Santa Clara University School of Law

Santa Clara High Technology Law Journal

Volume 38 | Issue 1 Article 2

2021

SHOULD PERSONAL INFORMATION AND BIOMETRIC DATA BE PROTECTED UNDER A COMPREHENSIVE FEDERAL PRIVACY STATUTE THAT USES THE CALIFORNIA CONSUMER PRIVACY ACT AND THE ILLINOIS BIOMETRIC INFORMATION PRIVACY ACT AS MODEL LAWS?

Buresh, Donald L.

SHOULD PERSONAL INFORMATION AND BIOMETRIC DATA BE PROTECTED UNDER A COMPREHENSIVE FEDERAL PRIVACY STATUTE THAT USES THE CALIFORNIA CONSUMER PRIVACY ACT AND THE ILLINOIS BIOMETRIC INFORMATION PRIVACY ACT AS MODEL LAWS?

By Donald L. Buresh[1]

The issue addressed in this paper was that only a minority of states have passed privacy and biometric privacy rights laws. The collection, storage, use, and dissemination of personal information and biometric data is becoming paramount due to the public's ever-increasing desire for security. The purpose of this study was to understand and evaluate the privacy and property issues that states confront that are inherent within the use and results of employing personal information and biometric data to enhance corporate security in their efforts to protect individual privacy. This research addressed the following questions: (1) What are the biometric privacy issues that states face regarding individual and corporate needs for security and privacy?; (2) Why do the several states continue to be vulnerable to litigation regarding biometric privacy issues?; (3) How does the State of Illinois address biometric privacy issues in its statutory effort to protect individuals against organizations that employ biometric cybersecurity procedures?; and (4) How does the Illinois Biometric Information Privacy Act benefit the federal government and other states in their efforts to create and pass biometric privacy laws that

[1] Donald L. Buresh earned his Ph.D. in the management of engineering and technology from Northcentral University. His dissertation assessed customer satisfaction for both agile-driven and plan-driven software development projects. Dr. Buresh also earned a J.D. from The John Marshall Law School located in Chicago, Illinois, focusing on cyber law and intellectual property. He also earned an LL.M in intellectual property from the University of Illinois Chicago Law School (formerly, The John Marshall Law School). Dr. Buresh received an M.P.S. in cybersecurity policy and an M.S. in cybersecurity concentrating in cyber intelligence, both from Utica College. He has an M.B.A. from the University of Massachusetts Lowell, focusing on operations management, an M.A. in economics from Boston College, and a B.S. from the University of Illinois Chicago, majoring in mathematics and philosophy. Dr. Buresh is a member of Delta Mu Delta, Sigma Iota Epsilon, Epsilon Pi Tau, Phi Delta Phi, Phi Alpha Delta, and Phi Theta Kappa. He has over 25 years of paid professional experience in Information Technology and has taught economics, project management, and negotiation at several universities. Dr. Buresh is an avid Chicago White Sox fan and keeps active by fencing épée at a local fencing club.

protect the privacy rights of their citizens? Four key findings are discussed in this study. The major finding was that neither the California Consumer Privacy Act as amended, the California Privacy Right Act nor Illinois' Biometric Information Privacy Act overlap to form a far-reaching privacy law because the subject matters of both laws are different. The recommendations argue that the United States needs an all-inclusive privacy law that encompasses both personal information and biometric information.

CONTENTS

INTRODUCTION

The privacy rights regarding the collection, use, storage, and dissemination of individual biometric data are in flux. Illinois, Texas, and Washington have passed biometric privacy laws within the last 20 years. Two states that are evaluating biometric privacy bills before their respective legislatures are Maryland and New York. The issue is that only a tiny minority of states recognize biometric privacy rights. The collection, storage, use, and dissemination of biometric data is becoming paramount due to the public's ever-increasing desire for security. How both federal and state governments respond to this craving for security concerning individual biometric data is an open question. Thus, this section aims to introduce privacy law in general, biometric privacy law, and what biometric information is and what it is not.

The purpose of this essay is to understand and evaluate the privacy and property issues that States confront that are inherent within the use and results of using biometrics to enhance corporate security in their efforts to protect individual privacy. This paper examines the Supreme Court cases that deal with an individual's right to privacy as well as several cases involving Illinois' Biometric Information Privacy Act (BIPA). It also discusses the recent American approaches to privacy and compares these approaches to how privacy is addressed in the European Union. The three states that have passed biometric security legislation into law are Illinois, Texas, and Washington. The Maryland and New York legislatures are debating similar bills. In conjunction with a brief description of the Texas and Washington biometric laws, the study examines Illinois' BIPA because it is a comprehensive biometric law that could become a model for federal legislation and a future standard to be used by the other states. Finally, because individuals have a vested interest in protecting their biometric data from misuse, the public could benefit from this analysis by understanding what they can expect from their state and the federal government to collect, store, use, and disseminate biometric data.

This essay's questions are: (1) What are the biometric privacy issues that States face regarding individual and corporate needs for security and privacy?; (2) Why do several States continue to be vulnerable to litigation regarding biometric privacy issues?; (3) How does the State of Illinois address biometric privacy issues in its statutory effort to protect the individuals against organizations that employ biometric cybersecurity procedures?; and (4) How does the State of Illinois Biometric Information Privacy Act benefit the federal government and other states in their efforts to create and pass biometric privacy laws that protect the privacy rights of their citizens?

I. LITERATURE REVIEW

A. A Brief History of Privacy Law

In the United States, privacy law began with the publication of the 1890 Harvard Law Review article by Warren and Brandeis, where the authors declared that privacy as a liberty right is "the right to be left alone."[2] Warren and Brandeis asserted that the purpose of their article was to "consider whether the existing law affords a principle which can properly be invoked to protect the privacy of the individual; and, if it does, what the nature and extent of such protection is."[3] Warren and Brandeis suggested that the law of nuisance and defamation were inadequate protections because these laws did not "protect the privacy of the individual from invasion either by the too enterprising press, the photographer, or the possessor of any other modern device for recording or reproducing scenes or sounds."[4] Essentially, Warren and Brandeis argued that there was no law to prevent the publication of information regarding individuals.[5] The Boston Brahmins, the elite of Boston high society in the 1890s, desired their data to remain private and out of the public domain.[6] The authors proposed that there should be laws to prevent the publication of information individuals deem to be confidential.[7]

In the first 50 years of the 20th Century, the law in the United States did not recognize the right to privacy. In *Olmstead*, the Supreme Court held that "obtaining of the evidence and its use at the trial did not violate the Fourth Amendment."[8] According to the Fourth Amendment, an individual is protected against unreasonable searches and seizures.[9] The Fourth Amendment states that a search or seizure is reasonable only when a warrant is issued by a neutral magistrate, where probable cause exists, and where the warrant is "supported by [o]ath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized".[10] In this case, the Court concluded

