as The California Consumer Privacy Act ("CCPA").[55] CCPA took note of the protection that BIPA provides for an individual's biometric identifiers and included similar language under

---

phone).

[52] *See* S. Gregory Boyd, *Third State Adopts Biometric Privacy Laws,* FOCUS ON THE DATA (July 10, 2017), https://www.focusonthedata.com/2017/07/third-state-adopts-biometric-privacy-law/ (elaborating on how the individual in Washington State does not have a private right of action for claims against companies who compromised their biometric identifiers but instead the Attorney General may enforce the regulation at their discretion); *see also* Zych, *supra* note 29 (finding that Washington's law will clarify how a breach in data privacy would impact the individuals and requires that individuals and others be notified if an entity that stores biometric data is breached).

[53] *See* Halpert, *supra* note 50 (expanding on how the Washington State Biometric Privacy Act does not provide a private right of action and the enforcement could only be done by the Washington State Attorney General at his or her discretion); *see also* Tumeh, *supra* note 44 (showing how Illinois is the only state out of the three states: Illinois, Texas, and Washington, that has created the private right of action and as a result will most likely be the main leader of biometric privacy litigation in the United States).

[54] *See* Byer, *supra* note 49 (finding that the "protections and restrictions" of Washington's law reflects a balance of consumer protection while giving companies more freedom in using consumer's biometrics); *see also Washington Becomes the Third State with a Biometric Law*, COVINGTON (May 31, 2017), https://www.insideprivacy.com/united-states/state-legislatures/washington-becomes-the-third-state-with-a-biometric-law/ (finding that the Washington State Law has a more defined standard regarding the requirements for entities that collect, use, or retain biometric identifiers, but that there is no private right of action and suit is at the discretion of the Attorney General).

[55] *See* Maria Korolov, *California Consumer Privacy Act (CCPA): What You Need To Know To Be Compliant*, CSO ONLINE (Oct. 4, 2019, 3:00 AM), https://www.csoonline.com/article/3292578/california-consumer-privacy-act-what-you-need-to-know-to-be-compliant.html (finding that the California Consumer Privacy Act will go into effect on January 1, 2020); *see also Top 5 CCPA Questions to Ask Right Now*, DAVIS WRIGHT TREMAINE (Jan. 28, 2019), https://www.dwt.com/blogs/privacy--security-law-blog/2019/01/top-5-ccpa-questions-to-ask-right-now (finding that the CCPA will cause a "dramatic shift" in the ways in which companies will have to assess consumers' privacy rights).

its newest legislation.[56] However, CCPA took the framework set out in BIPA, which was originated to protect biometric identifiers from being compromised, a step further by broadening the category of protections that individual consumers will receive under its application.[57] CCPA applies to any business corporation that garners over "$25 million in revenue, or buys or sells the personal information of 50,000 or more consumers, or derives [fifty] percent or more of its annual revenue from selling consumers' personal information . . . ."[58] CCPA is a California state law that will allow the individual consumer to be made aware of the information that large business corporations are collecting from them.[59] This new legislation will only continue the trend that BIPA began back in 2008 for several large companies across the nation who capture consumers' information, including those who gather the information using biometric identifiers.[60]

Large corporations who use biometric identifiers to gather information from consumers, or who do business in California, will need to

---

[56] *See* Zych, *supra* note 29 (finding that California expanded its framework to include language which protects consumer's biometric identifiers); *see also* Quinn Emanuel Urquhart & Sullivan, LLP, *supra* note 5 (explaining how the CCPA will include protection for "personal information" which will include biometric information).

[57] *See* Gold, *supra* note 12 (expanding on how the CCPA is one of two "high profile examples" of privacy legislation efforts that attempt to include biometric identifiers in their language); *see also* Danielle Ochs, *The Latest on California's Approach to Biometrics in the Workplace*, NAT'L L. REV. (Oct. 19, 2019), https://www.natlawreview.com/article/latest-california-s-approach-to-biometrics-workplace (finding that employers in California who use biometrics in the workplace will have to inform employees of their use and ask for consent before using them).