---

[2] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARVARD L. REV. 193, 193 (1890).
[3] *Id.* at 197.
[4] *Id.* at 206.
[5] *See generally* Warren & Brandeis, *supra* note 1.
[6] *Id.*
[7] *Id.*
[8] Olmstead v. United States, 277 U.S. 438, 438 (1928).
[9] U.S. CONST. amend. IV.
[10] *Id.*

that wiretapping a private telephone conversation without a warrant did not violate Olmstead's Fourth Amendment rights.[11]

The Supreme Court first expressly recognized the right to privacy in *Griswold*.[12] Here, three individuals were arrested and fined for providing contraceptive advice: the executive director of the Planned Parenthood League of Connecticut, a physician, and a Yale University professor.[13] In 1965, Connecticut law prohibited any method of preventing conception.[14] The issue was whether a married couple possessed a right to privacy when given contraceptive advice.[15] The Court held that the Connecticut law was unconstitutional and that married couples enjoyed a right to privacy when being given contraceptive advice.[16]

In *Katz*, the Supreme Court overruled *Olmstead* by extending an individual's Fourth Amendment protection to all areas or places where that person demonstrates a reasonable expectation of privacy.[17] In his concurring opinion, Justice Harlan created the reasonable expectation of privacy test for determining when a government activity is a search.[18] Justice Harlan formulated a two-pronged test for determining whether the privacy interest is present.[19] First, an individual must exhibit an actual or subjective expectation of privacy.[20] Second, the expectation of privacy must be an expectation that society recognizes or is prepared to acknowledge as reasonable.[21]

After *Griswold* and *Katz*, the Court seemed to reverse itself when it opined that the use and installation of a pen register, which is an electronic machine that records the numbers that are dialed from a telephone, by law enforcement is not a violation of an individual's reasonable expectation of privacy under the Fourth Amendment.[22] A pen register is an archaic and pre-Internet device that only recorded telephone numbers.[23]

---

[11] *See Olmstead*, 277 U.S. at 438.
[12] Griswold v. Connecticut, 381 U.S. 479, 484-85 (1965).
[13] *Id.* at 480.
[14] *Id.*
[15] *See generally Griswold*, 381 U.S. 479.
[16] *Id.*
[17] *See generally* Katz v. United States, 389 U.S. 347 (1967).
[18] *See Katz* 389 U.S. 347, 361 (Harlan, J., concurring).
[19] *Id.*
[20] *Id.*
[21] *Id.*
[22] Smith v. Maryland, 442 U.S. 735 (1979).
[23] 18 U.S.C. § 3127 (2018).

In *Kyllo*, the Court opined that using a forward-looking infrared (FLIR) device, which is also known as a thermal imaging device, to monitor the amount of infrared radiation that emanates from an individual's home, was a search that required a warrant based on probable cause.[24] A FLIR is a thermographic camera, typically employed on military and civilian aircraft, that senses infrared radiation.[25] Justice Scalia, who wrote the opinion, contended that the device's employment violated Kyllo's reasonable expectation of privacy.[26] A decade later, Justice Scalia concluded that the Fourth Amendment bars law enforcement from putting a global positioning system on a vehicle to keep track of its location without a warrant.[27]

In *Riley*, the Supreme Court stated that the search and seizure of a cell phone's digital contents when a person is being arrested are unconstitutional.[28] In the Court's opinion, a cell phone's digital contents are not a threat to officer safety.[29] In this case, the issue was that significant problems exist when searching the contents of a cell phone.[30] The Court concluded that searching the contents of a person's cell phone is equivalent to law enforcement searching through the private papers located in an individual's house.[31]

In *Carpenter*, Chief Justice Roberts wrote the majority opinion.[32] Here, the Court refused to give law enforcement access to cell phone metadata without a warrant.[33] The reasons dealt with the breadth, depth, and comprehensive nature of the metadata collection process.[34] In other words, a person has a reasonable expectation of privacy regarding the collection, use, and dissemination of cell phone metadata.[35]

However, *Carpenter*'s four separate minority opinions are particularly relevant regarding collecting, storing, using, and disseminating biometric information about human beings' innate

---

[24] Kyllo v. United States, 533 U.S. 27, 31-41 (2001).
[25] Anatholy Medvev, *What is a "Forward Looking Infrared Imaging System?"*, GUARDIAN.CO.UK, (n.d.), https://www.theguardian.com/notesandqueries/query/0,,-203857,00.html.
[26] *Kyllo*, 533 U.S. 31, 33-35.
[27] United States v. Jones, 565 U.S. 400 (2012).
[28] Riley v. California, 573 U.S. 373 (2014).
[29] *Id.* at 387.
[30] *Id.* at 378.
[31] *Id.* at 396-397.
[32] Carpenter v. United States, 138 S. Ct. 2206 (2018).
[33] *Id.* at 2223.
[34] *Id.*
[35] *Id.* at 2219.

characteristics.[36] The views of Justices Alito, Kennedy, and Thomas can be encapsulated into a simple phrase – no property rights, no privacy.[37] Justice Gorsuch's opinion is of particular interest when discussing whether biometric information should be protected.[38] According to Justice Gorsuch, cell phone providers are bailees who hold cell phone metadata to benefit the metadata or cell phone owners, also known as bailors.[39] A bailor is a person, natural or corporate, who temporarily relinquishes possession of a good or other property under a bailment agreement without surrendering ownership or property rights.[40] The bailor entrusts possession of a good or property to another person known as the bailee.[41] An example of a bailor/bailee relationship occurs when an individual takes their watch to a jeweler to be repaired. In this instance, the bailor is the watch owner who is taking the watch to a jeweler to be repaired. The bailee is the jeweler whom the bailor hires to repair the watch. The bailment is the agreement or contract between the bailor and the bailee whereby the bailor entrusts the bailee with the watch to be repaired.[42]

B. Definition of Biometric Information and Biometric Identifiers

The link between cell phone metadata and biometric data is that biometric information can be considered metadata about an individual. This is significant because, according to Pomerantz, the common-sense definition of metadata is that it is data about data.[43] This definition is unsatisfactory because it is vague.[44] However, Pomerantz pointed out that the definition can be salvaged if data are thought of as a "potentially informative object about another potentially informative object".[45] In other words, metadata is a statement about a potentially informative object.[46] The conclusion is that human beings can be

---

[36] *Id.* at 2223-61 (Kennedy, CJ, Alito & Thomas, JJ., dissenting).
[37] *Id.*
[38] *Id.* at 2268-69 (Gorsuch, J., dissenting).
[39] *Id.; see generally* Donald L. Buresh, *The Meaning of Justice Gorsuch's Dissent in Carpenter v. United States*, 43 AMER. J. OF TRIAL ADV. 55 (2019), https://heinonline.org/HOL/LandingPage?handle=hein.journals/amjtrad43&div=7&id=&page=.
[40] *Bailor*, BALLENTINE'S LAW DICTIONARY (3d ed. 1969).
[41] *Bailee*, BALLENTINE'S LAW DICTIONARY (3d ed. 1969).
[42] *Regular deposit*, BALLENTINE'S LAW DICTIONARY (3d ed. 1969).

[43] JEFFREY C. POMERANTZ, METADATA 19 (2015).
[44] *Id.*
[45] *Id.* at 26.
[46] *Id.*

modeled as potentially informative objects, where biometric information are implied statements about a person.

In consonance with these ideas, Illinois' Biometric Information Privacy Act defined biometric information to be "any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual."[47] Biometric information does not include information derived from items or procedures excluded under the definition of biometric identifiers.[48] Youmarin and Adler defined biometric information as the "decrease in uncertainty about a person's identity due to a set of biometric features measurements."[49]

Biometric features or identifiers are distinctive and measurable characteristics used to label and describe individuals.[50] Biometric identifiers are typically categorized as physiological versus behavioral characteristics.[51] Physiological characteristics are related to the shape of the body.[52] For example, fingerprints, palm veins, face geometry, deoxyribonucleic acid (DNA), palm prints, hand scans, iris recognition, retina, and odor or scent are all physiological characteristics.[53] Behavioral factors are associated with behavior patterns, including typing rhythm, gait, keystroke, signature, behavioral profiling, and voice.[54]

It is also essential to understand what is not biometric information. The Biometric Information Privacy Act states that "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,

---

[47] Biometric Information Privacy Act, 740 ILCS 14/10 (2008), https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57.
[48] *Id.*
[49] Richard Youmarin, & Andy Adler, *Measuring Information Content in Biometric Features*, In NIKOLAOS V. BOULGOURIS, KONSTANTINOS N. PLATANIOTIS, & EVANGELIA MICHELI-TZANAKOU (EDS.). BIOMETRICS: THEORY, METHODS, AND APPLICATIONS 579, 579-580 (John Wiley & Sons, Inc., 2010).
[50] Abdulaziz Alzubaidi & Jugal Kalita,, *Authentication of Smartphone Users Using Behavioral Biometric*s, 18 IEEE COMMUNICATIONS SURVEYS & TUTORIALS, 1998, 2001 (2016).
[51] *Id.*
[52] *Id.*
[53] Natalie Prescott, *The Anatomy of Biometric Laws: What U.S. Companies Need To Know in 2020*, THE NATIONAL LAW REVIEW (2020), *available at* https://www.natlawreview.com/article/anatomy-biometric-laws-what-us-companies-need-to-know-2020.
[54] Alzubaidi & Kalita, *supra* note 49, at 2001.

weight, hair color, or eye color are not biometric information."[55] Biometric information also does not include "donated organs, tissues, or parts … or blood or serum stored on behalf of recipients or potential recipients of living or cadaveric transplants and obtained or stored by a federally designated organ procurement agency."[56] The term biometric identifiers does not cover regulated biological materials (specifically, in Illinois, the Genetic Information Privacy Act of 2020), information captured from a patient in a health care setting, or information collected, used, or stored for health care treatment, payment, or operations under the federal Health Insurance Portability and Accountability Act.[57] Finally, biometric identifiers do not involve "an X-ray, roentgen process, computed tomography, M.R.I., P.E.T. scan, mammography, or other image or film of the human anatomy used to diagnose, prognose, or treat an illness or other medical condition or to further validate scientific testing or screening."[58]

C. Reasonable Expectation of Privacy

The reasonable expectation of privacy test may be inapplicable when analyzing the implications of collecting, using, storing, and disseminating biometric information because it may be readily discernable by third parties. When information is released voluntarily by an individual to a third party, that individual has no reasonable expectation of privacy.[59] Conversely, it can be inferred that when information is revealed involuntarily, a person may have a reasonable expectation of privacy.[60] Even so, the scope of this study is limited to when biometric information is voluntarily divulged. This study also discusses the legal consequences to third parties that involuntarily collect, use, store, and disseminate biometric data about individuals, as set forth in more detail below.

D. Biometric Information and Property Rights

Property rights give individuals privacy rights regarding their biometric information. In *Carpenter*, Justices Alito, Kennedy, and Thomas proclaimed in their minority opinions that property rights bestow an individual's privacy rights.[61] Justice Gorsuch also

---

[55] Biometric Information Privacy Act § 10.
[56] *Id.*
[57] *Id.*
[58] *Id.*
[59] United States v. Jones, 565 U.S. 400, 409 (2012).
[60] *See Id.*
[61] Carpenter v. United States, 138 S. Ct. 2206, 2223-61 (2018) (Kennedy, CJ, Alito & Thomas, JJ., dissenting).

acknowledged that privacy rights are intimately related to property rights when he stated that cell phone providers are bailees when entrusted with the metadata generated by a cell phone by cell phone owners or bailors.[62] In his seminal work on privacy, Lessig argued that property is privacy.[63] Humbach effectively argued that property rights had protected privacy in privately-owned spaces that store personal information such as papers and digital equipment for hundreds of years.[64] Kerrane observed that when an individual possesses a legitimate property interest in a location or an item, third parties that gain unauthorized access to that property violate an individual's reasonable expectation of privacy.[65]

Because places and objects are external to a human being and thus not necessarily "private," the question is whether individuals possess property rights to their biometric information. According to the Biometric Information Privacy Act, "[n]o 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."[66] This statement sounds all too familiar to the right of publicity which protects a person's intangible proprietary interest in the commercial value in their identity.[67] The right to privacy to information regarding one's person was clarified by Prosser when he organized the right to privacy doctrine into the following four distinct torts: (1) unreasonable intrusion upon another's seclusion, (2) public disclosure of private facts, (3) false light invasion of privacy, and (4) appropriation of another's name or likeness.[68]

From the four torts listed above, the public disclosure of private facts is the most relevant to disclosing biometric information. Although most state laws specify that the right of publicity protects a person's

---

[62] *Id.* at 2268-69 (Gorsuch, J., dissenting).

[63] *See generally* Lawrence Lessig, *Privacy as Property*, 69 SOC'Y. RSCH. 247 (2002), https://www.jstor.org/stable/40971547?seq=1#page_scan_tab_contents.

[64] John A. Humbach, *Privacy and the Right of Free Expression*, 11 FIRST AMEND. L. REV. 16, 17 (2012), https://digitalcommons.pace.edu/lawfaculty/863/.

[65] Kaitlyn A. Kerrane, *Keeping up with Officer Jones: A Comprehensive Look at the Fourth Amendment and GPS Surveillance*. 79 FORDHAM L. REV. 1695, 1709 (2011), https://ir.lawnet.fordham.edu/flr/vol79/iss4/8.

[66] Biometric Information Privacy Act, 740 ILCS 14/15(c) (2008), https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57.