[58] *See* John Stephens, *California Consumer Privacy Act*, A.B.A. (Feb. 14, 2019), https://www.americanbar.org/groups/business_law/publications/committee_newsletters/bcl/2019/201902/fa_9/ (quoting language from the CCPA which distinguishes which types of corporations the Act would ultimately provide protection for); *see also* Anna Attkisson, *How California's Consumer Privacy Act Will Affect Your Business*, BUS. NEWS DAILY (Dec. 31, 2019), https://www.businessnewsdaily.com/10960-ccpa-small-business-impact.html (finding that the law will be aimed towards businesses that earn "$25 million in revenue a year, sell 50,000 consumer records per year, or derives 50% of its annual revenue from selling personal information").

[59] *See* Jeff John Roberts, *Here Comes America's First Privacy Law: What the CCPA Means for Business and Consumers*, FORTUNE (Sept. 13, 2019, 6:30 AM), https://fortune.com/2019/09/13/what-is-ccpa-compliance-california-data-privacy-law/ (finding that the CCPA will grant consumers more access to control over their personal information); *see also* Catherine D. Meyer, Fusae Nara & James R. Franco & Fusae Nara, *Countdown to CCPA #3: Updating Your Privacy Policy*, PILLSBURY L. (July 8, 2019), https://www.pillsburylaw.com/en/news-and-insights/ccpa-privacy-policy.html (explaining that the CCPA will affect all businesses with privacy policies which interact California consumers on an online platform).

[60] *See* Erin Jane Illman, *Data Privacy Laws Targeting Biometric and Geolocation Technologies*, 73 THE BUS. LAW. 191, 196–197 (2017–18) https://heinonline.org/HOL/Page?handle=hein.journals/busl73&div=13&g_sent=1&casa_token=&collection=journals (concluding that the trend towards protection of consumer rights in technology will only continue on as more state legislatures are created); *see also* Ochs, *supra* note 57 (stating that although California's law is not directly exclusive to biometric identifiers, the CCPA will have a large effect on the ways in which employers use biometrics in the workplace).

abide by the regulations as set out by CCPA.[61] Similarly to BIPA, CCPA will create a private right of action for aggrieved California residents to sue if their personal information was subject to "unauthorized access and exfiltration, theft, or disclosure as a result of a business's failure to implement and maintain reasonable security procedures and practices appropriate to the nature of the information."[62] Although the legislation is designed to protect only California residents, the law's effects will be felt in other states across the nation.[63] The language of the Act is similar to that of BIPA in that it requires businesses to disclose to participants for whom they collect data about the information they will be collecting, the purpose of collection, and if they plan to sell or distribute the information to other companies.[64] CCPA seems as though it will serve as landmark law as it continues to put pressure on Congress and lead the way for potential federal legislation to protect all Americans from data privacy breaches.[65]

---

[61] *See* Alan L. Friel, *U.S. Consumer Privacy and the CCPA,* BAKERHOSTLETLER https://www.bakerlaw.com/USConsumerPrivacyandtheCCPA, (last visited May 27, 2020) (discovering the ways in which companies who collect personal information from consumers will have to abide by new regulations as set out by the CCPA); *see also* Maya Atrakchi, Mary Costigan, Jason Gavejian & Joseph Lazzarotti, *Does The CCPA Apply to Your Business?,* JDSUPRA (Aug. 14, 2019), https://www.jdsupra.com/legalnews/does-the-ccpa-apply-to-your-business-91898/ (establishing that for this law to apply to a business it would be collecting personal information from their consumers and this could mean "on behalf of the business" such as through a third party).

[62] *See* Al Saikali, *The Coming Litigation Tsunami?: Why Private- Right- of- Action Enforcement Undermines Privacy and Data Security,* WASH. LEGAL FOUND. (Apr. 5, 2019), https://www.wlf.org/2019/04/05/publishing/the-coming-litigation-tsunami-why-private-right-of-action-enforcement-undermines-privacy-and-data-security/ (quoting the language that is written in the CCPA statute which explains the ways the aggrieved individual would have a private right of action against any unauthorized employers); *see also* Jonathan (Yoni) Schenker, Michael F. Buchanan, & Alejandro H. Cruz, *A Closer Look at the CCPA's Private Right of Action and Statutory Damages,* PATTERSON BELKNAP (Aug. 22, 2019), https://www.pbwt.com/data-security-law-blog/a-closer-look-at-the-ccpas-private-right-of-action-and-statutory-damages (explaining how the California consumer whose information is used in violation of the CCPA regulations may bring a private right of action for damages under the data breach law).