[67] Lugosi v. Universal Pictures, 603 P.2d 425, 445 (1979).

[68] William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383, 389 (1960), https://www.jstor.org/stable/3478805?refreqid=excelsior%3Ab690af40da42182b188450a5d603a842&seq=1.

identity when such information is used for commercial purposes, private individuals, not just celebrities, can also sue for instances of public disclosure of private facts.[69] In other words, the unauthorized use of biometric information about a person, much like the infringement of a person's right of publicity, is an encroachment on an individual's property rights.[70] The implication is that individuals possess property rights to their biometric information, and those rights are deserving of legal protection. One function of a sovereign state should be to protect individual property rights.[71]

E. The Importance of Biometric Privacy

At both the federal and state levels, private organizations and governments readily acquire vast amounts of data on individuals as they go about their daily business.[72] Almost everything people use these days demands that they log into their email address, Facebook profile, and even cell phones.[73] These software applications collect and store metadata regarding what websites are visited, how long one is on a website, what a person buys on a website, etc.[74] These organizations, such as Facebook and Google, make money by collecting personal information and then selling it to third parties.[75] What is immediately apparent from the picture just painted is that privacy is on the decline.

F. Reasons for Why Biometric Privacy Is Important

According to Reetz and his colleagues, the technologies associated with social media, electronic communication, mobile devices, intelligent home assistants, biometric authentication, autonomous vehicles, digital health monitors, and the emerging dominance of artificial intelligence are some of the forces transforming

---

[69] JONATHAN S. JENNINGS, & J. MICHAEL MONAHAN, TRADEMARKS AND UNFAIR COMPETITION: CRITICAL ISSUES IN THE LAW 5-13 (2014).
[70] *Id.* at 174-175.
[71] ROGER PILON, *Property Rights and the Constitution*, in CATO INSTITUTE, CATO HANDBOOK FOR POLICYMAKERS 173-91 (8th ed. 2017), https://www.cato.org/cato-handbook-policymakers/cato-handbook-policy-makers-8th-edition-2017/property-rights-constitution.
[72] Michael Monajemi, *Privacy Regulation in the Age of Biometrics that Deal with a New World Order of Information*, 25 UNIV. OF MIAMI INT'L. & COMP. L. REV. 371, 373 (2018), https://repository.law.miami.edu/umiclr/vol25/iss2/7.
[73] *Id.*
[74] *Id.*
[75] *Id.*

human activities, both in the public and private arenas.[76] Central to understanding privacy in general, and biometric privacy in particular, is the question of how much people value their privacy and what evils should privacy and biometric privacy attempt to deter.[77] The public's comfort level regarding collecting personal information depends on the type of data being collected and how such data is used by organizations collecting, storing, using, and disseminating that data.[78]

On its face, the future of privacy is uncertain. According to Kleven, privacy cases' critical procedural issue is "minimum virtual contacts" to establish personal jurisdiction.[79] According to the Legal Information Institute, minimum contacts for a non-resident defendant with a forum state (i.e., the state where a plaintiff brings a suit) are the connections that a defendant has with the forum state.[80] The maintenance of a lawsuit without minimum contacts in the state offends the "traditional notions of fair play and substantial justice" and, in turn, violates the Due Process Clause.[81] Kleven proposed that minimum virtual contacts are similar to, if not the same as, the traditional minimum contacts legal principle.[82]

Hu observed that governments' evolution into cyber-surveillance states is occurring because governments are employing technologies that combine biometric and biographic data to target digital data associated with suspicious individuals.[83] Hu opined that the progression to becoming a cyber-surveillance state is making it increasingly difficult to identify and challenge an individual's

---

[76] Margaret A. Reetz, Lauren B. Prunty, Gregory S. Mantych, & David J. Hommel, *Cyber Risks: Evolving Threats, Emerging Coverages, and Ensuing Case Law*, 122 PENN STATE L. REV. 727, 727 (2018), https://www.pennstatelawreview.org/print-issues/cyber-risks-evolving-threats-emerging-coverages-and-ensuing-case-law/.

[77] Matthew B. Kugler, *From Identification to Identity Theft: Public Perceptions of Biometric Privacy Harms*, 10 U.C. IRVINE L. REV. 107, 107 (2019), https://scholarship.law.uci.edu/ucilr/vol10/iss1/5.

[78] *Id.* at 112.

[79] Adam R. Kleven, *Minimum Virtual Contacts: A Framework for Specific Jurisdiction in Cyberspace*, 116 MICH. L. REV. 785, 785 (2018), https://repository.law.umich.edu/mlr/vol116/iss5/4.

[80] *Minimum Contacts*, LEGAL INFORMATION INSTITUTE, https://www.law.cornell.edu/wex/minimum_contacts (last visited Aug. 30, 2021).

[81] International Shoe Co. v. Washington, 326 US 310, 316 (1945).

[82] Kleven, *supra* note 78, at 809.

[83] Margaret Hu, *From the National Surveillance State to the Cybersurveillance State*, 13 ANN. REV. OF L. AND SOC. SCI. 161, 161 (2017).

constitutional right to a reasonable expectation of privacy.[84] Jones observed that biometric identification systems had transformed government, military, and private-industry identification and verification procedures.[85]

G. Examples of Why Biometric Privacy Is Important

But there is more. According to Metzger, businesses increasingly require their employees to permit biometric data collection technologies to clock their hours, probably to verify or increase productivity.[86] The issue is that with this embracing of biometric technology comes privacy and security concerns.[87] For example, the front office of a Major League Baseball (MLB) team is charged with creating a solid team, which usually results in winning more games, attracting more fans, and increasing profits.[88] In many cases, players need coaching to hone their baseball skills, and clubs need to separate major league-caliber players from the plethora of minor league players whose abilities do not meet MLB performance standards.[89] Zych aptly observed that the question of property rights to biometric data is temporarily set aside in favor of exploiting the data to win baseball games.[90] Justice Gorsuch precisely attempted to resolve this issue in his dissent in *Carpenter* when he opined that cell phone providers are bailees entrusted with cell phone metadata by bailors or cell phone owners.[91] Furthermore, Garlewicz described how soccer teams are collecting biometric data about their players to determine which

---

[84] *See generally id.*

[85] Daveante Jones, *Protecting Biometric Information in Arkansas*, 69 ARK. L. REV. 117, 117 (2016).

[86] Anna L. Metzger, *The Litigation Rollercoaster of BIPA: A Comment on the Protection of Individuals from Violations of Biometric Information Privacy*, 50 LOYOLA UNIV. OF CHICAGO L. J. 1051, 1060 (2020), https://lawecommons.luc.edu/luclj/vol50/iss4/14.

[87] *Id*.

[88] Nicholas Zych, *Collection and Ownership of Minor League Athlete Activity Biometric Data by Major League Baseball Franchises*, 14 DEPAUL J. OF SPORTS L. & CONTEMP. PROBS. 129, 130 (2018), http://via.library.depaul.edu/cgi/viewcontent.cgi?article=1155&context=jslcp .

[89] *Id.*

[90] *Id.* at 130-31.

[91] Carpenter v. United States, 138 S. Ct. 2206, 2268-69 (2018) (Gorsuch, J., dissenting).

players will be successful in the major leagues.[92] Gale analyzed the legal implications in collecting athlete biometric data (ABD), pointing out that a precise ABD definition is difficult to achieve due to the myriad of ways ABD interacts with the sports industry.[93]

Logan stated that eye-tracking technology has existed since the 1950s.[94] As eye-tracking hardware and software have become ubiquitous,[95] Logan argued that if privacy rights are established for biometric identifiers, there will be less friction in creating new technologies.[96] According to Logan, this situation will permit rapid growth for eager and informed consumers.[97] In particular, Norris pointed out that casinos have been tracking people's activities inside their establishments for years.[98] Casinos possess an abundance of private data that demonstrates how people behave when they are under surveillance.[99]

Still another example is that immigration officials and other bureaucrats collect biometric data to ensure that immigrants' identities can be unambiguously determined.[100] Classification systems were generated to ensure that a person's identity was unambiguously verified by employing official documents over time and across countries.[101] According to Kim, the use of biometric data in the immigration process is beneficial not only to the government but also

---

[92] Adam Garlewicz, *Athlete Biometric Data in Soccer: Athlete Protection or Athlete Exploitation?*, 16 DEPAUL J. OF SPORTS L. & CONTEMP. PROBS. 1 (2020), https://via.library.depaul.edu/jslcp/vol16/iss1/2.

[93] Kristy Gale, *Evolving Sports Technology Makes Its Mark on the Internet of Things: Legal Implications and Solutions for Collecting, Utilizing, and Disseminating Athlete Biometric Data Collected via Wearable Technology*, 5 ARIZ. ST. SPORTS & ENTER. L. J., 337, 363 (2016), http://asuselj.org/wp-content/uploads/2015/10/Full-Volume-5-Issue-2-1.pdf.

[94] Ian Taylor Logan, *For Sale: Window to the Soul Eye Tracking as the Impetus for Federal Biometric Data Protection*, 123 PENN STATE L. REV. 779, 779 (2019), https://elibrary.law.psu.edu/pslr/vol123/iss3/7.

[95] *Id.*

[96] *Id.* at 779-80.

[97] *Id.*

[98] Stacy Norris, *"...And the Eye in the Sky is Watching Us All" - The Privacy Concerns of Emerging Technological Advances in Casino Player Tracking*, 9 UNLV GAMING L. J. 269, 271 (2019), https://scholars.law.unlv.edu/glj/vol9/iss2/9.

[99] *Id.* at 272.

[100] Jaeeun Kim, *Establishing Identity: Documents, Performance, and Biometric Information in Immigration Proceedings*, 36 LAW & SOCIAL INQUIRY 760, 762 (2011).

[101] *Id.* at 763.

to the individual because it can speed up an inherently tedious process.[102]

There are definite and well-defined benefits of collecting, storing, using, and disseminating biometric information by organizations.[103] However, in all fairness, the harms should also be discussed. Reetz and his colleagues observed that significant risks and exposures have evolved from concerns regarding personal privacy and the confidentiality of corporate assets to threats of organizational interference and operational disruptions, such as cybersecurity attacks.[104] They also observed that with the emergence of biometric data collection, storage, use, and dissemination, there are direct threats of illegal transfers of funds and actual physical harm, injury, and loss.[105] The question that Reetz and his colleagues asked was whether the privacy "landscape [has] changed so profoundly that entirely new approaches are required."[106]

H. Harms Due to Violations of Biometric Privacy

According to Wright, there are broad implications of biometric privacy harms that justify far-reaching privacy regulations rather than a narrow concentration on data security and self-regulation.[107] Wright argued that in regulating the collection, storage, use, and dissemination of biometric data, a collaborative approach with private organizations might significantly benefit society because of the lack of technical expertise among legislators.[108] An example of harm is privacy leakage, where privacy leakage is the amount of information that a public

---

[102] *Id.* at 774.

[103] Hu, *supra* note 82, at 163 ("Biometric identification and identity assessments are becoming essential tools for multiple preventive purposes in criminal, military, and intelligence contexts."); Zych, *supra* note 87, at 130-131 (discussing the relationship between athlete biometric data and team success); Norris, *supra* note 97, at 286-287 (explaining how biometric data can benefit casinos and their players); Kim, *supra* note 99, at 760 (explaining how migrants use biometric information as "identity tags" to establish the authenticity of family relations).

[104] Reetz et al., *supra* note 75, at 727.

[105] *Id.* at 727, 751 n. 143.

[106] *Id* at 727.

[107] Elias Wright, *The Future of Facial Recognition Is Not Fully Known: Developing Privacy and Security Regulatory Mechanisms for Facial Recognition in the Retail Sector*, 29 FORDHAM INTELL. PROP., MEDIA, AND ENT. L. J. 611, 611 (2019), https://ir.lawnet.fordham.edu/iplj/vol29/iss2/6.

[108] *Id.* at 677.

message contains about biometric enrollments.[109] According to Gomez-Barrero and his colleagues, when morphed biometric samples or templates are introduced into a biometric recognition system, the subjects that contribute to the morphed sample can be successfully verified against an enrolled template.[110] This unique link precipitates serious security gaps when verifying electronic travel documents.[111] Gomez-Barrero and his colleagues observed that a systematic approach to predicting biometric vulnerabilities has not yet been established.[112] They then proposed a framework for evaluating the exposure to security gaps of biometric systems.[113]

Thus, it is evident that biometric privacy is of paramount importance. However, to appreciate the importance of biometric privacy, a melodic interlude into the realm of privacy law, in general, is needed. The succeeding subsections of this literature will discuss the European Union's (EU) General Data Protection Regulation (GDPR), followed by a brief discussion of the privacy laws of the several states, including the California Consumer Privacy Act and its amendment, the California Privacy Rights Act, the Nevada Revised Statutes Chapter 603A, the Virginia Consumer Data Protection Act, along with a discussion of the status of various privacy bills in the several states. Next, the essay will talk about the biometric privacy laws in Illinois, Texas, and Washington, where the emphasis is given to the Illinois Biometric Privacy Act (BIPA) because it is the most detailed of the various biometric privacy laws currently in force. Finally, the study will summarize the literature review contained herein.

II. GENERAL DATA PROTECTION REGULATION

The General Data Protection Regulation (GDPR) is a set of legal guidelines that deal with collecting and processing personal information about people who live and reside in the European Union.[114]

---

[109] Tanya Ignatenko & Frans M. J. Willems, *Biometric Security From an Information-Theoretical Perspective*, 7 FOUND. AND TRENDS IN COMM. AND INFO. THEORY, 135 (2012).