[63] *See* Atrakchi*, supra* note 61 (finding that although it is a California state legislation, the law will affect those not present in the state because a business can be located outside of California and have an online component that could be considered doing "business" in California); *see also* Spencer Persson et. al, *California Passes Major Legislation, Expanding Consumer Privacy Rights and Legal Exposure for US and Global Companies,* DATA PROTECTION REP., https://www.dataprotectionreport.com/2018/06/california-passes-major-privacy-legislation-expanding-consumer-privacy-rights/ (last visited on May 27, 2020) (explaining how the CCPA will open the door to policy conversation across the United States as it goes into effect in January of 2020).

[64] *See* Persson, *supra* note 63 (explaining how the CCPA requires businesses to disclose that they will collect information from consumers, the purpose of the collection, and whether it is to sell or distribute); *see also* Friel, *supra* note 61(finding that the CCPA requires that the consumers be informed of the categories of personal information which are being collected).

[65] *See* Chris Burt, *Biometrics to Step in When CCPA Kills the Password, ImageWare Exec Says,* BIOMETRIC UPDATE (Oct. 15, 2019), https://www.biometricupdate.com/201910/biometrics-to-step-in-when-ccpa-kills-the-password-imageware-exec-says (finding that the CCPA is sure to begin a revolution because eventually other states will follow suit and the Federal government has failed to put legislation around); *see also* Roberts, *supra* note 59 (finding that the CCPA is similar to the

IV. AMERICAN BIOMETRICS LEGISLATION IN COMPARISON TO THE EUROPEAN UNION'S PRIVACY EFFORTS

A. THE EUROPEAN UNION'S GENERAL DATA PROTECTION REGULATION

CCPA is similarly modeled after the laws established by the GDPR.[66] The GDPR was established in Europe in the Spring of 2018, and it has become the "uniform law" across the Union regarding protection of consumer and personal data from any corporation who engages its European citizens.[67] The GDPR's goal was to ensure that any company that does business, either by selling goods or services, within the European Union abides by the established law, regardless of the company's location.[68] The legislation is broken into several chapters which provide a broad range of regulations to ensure protection over individual's right to privacy that was established at the 1950 European Convention on Human Rights.[69] A few of the topics covered under the GDPR include the data subject's right of access to data, the right to be rectified, the right to restrict processing, the right to be informed, and the right to erasure, to name a few.[70]

GDPR laws set out in Europe because consumers will have a lot more protection over their information than they were given before these laws).

[66] *See* Friel, *supra* note 61 (explaining how the CCPA will make an impact on a wave of consumer data privacy acts similarly as to how the GDPR has done for the European Union); *see also* Stephens, *supra* note 58 (explaining how the CCPA is designed similarly to the European GDPR legislation which allows consumers to have more protection over the data that is shared to corporations).

[67] *See* Juliana de Groot, *What is the General Data Protection Regulation? Understanding & Complying with GDPR Requirements in 2019*, DATA INSIDER (Dec. 2, 2019), https://digitalguardian.com/blog/what-gdpr-general-data-protection-regulation-understanding-and-complying-gdpr-data-protection (finding that the GDPR is the primary law in the EU which governs the ways in which companies use the EU citizens' personal data); *see also EU data protection rules*, EUR. COMMISSION, https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules/eu-data-protection-rules_en (last visited May 27, 2020) (outlining the regulations included in the GDPR).

[68] *See* de Groot, *supra* note 67 (finding that the GDPR ensures that companies who do business within the EU are subject to the regulation); *see also Whats the Real Purpose of the GDPR?*, PRIVACY TR., https://www.privacytrust.com/gdpr/whats-the-real-purpose-of-the-gdpr.html (last visited May 27, 2020) (explaining that the GDPR's purpose was to make a standardized set of laws for all member countries which would make it easier on EU citizens to understand how their data is being used).

[69] *See* de Groot, *supra* note 67 (explaining that the GDPR has eleven chapters and ninety-one articles which have a large impact on the way that security operations are to be handled in the EU); *see also* Ben Wolford, *What is GDPR, the EU's new data protection law?*, GDPR.EU, https://gdpr.eu/what-is-gdpr/ (last visited May 27, 2020) (noting that the GDPR stems from the right to privacy which was explained at the 1950 European Convention on Human Rights and states, "[e]veryone has the right to respect for his private and family life, his home and his correspondence.").