[110] Marta Gomez-Barrero, Christian Rathgeb, Ulrich Scherhag, & Christoph Busch, *Predicting the Vulnerability of Biometric Systems to Attacks Based on Morphed Biometric Information*, 7 IET BIOMETRICS 333, 333 (2018).

[111] *Id.*

[112] *Id.*

[113] *Id.*

[114] Jake Frankenfield, revised by Amy Drury, *General Data Protection Regulation (GDPR)*, INVESTOPEDIA, (November 11, 2020), https://www.investopedia.com/terms/g/general-data-protection-regulation-gdpr.asp; *see also* IT GOVERNANCE PRIVACY TEAM, EU GENERAL DATA

The GDPR applies independently from where a website is based.[115] Any site accessed by a European visitor, regardless of whether an organization markets goods or services to EU residents, must comply with the regulation.[116]

A. A Brief History of the General Data Protection Regulation

On September 23, 1980, the Organization for Economic Co-operation and Development (OECD), a European international organization, approved the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.[117] Although the OECD guidelines were not obligatory, the document specified a framework for future privacy legislation and court opinions.[118] The principles listed in the guidelines (1) ensured that the collection of personal information was lawful, (2) specified that the use of personal information should be accurate, complete, and current, (3) stated that the purpose of collecting information should be explicit before any data is collected, (4) required that personal information should be reasonably protected against the risks of destruction, disclosure, loss, modification, unauthorized access, and use, (5) demanded that practices and procedures be readily available, (6) acknowledged that individuals have the right to acquire their personal information that was collected or verify that the data exists, and (7) warranted that data control organizations were accountable for complying with these principles.[119]

PROTECTION REGULATION (GDPR): AN IMPLEMENTATION AND COMPLIANCE GUIDE 11, 11 (2nd ed. 2017).

[115] Frankenfield*, supra* note 113; *see also* IT GOVERNANCE PRIVACY TEAM, *supra* note 113, at 16.

[116] Frankenfield, *supra* note 113; *see also* IT GOVERNANCE PRIVACY TEAM, *supra* note 113, at 28-29.

[117] OECD Guidelines, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, (n.d.), https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

[118] *Id.*

[119] Donald L. Buresh, *A Comparison between the European and American Approaches to Privacy*, 6 INDONESIAN J. OF INT. AND COMP. L. 253, 255-56 (2019), https://heinonline.org/HOL/LandingPage?handle=hein.journals/indjicl6&div=16&id=&page=.

In 1990, the European Commission (EC) published a Data Protection Directive (DPD) proposal.[120] In 1995, after five years of negotiations, the final DPD, also known as Directive 95/46/EC, was adopted by the EU.[121] There were immediate problems with the directive because it did not harmonize with the privacy laws of EU member nations, and thus, the enforcement of the directive was haphazard.[122] In 2009, the EC began consulting with the EU member nations, and in 2012, the EC published the first proposed text of the GDPR.[123] In 2015, and after nearly 4,000 amendments, the Council of the European Union (CEU) published its proposal for the GDPR and started its negotiations with the European Parliament (EP).[124] In December 2015, the EP and the CEU agreed on the final text of the GDPR, which was adopted in May 2016, and went in force on May 25, 2018, replacing the DPD.[125]

B. Content of the General Data Protection Regulation

The GDPR consists of 11 chapters, 99 articles, and 173 recitals.[126] The general obligations that an organization must follow are contained in Article 24, whereas Article 28 categorizes the technical and organizational measures for data processors.[127] According to Article 6, the processing of personal information should be predicated on at least one lawful basis, such as "consent, compliance with a legal duty, contract, performance, protection of the vital interests of the data subject, and the legitimate interest of the data controller."[128] Article 9(1) prevents entities from the processing of personal information that reveals "racial or ethnic origin, sexual orientation, political sentiments, religious beliefs, union membership, or genetic or *biometric data* that can be employed in identifying an individual."[129] Article 9(2) lists the

---

[120] Chris Jay Hoofnagle, Bart van der Sloot, & Frederik Zuiderveen Borgesius, *The European Union General Data Protection Regulation: What It Is and What It Means*. INFO. & COMM. TECH. L., 28(1), 65-98, (February 10, 2019), https://doi.org/10.1080/13600834.2019.1573501.
[121] *Id.*
[122] Hoofnagle et al., *supra*, note 119.
[123] *Id.*
[124] *Id.*
[125] *Id.*; *see also* Manuel Klar, *Binding Effects of the European General Data Protection Regulation (GDPR) on US Companies*, 11 HASTINGS SCI. & TECH. L. J. 101, 102 (2020).
[126] Buresh, *supra*, note 118, at 261.
[127] *Id.*
[128] *Id* at 261.
[129] *Id* at 261-62 (emphasis added).

exclusions to Article 9(1), including when a data subject agrees to publicize personal information.[130]

Article 30 requires that personal information controllers and processors maintain a record of their processing activities.[131] Article 4(11) posits that consent must be explicit, while opt-out consent is forbidden.[132] A data subject can withdraw consent at any time.[133] Under Article 33, data protection authorities must be informed within 72 hours after a breach becomes known.[134] Article 34 demands that if there is a high risk that individual rights and freedoms will be violated due to a breach, data subjects must be informed, subject to the exceptions in Article 34(3).[135] Article 37 specifies that organizations have a data protection officer charged with protecting the personal information of data subjects and is responsible for informing data controllers, processors, and employees that they are accountable under the GDPR.[136]

According to Article 3(2), the GDPR applies to any company that falls within its territorial and material scope, including firms located in the United States.[137] First, Article 3(2) applies to the processing of personal information of an establishment or organization.[138] Second, the GDPR pertains to the processing of personal information of data subjects regarding the offering of goods or services to EU data subjects.[139] Finally, the GDPR concerns the data processing activities that deal with monitoring the activities of EU data subjects.[140] What Article 3(2) means is that if an American firm does business with individuals or organizations in the EU, it must comply with the GDPR. Regarding biometric privacy, Article 14(4) is particularly relevant because when a data controller intends to process data for which the relevant consents are not obtained, the GDPR

---

[130] Buresh, *supra*, note 118 at 262; *see also* Hoofnagle et al., *supra* note 119, at 82.
[131] Buresh, *supra*, note 118 at 262; *see also* Hoofnagle et al., *supra* note 119, at 85.
[132] Buresh, *supra*, note 118 at 262; *see also* Hoofnagle et al., *supra* note 119, at 79.
[133] Buresh, *supra*, note 118 at 262; *see also* Hoofnagle et al., *supra* note 119, at 90.
[134] Buresh, *supra*, note 118 at 262.
[135] *Id.*; *see also* Hoofnagle et al., *supra* note 119, at 87.
[136] Buresh, *supra* note 118, at 262; Hoofnagle et al., *supra* note 119, at 86.
[137] Klar, *supra* note 124, at 105.
[138] *Id.*
[139] *Id.* at 110
[140] *Id.* at 115

requires that the data controller provide the data subject with the new reason for collecting the data.[141] When considering Articles 9(1) and 14(4) together, they explicitly address how biometric information should be handled by organizations that do business with EU data subjects or EU establishments.