[70] *See Data Subject Rights and Personal Information: Data Subject Rights Under the GDPR*, I-SCOOP, https://www.i-scoop.eu/gdpr/data-subject-rights-gdpr/ (last visited May 27, 2020) (listing

Several of the articles within the GDPR give the private consumer the ability to have more control over their personal data which is being transferred, processed, and sold to companies.[71] The purpose of the regulation is to relieve the public's concern over the way their private information is being handled by corporations and, in that sense, mirrors the concerns of United States consumers.[72] For example, in the GDPR, biometric data is categorized as a special category under personal data and defined as "personal data resulting from specific technical processing relating to the physical, physiological," genetic, mental, economic, cultural, or social identity of that person.[73] In regards to biometric information, the European Union's regulation has set out strict guidelines that only permits companies who wish to process an individual's biometric data to do so by meeting certain conditions which include, "explicit consent of the data subject, the performance of specific contracts, or processing for certain purposes."[74]

---

the different data subject rights that consumers receive under the GDPR); *see also Articles of the GDPR*, IT GOVERNANCE, https://www.itgovernance.co.uk/articles-of-the-gdpr (last visited May 27, 2020) (outlining the eleven chapters and articles that the GDPR includes ranging from the general provisions to the potential remedies and penalties that companies may be faced with if non-compliant).

[71] *See* Noah Ramirez, *6 Facts about GDPR Compliance Regulations You Need to Know*, OSANO (Oct. 3, 2019), https://www.osano.com/articles/gdpr-compliance-regulations (stating that the GDPR is one of the most significant data privacy regulations which will change the way organizations handle consumer data and will allow consumers to have control over how their data is collected and used); *see also* Michael Nadeau, *General Data Protection Regulation (GDPR): What You Need to Know to Stay Compliant*, CSO (May 29, 2019, 10:28 AM), https://www.csoonline.com/article/3202771/general-data-protection-regulation-gdpr-requirements-deadlines-and-facts.html (finding that the GDPR gives consumers the right to request that personal data be erased and will only allow companies to store and process personal data with individual consent).

[72] *See* Nadeau, *supra* note 71 (explaining how the RSA Data Privacy and Security Report surveyed 7,500 consumers in the U.S. and the EU and found that "80 percent of consumers said lost banking and financial data is a top concern" while lost security information and identity information was seventy-six percent of people's concern); *see also* Todd Ehret, *Data Privacy and GDPR at One Year, A U.S. Perspective. Part One - Report Card*, REUTERS (May 22, 2019, 3:08 PM), https://www.reuters.com/article/bc-finreg-gdpr-one-year-report-card-part/data-privacy-and-gdpr-at-one-year-a-u-s-perspective-part-one-report-card-idUSKCN1SS2K5 (analyzing how the GDPR was designed to address "the privacy rights of EU individuals but applies to all companies processing or controlling the personal information of EU residents").

[73] *See* Jeremy Dunn, *Managing Biometric Data: The GDPR's Requirements*, INFOGOTO (Oct. 16, 2018), https://www.infogoto.com/managing-biometric-data-the-gdprs-requirements/ (finding that the GDPR defines biometric identifiers as "one of the special categories of personal data" and that can only be used by companies upon consent of the individual); *see also* Luke Irwin, *GDPR: Things to Consider When Processing Biometric Data*, IT GOVERNANCE (Sept. 15, 2017), https://www.itgovernance.eu/blog/en/gdpr-things-to-consider-when-processing-biometric-data (explaining that the GDPR attempts to provide organizations who collect biometric information guidelines to "collect that data responsibly and keep it secure").

[74] *See* Billee Elliott McAuliffe et al., *Privacy Regimes for Protecting Biometric Information,* LEWIS RICE (Sept. 2019), https://www.lewisrice.com/publications/privacy-regimes-for-protecting-biometric-information/ (explaining that the GDPR allows companies to collect information so long as they follow the conditions as stated in the regulation); *see also* Mohammed Murad, *How Biometrics Complement GDPR Regulations,* IRIS ID (June 3, 2019), https://www.irisid.com/home-biometrics-

B. BREACH OF THE GENERAL DATA PROTECTION REGULATION

The GDPR handles a breach of compliance differently from that of the U.S. because the fiscal penalties which the companies must pay if they fail to abide by the regulations in the European Union are significant.[75] If a company has breached the terms of one of the articles under the GDPR, they have seventy-two hours from the moment the breach is detected to alert authorities and individuals who may be affected by it.[76] The fiscal penalty has proven lucrative for the European Union as a whole seeing that in 2018 alone there were a reported 60,000 breaches.[77] In the first nine months of the GDPR being effective in the European Union, the European Data Protection Board reported that violation penalties amounted to approximately 56 million Euros.[78] These significantly large figures seem as though they would enable companies that do business with the member states to ensure they are compliant with the regulations, however, the fining method has proven less significant than the implications that the breach notification policy has been in practice.[79] The regulation requires that the data controller and processor, usually a

complement-gdpr-regulations/ (emphasizing that under the GDPR, biometric information requires "active consent and represents a choice made by the consumer").

[75] *See GDPR Fines,* IT GOVERNANCE, https://www.itgovernance.co.uk/dpa-and-gdpr-penalties (last visited on May 27, 2020) (finding that the maximum administrative fine under the GDPR is split into two tiers, the first fine being up to ten million euros and the second being up to twenty million euros); *see also* Neil Hodge, *What We Can Learn From the Biggest GDPR Fines So Far,* GDPR ASSOCIATES (July 19, 2019, 9:11 PM), https://www.gdpr.associates/what-we-can-learn-from-the-biggest-gdpr-fines-so-far/print/ (expanding on how the U.K. fined British Airways $230 million and Marriott a total of $124 million for data breach violations in July of 2019).

[76] *See* Nadeau, *supra* note 71 (explaining that alongside the seventy-two hour alert the company must give supervisory authority and individuals, the use of impact assessments are in place to prevent the risk of breaches); *see also* Ramirez, *supra* note 71 (comparing the EU's GDPR requirement of giving the individuals a notice of the breach after seventy-two hours of its detection to the U.S., where more than half of American companies lack incident response procedures and around sixty-two percent fail to share their data on breaches).

[77] *See* Josephine Wolff, *How Is the GDPR Doing?*, SLATE (Mar. 20, 2019, 5:42 PM), https://slate.com/technology/2019/03/gdpr-one-year-anniversary-breach-notification-fines.html (elaborating on how in June 2018 companies reported 1700 data breaches and that the estimate total by 2019 would be at 36,000 breaches and estimating that 60,000 breaches were reported in the EU between May 25, 2018, and January 28, 2019).

[78] *See* Ehret, *supra* note 72 (stating that the EU will expect to see several more fines in 2019 ranging in the several millions of Euros); *see also* Ramirez, *supra* note 71 (explaining that penalties are tiered in two categories depending on violation and could be "as high as four percent of global turnover, or $24.4 million, whichever is greater").

[79] *See* Wolff, *supra* note 77 (expanding that the GDPR has been a "positive model" for breach notification policy while the fines, which were supposed to be imposed for companies who breach, has proven less effective because although the fine is an impressive percentage of total revenue, several of those companies are too small and others have yet to be penalized for failing to protect consumers data); *see also* Hodge, *supra* note 75 (finding that following the breach by British Airways, companies are concerned that the Information Commissioner's Office has overlooked other European supervisory authorities in granting fines under the GDPR as it has taken the regulators more time than expected to process the complaints).

cloud service, assign a Data Protection Officer ("DPO") to the company in order to ensure compliance.[80] In addition to the company who processed the biometric information being held liable, the GDPR holds the processors and third parties, such as a cloud service for data storage, accountable in the event of breach.[81]

V. SOLUTION

The absence of certain rights that private consumers should be granted in the United States regarding their biometric information grants corporations a wealth of power over individuals.[82] The legal action which the European Union has taken to protect the individual consumer's biometric data far outstretches the efforts of the United States because the European Union regulation is based on the principal that the individual is the proper owner of their data and that right does not belong to the data controllers or processors.[83]

Currently, there is not one uniform federal legislation implemented to protect individuals against the abuse of all categories of biometric information being processed, sold, and used by corporations.[84] Federal

---

[80] *See* Nadeau, *supra* note 71 (finding that the GDPR requires that a DPO position be created if that company "processes or stores large amounts of EU citizen data, process or store special personal data, regularly monitors data subjects, or are a public authority."); *see also* de Groot, *supra* note 67 (noting that in order to stay compliant with the GDPR, companies should assign a data protection officer to create a data protection program and ensure the company meets the requirements).