C. Google v. Costeja González and The Right to Be Forgotten

The case *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González* is particularly significant when discussing privacy and biometric privacy within the European Union.[142] *Costeja González* is significant because it demonstrates the European belief that the right to privacy, and biometric privacy, can be construed to be the right to be forgotten.[143] The case balances an individual's right to privacy and the EU's data protection regulations versus an organization's and the public's right to know.[144]

In the case, the Court of Justice of the European Union (CJEU) held that Google Spain SL and Google, Inc. must eradicate links to web pages that are freely accessible worldwide when individuals whose personal information is contained therein demand that the links be removed.[145] The result of the CJEU ruling was that an internet search engine must address the requests of individuals who ask that links be eliminated to freely accessible web pages when a third party conducts a search based on the individual's name.[146] The eradication reasons include situations where the search results are facially inadequate, no longer relevant, or an excessive amount of time has elapsed.[147] If the search engine refuses to honor the plea, an individual can petition the EU courts to redress grievances.[148] The European courts reserve the

---

[141] Parliament Regulation 2016/679, 2018, Art. 14(4) (2018), *available at* https://gdpr-text.com/read/article-14/.https://gdpr-text.com/read/article-14/.
[142] Press Release No 70/14, Court of Justice of the European Union, An Internet Search Engine Operator is Responsible for the Processing That it Carries Out of Personal Data Which Appear on Web Pages Published by Third Parties (May 13, 2014), available at https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070en.pdf.
[143] *Id.*
[144] Buresh, *supra* note 118, at 259.
[145] Press Release, No. 70/14 *supra* note 141.
[146] *Id.*
[147] *Id.*
[148] *Id.*

right to overrule the search engine's decision and order the controller to take specific measures accordingly.[149]

In 1998, La Vanguardia, a Spanish newspaper, published two announcements regarding a forced sale of properties from social security debts.[150] The statements were published by the Spanish Ministry of Labor and Social Affairs to entice people to bid on an auction's properties.[151] The announcements were also published on the newspaper's website.[152] One of the properties belonged to Mario Costeja González, and he was specifically named in one of the announcements.[153] In 2010, Costeja González requested that his name no longer be part of the Google database.[154] Costeja González wanted his name removed because the forced sale occurred nearly ten years earlier and was no longer relevant.[155] La Vanguardia denied the request under the belief that erasing Costeja González's data was improper because the Spanish Ministry of Labor and Social Affairs had ordered that his name be published.[156]

In his complaint, Costeja González asked Google Spain SL to remove the links.[157] Google Spain SL alerted Google, Inc., regarding the suit.[158] Costeja González then filed a complaint with the Spanish Data Protection Agency, or the Agencia Española de Protección de Datos (AEPD), requesting that La Vanguardia, and Google Spain SL or Google, Inc. delete the links.[159] On July 30, 2010, the AEPD rejected the complaint against La Vanguardia but endorsed the complaint against Google Spain SL and Google, Inc.[160] Google Spain SL and Google, Inc. appealed Spain's National High Court decision, or the Audiencia Nacional (AN).[161] Google Spain SL and Google, Inc. argued that (1) EU Directive 95/46/EC did not have jurisdiction over Google,

---

[149] *Id.*
[150] *Id.*
[151] *Id.*
[152] *Id.*
[153] *Id.*
[154] Jeffrey Toobin, *The Solace of Oblivion*, THE NEW YORKER, (Sep. 22, 2014), *available at* https://www.newyorker.com/magazine/2014/09/29/solace-oblivion.
[155] Press Release, No. 70/14 *supra* note 141.
[156] *Id.*
[157] *Id.*
[158] *Id.*
[159] *Id.*
[160] *Request for a Preliminary Ruling from the Audiencia Nacional*, AUDIENCIA NACIONAL (SPAIN), (May 13, 2014), *available at* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131.
[161] Press Release, No. 70/14 *supra* note 141.

Inc., (2) no data processing occurred, (3) if data processing did occur, neither Google, Inc. nor Google Spain SL were data controllers, and Costeja González had no right to ask the search engine to remove the offending links.[162] The AN issued a stay pending a preliminary decision from the CJEU based on EU Directive 95/46/EC.[163] The case was heard by the CJEU, and on May 13, 2014, the CJEU published its judgment.[164]

The CJEU concluded that Google Spain SL's and Google, Inc.'s reasons were not compelling.[165] The court opined that Google, Inc. was responsible for removing Costeja González's data.[166] The forced sale of Costeja González's property should be electronically forgotten because the information was no longer relevant.[167] The CJEU also held that Article 14(a) of EU Directive 95/46/EC as related to Articles 7(e) and 7(f) permitted Costeja González to object to the search engine keeping his data online.[168] Finally, Article 12(b) allowed Costeja González to ask the search engine to remove his data.[169] In terms of biometric information, *Costeja González* implies that EU data subjects have the right to request that organizations subject to the GDPR remove their data without limitation, subject to the exceptions contained in the regulation.[170]

III. PRIVACY LAWS IN THE SEVERAL STATES

In this section of this essay, the California Consumer Privacy Act and its amendment, the California Privacy Rights Act, the Nevada privacy law, the Maine privacy law, the Virginia Consumer Data Protection Act, and the Colorado Privacy Act will be discussed in turn. The states where privacy bills are under legislative review will also be examined because it is crucial to understand where privacy law is headed.

---

[162] *Id.*
[163] *Request for a Preliminary Ruling from the Audiencia Nacional*, *supra*, note 159.
[164] Press Release, No. 70/14 *supra* note 141
[165] *Id.*
[166] *Id*.
[167] *Id.*
[168] *Id. see also Request for a Preliminary Ruling from the Audiencia Nacional*, *supra* note 159.
[169] *Id.*
[170] *Id*.