[81] *See* Nadeau, *supra* note 71 (noting that the data controller, data processor and the data protection officer will be held responsible for complying with the GDPR); *see also* Allan Ballany, *GDPR: Who's Responsible?*, CULTURE REPUBLIC (Oct. 30, 2017), https://www.culturerepublic.co.uk/blog/news-&-resources/gdpr-responsible/ (explaining that the data controller is the person or organization that decides the way the data will be used and the data processor is the person or organization that stores the data on behalf of the controller).

[82] *See* Will Yakowicz, *How Collecting Biometric Information from Employees and Customers Could Get You Sued,* INC. (May 12, 2016), https://www.inc.com/will-yakowicz/legal-risks-of-biometrics-at-the-office.html (explaining that because biometric identifiers are unique to each individual and are non-changeable such as the use of a password or key fob, when there is a risk of loss of that information, it is more detrimental to the employer); *see also* Ana Dascalescu, *Love Affair with Facial Recognition Software: What are the Cybersecurity Risks?,* CPO MAG. (May 23, 2019), https://www.cpomagazine.com/cyber-security/love-affair-with-facial-recognition-software-what-are-the-cybersecurity-risks/ (expanding on how there are no laws underway that fully protect the ways in which we use facial recognition infrastructure seeing as it is still evolving).

[83] *See* Andrada Coos, *EU vs US: How Do Their Privacy Regulations Square Off?*, ENDPOINT PROTECTOR (Jan. 17, 2019), https://www.endpointprotector.com/blog/eu-vs-us-how-do-their-data-protection-regulations-square-off/ (concluding that the EU's privacy and data protection is granted to all member states whereas in the United States, the regulations are at the state level); *see also* Danny Palmer, *What is GDPR? Everything You Need yo Know About the New General Data Regulations,* ZD NET (May 17, 2019), https://www.zdnet.com/article/gdpr-an-executive-guide-to-what-you-need-to-know/ (finding that the GDPR provides consumers with easier access to their personal information and a right to know when their data has been hacked in order for the individuals to act accordingly).

[84] *See Biometric Data and Data Protection Regulations (GDPR and CCPA)*, *supra* note 13 (explaining that in the United States there is "no single comprehensive federal law" regulating the use of biometric information); *see also* Todd Ehret, *Data Privacy and GDPR at One Year, A U.S.*

legislation should be passed which emulates the groundwork laid out by the GDPR and more specifically, it should mirror that of Article 17 of the GDPR titled, "The Right to be Forgotten" and apply it to biometric identifiers.[85] The Right to be Forgotten grants the individual consumer the ability to have their personal sensitive information erased from the internet at their request.[86] If the private consumer in the United States had the same right to have their biometric information erased from a company's database at their request as the citizens in Europe do for their online information, it would grant the individual sole ownership over their biometric identifiers, which are frequently processed and sold to third parties.[87] Biometric identifiers vary greatly from other types of personal information seeing as they are unique to a person's individual fingerprint, voice, and iris; therefore, the ability for a person to have their biometric identifiers completely erased at their request would do away with the concern over future breaches.[88]

Alongside the permanent erasure of personal information from the internet, this federal legislation would create a uniform biometric data privacy code for all states to adopt and enforce so that it becomes the

---

Perspective, Part Two – U.S. Challenges Ahead, REUTERS (May 29, 2019), https://www.reuters.com/article/us-bc-finreg-gdpr-report-card-2/data-privacy-and-gdpr-at-one-year-a-u-s-perspective-part-two-u-s-challenges-ahead-idUSKCN1SZ1US (elaborating on how the GDPR has set a "new standard for privacy laws" globally however, the U.S. has not advanced federal legislation in its response yet).

[85] *See* Ben Wolford, *Everything You Need to Know About the Right to be Forgotten*, GDPR.EU, https://gdpr.eu/right-to-be-forgotten/ (last visited May 27, 2020) (explaining that the Right to be Forgotten grants the data subject "the right to obtain from the controller the erasure of personal data concerning him or her without undue delay."); *see also* Michael Nuncic & Marion Wernado, *Understanding GDPR Article Seventeen and the Need for Secure Data Erasure*, ONTRACK (Mar. 20, 2018), https://www.ontrack.com/blog/2018/03/20/understanding-article-17/ (analyzing how the Right to Erasure requires companies to delete personal data if it is no longer needed, if the subject has withdrawn their consent, or if the data has been improperly processed).

[86] *See* Adam Satariano, *'Right to be Forgotten' Privacy Rule is Limited by Europe's Top Court*, N.Y. TIMES (Sept. 24, 2019), https://www.nytimes.com/2019/09/24/technology/europe-google-right-to-be-forgotten.html (finding that the Right to be Forgotten allows for large search engines such as Google to delete links, websites, news articles, and databases that have personal information that the subject considers, "old, no longer relevant, or not in the public interest"); *see also* Leo Kelion, *Google Wins Landmark Right to be Forgotten Case*, BBC (Sept. 24, 2019), https://www.bbc.com/news/technology-49808208 (explaining that the Right to be Forgotten, also known as the Right to Erasure, ensures EU citizens may request in writing or verbally that their information be taken down from the internet and the company has one month to respond).

[87] *See* Wolff, *supra* note 77 (finding that the United States should do away with the "patchwork system" that is currently in place and focus on a more unified data privacy regulation as that implemented in the EU); *see also* Satariano, *supra* note 86 (elaborating on how the Court in the EU stated that "certain categories of data deserve special consideration but must be weighed against the public's right to information").

[88] *See* Coos, *supra* note 83 (noting how the United States approach to data privacy is much more commercial focused unlike that of the EU which focuses on the individual's rights); *see also* NAT'L RES. COUNCIL, BIOMETRIC RECOGNITION: CHALLENGES AND OPPORTUNITIES, 85 (Joseph N. Pato et. al eds., 2010) (exploring how biometric information has an inherent link between "our physical bodies" and the biometric techniques employed to register information).

standard across all business operations which collect this type of information.[89] The standard would call for each company to hire or consult with a biometrics privacy data analyst who would ensure compliance with the law and aid in ways to avoid financial penalties and potential for litigation.[90] The closest the United States has been to setting out a standard for privacy data operations was with CCPA in California.[91] It aims to set a standard which would allow an individual consumer to have access to their biometric information that is collected by corporations. However, the standard does not apply to states who do not do business within California.[92]

Another way to grant the individual consumer in the United States ownership over their biometric information would be to implement a private right of action for each person who has been affected by a breach.[93] As a private consumer under the GDPR in the European Union, an aggrieved party is given the right to file a claim for "material and non-material damage" whereas in the United States, there is only a private right of action developed in Illinois.[94] This would further protect the sensitive

---

[89] *See* Wolff, *supra* note 77 (finding that the United States should be guided by the GDPR and note how a "unified framework for breach notifications" would be more effective than the individual state laws that are currently in place); *see also Biometric Data and Data Protection Regulations (GDPR and CCPA)*, *supra* note 13 (expanding on how the system that is established in the U.S. with its "patchwork" of state legislation can at times overlap and even be contradicting).

[90] *See* David Meyer, *In the Wake of GDPR, Will the US Embrace Data Privacy?*, YAHOO! FIN. (Nov. 29, 2018), https://finance.yahoo.com/news/wake-gdpr-u-embrace-data-113011021.html (finding that any future legislation the U.S. implements should include an agency who would "coordinate enforcement and report on the current state of affairs and threats to people's privacy"); *see also* Nadeau, *supra* note 71 (explaining that companies who wish to stay compliant with the GDPR should either hire a data protections officer to oversee data security strategy and compliance).

[91] *See* Stephens, *supra* note 58 (explaining that California's legislation set the bar "higher than ever before" in the U.S. for data privacy legislation); *see also* Korolov, *supra* note 55 (expanding that California's legislation took a broader approach than the GDPR in including protection over other types of personal information such as internet browsing history).

[92] *See* Korolov, *supra* note 55 (explaining that the CCPA does not require businesses to record a breach as the GDPR does and it also requires that consumers file complaints of the breach before a fine may be given to the corporation); *see also* Stephens, *supra* note 58 (finding that the CCPA would attempt to create the same amount of protection that the GDPR provides the EU but it may potentially be preempted by federal legislation).

[93] *See* Nathan Freed Wessler, *Ruling is a Warning to Companies Collecting Biometric Scans Without Permission*, ACLU (Feb. 8, 2019), https://www.aclu.org/blog/privacy-technology/surveillance-technologies/ruling-warning-companies-collecting-biometric (outlining that the decision in *Rosenbach* which held that a person need not allege "actual injury or adverse effect, beyond violation of his or her rights under the Act" in order to have standing to sue, stood for a principle that it is imperative that Congress and state legislatures allow for "strong laws" to protect people's rights to sue); *see also* Katherine Schwab, *A Landmark Ruling Gives New Power to Sue Tech Giants for Privacy Harms,* FAST COMPANY (Jan. 26, 2019), https://www.fastcompany.com/90297382/illinois-supreme-court-decision-marks-a-landmark-win-for-biometric-privacy-harm (finding that a citizen's ability to have a private right of action to sue companies who breach is necessary in "holding privacy-violating companies accountable for their actions").

[94] *See* Ehret, *supra* note 72 (expanding on how the EU's regulation has opened up a higher risk to private litigation because the people are able to file claims against any company who breaches the

information that is attached by putting large corporations on notice of their data privacy policies and in turn, grant justice to those who have been wronged.[95]

VI. CONCLUSION

There is a nationwide concern over policies which govern the ownership and distribution of an individual's biometric information at the expense of corporations.[96] Although there have been efforts by the Illinois, Texas, Washington, and California legislatures to create regulations surrounding the use, distribution, and selling of biometric identifiers, none have provided individual consumers with the adequate protection necessary to combat a dangerous breach.[97] The European Union's data regulation, the GDPR, has taken the global stage by implementing a large scale data privacy legislation in hopes of combating potential breaches and giving the individual consumer more control over their information.[98] The United States' efforts to give the individual consumer control over biometric identifiers, which are shared with corporations, does not grant the individual to have full range ownership.[99] Therefore, federal legislation, a private right of action, and standardized methods of processing and distribution of biometric data are imperative to give Americans their proper rights.[100]

GDPR); *see also* Duane C. Pozza & Kathleen E. Scott, *Biometrics Laws are on the Books and More are Coming: What You Need to Know*, WILEY REIN LLP (Apr. 2019), https://www.wileyrein.com/newsroom-newsletters-item-Apr_2019_PIF-Biometrics-Laws-Are-on-the-Books-and-More-Are-Coming-What-You-Need-to-Know.html (explaining that Illinois privacy law establishes a private right of action whereas Texas and Washington State do not).

[95] *See* Jason C. Gavejian & Joseph J. Lazzarotti, *Workplace Privacy, Data Management & Security Report*, WORK PLACE PRIVACY REP. (Jan. 25, 2019), https://www.workplaceprivacyreport.com/2019/01/articles/uncategorized/actual-harm-not-required-to-sue-under-illinois-biometric-information-privacy-law/ (expanding on how companies should adhere to BIPA regulations because the expenses incurred in order to stay compliant with the law's requirements are "insignificant" in comparison to the detrimental harm a breach in biometric identifiers can be if not properly secured); *see also* Nadeau, *supra* note 71 (reporting that companies should have a sense of urgency from top management in order to "prioritize cyber preparedness" in regards to the GDPR).

[96] *See* Meyer, *supra* note 90 (reporting how nine percent of Americans feel as though they have control over their personal information and how sixty-five percent of people would want control over what information is being shared about themselves); *see also Consumers are Concerned about Biometrics and Online Payments*, SECURITY MAG. (June 10, 2019), https://www.securitymagazine.com/articles/90347-consumers-are-concerned-about-biometrics-and-online-payments (reporting that fifty-six percent of North American and European consumers are concerned about the safety of biometric information).

[97] *See* Meyer, *supra* note 90 (finding that there is a philosophical difference in the way that Americans view the right to privacy data and the way Europeans view it); *see also* Wessler, *supra* note 93 (explaining that lawmakers should be conscious of the ways in which state legislatures, such as Illinois, have led the way for stricter regulations around biometric information which grant consumers a private right of action to sue).

[98] *See supra* Part IV.

[99] *See supra* Part III.

[100] *See supra* Part V.