A. California Consumer Privacy Act

On June 28, 2018, then California Governor Jerry Brown signed SB-375, also known as the California Consumer Privacy Act (CCPA).[171] The California legislature passed the first amendments to the CCPA on August 31, 2018, and the CCPA became effective on January 1, 2020.[172] The purpose of the law was to protect the personal information of California consumers regardless of what sector of the economy the data originated.[173] In the United States, there is no comprehensive privacy law that defends consumers from the collection, storage, use, and dissemination of personal information by private entities such as the GDPR.[174] Congress has passed privacy laws on a topic-by-topic basis predicated on practical political needs, such as adopting the Fair Credit Reporting Act, the Health Insurance Portability and Accountability Act, and the Gramm-Leach-Bliley Act.[175]

The CCPA considers a California resident domiciled to be a California consumer under the CCPA.[176] The statute does not protect the personal information of individuals temporarily located within California.[177] The CCPA applies to for-profit businesses and partnerships that collect and process personal information of California consumers, where (1) the annual revenue of the company is greater than $25 million, (2) the firm receives or discloses the personal information of at least 50,000 California residents, and (3) fifty percent or more of an entity's annual revenue is derived from selling personal information.[178]

According to the CCPA, a California resident possesses the right to know the classes of personal information collected, the source of the personal information, and what entities are purchasing that information.[179] California residents also have the right to review the personal information being amassed to ensure that only correct

---

[171] Buresh, *supra* note 118, at 269.
[172] *Id.*
[173] *Id.*
[174] Jeeyun (Sophia) Baik, *Data Privacy Against Innovation or Against Discrimination? The Case of the California Consumer Privacy Act (CCPA)*, 52 TELEMATICS AND INFORMATICS 1, 5 (2020).
[175] *Id.*
[176] Buresh, *supra* note 118, at 270.
[177] *Id.*
[178] KPMG Staff, *The Time Is Now to Prepare for Changes to California's Privacy Law*, KPMG, LLP 2 (2018), https://advisory.kpmg.us/content/dam/advisory/en/pdfs/driving-change.pdf.
[179] Buresh, *supra* note 118, at 270.

information is being marshaled.[180] Finally, California residents enjoy the right to request that their personal information be deleted, or in other words, California residents possess the right to be forgotten.[181]

There are seven critical provisions in the CCPA. First, California consumers have the right to opt out of the sale of their personal information.[182] Second, businesses that the CCPA cover cannot charge California residents a higher price when they exercise their rights under the Act.[183] Third, a data collection firm is required to give California consumers a copy of their data in an electronic format that is easily transferable.[184] Fourth, for individuals that are under 16 years of age, a data collection company must be given permission by the parents or guardians of that individual before the entity can sell the person's personal information.[185] Fifth, any company doing business in California must disclose to the public on an annual basis the categories, recipients, and sources of all of the data that the firm collects, stores, discloses, or sells.[186] Sixth, a link must exist on a corporation's website entitled "Do Not Sell My Personal Information" that allows California residents to exercise their right not to sell their personal information.[187] Finally, an organization doing business in California is required to stipulate two methods where a consumer can request their personal information from a company.[188]

The CCPA specifies two types of non-compliance penalties. First, there are penalties due to security breaches. According to the CCPA, the damages are at most $750 per violation or the actual damages, whatever is the greater amount.[189] The Attorney General of California may enforce the privacy provision of the CCPA via civil penalties with a maximum of $7,500 per violation.[190] For example, it is not uncommon for a data breach to involve one million individuals. At

---

[180] *Id.*
[181] *Id.*
[182] Rodgin Cohen, John Evangelakos, Nader Mousavi, Matthew Schwartz, & Nicole Friedlander, *Sullivan & Cromwell Discusses California Consumer Privacy Act of 2018*, THE CLS BLUE SKY BLOG, (July 23, 2018), https://clsbluesky.law.columbia.edu/2018/07/23/sullivan-cromwell-discusses-california-consumer-privacy-act-of-2018/.
[183] *Id.*
[184] Buresh, *supra* note 118, at 271.
[185] Cohen et al., *supra* note 181, at 5.
[186] Buresh, *supra* note 118, at 271-72.
[187] *Id.* at 272.
[188] Cohen et al., *supra* note 181, at 3.
[189] Buresh, *supra* note 118, at 272.
[190] *Id.*

$750 per violation, the maximum penalty would be $750 million, whereas if the Attorney General of California decides to sue the entity, the maximum penalty would be $7.5 billion.[191] Thus, it is readily apparent that the maximum penalties under the CCPA could be beyond the financial reach of many organizations.[192]

Palmieri employed a three-prong analysis framework when analyzing the effectiveness of the CCPA.[193] First, the data stewardship prong examines a company's personal information collection process.[194] In this first element, Palmieri opined that although an individual is at the center of the decision-making process regarding collecting, storing, using, and disseminating their personal information, consumers are rarely aware of the nature of the data being collected or how that data will be used.[195] Another issue with this first prong is that many websites use a *take-it-or-leave-it* approach when an individual is given a choice whether to accept or reject a firm's collection of their personal information.[196] In the initial version of the CCPA, the consent mechanism was not nuanced, reflecting the consent process' myriad variations.[197]

The second prong of Palmieri's analysis dealt with a government's balancing of the harms between alienating an individual versus a business when an entity collects personal information on the person.[198] The issue is what weight the State of California should be given to each possible harm.[199] One factor to consider is the industry being examined when safeguards are present to prevent or regulate cross-industry sharing of data.[200] According to Palmieri, the CCPA volunteers no guidance to entities contemplating whether a specific processing activity is worth the risk.[201] The third and final prong of Palmieri's analysis is the element of redressability, meaning that there are sufficient procedures and precautions to ensure that California consumers have access to their personal information and can respond

---

[191] Cohen et al., *supra* note 181, at 6.
[192] Buresh, *supra* note 118, at 273.
[193] Nicholas F. Palmieri, *Who Should Regulate Data? An Analysis of the California Consumer Privacy Act and Its Effects on Nationwide Data Protection Laws*, 11 HASTINGS SCI. AND TECH. L. J. 37, 40 (2020).
[194] *Id.*
[195] *Id.* at 41.
[196] *Id.* at 41-42.
[197] *Id.* at 42.
[198] Palmieri, *supra* note 192, at 40-41.
[199] *Id.* at 45.
[200] *Id.* at 44.
[201] *Id.* at 45.

to improper uses of that data.[202] According to Palmieri, the CCPA excels at providing transparency to consumers.[203] Palmieri aptly pointed out that the deletion of personal information is not the only mechanism available.[204] Still, the opt-out choice also ensures that an individual's personal information is not collected.[205] In other words, data that are never collected in the first place can never be wrong.

For these and other limitations of the CCPA, in the November 2020 election, California residents amended the California Consumer Privacy Act in passing the California Privacy Rights Act.

B. California Privacy Rights Act

In the November 2020 election, the citizens of California passed Proposition 24, also known as the California Privacy Rights Act (CPRA), by 56 percent.[206] With the passage of the CPRA, California citizens now have the right to correct inaccurate information, the right to have their personal information that is collected be subordinate to data minimization and purpose limitations, and the right to receive a notice from businesses planning on employing sensitive personal information, along with the right to request that such an organization stop using that information.[207] The CPRA expanded the right to access information regardless of when it was collected unless it is impossible or impracticable, the right to opt-out of sharing information with third parties regardless of whether an individual is a buyer or a seller, and the right to sue a business when the entity exposes user names and passwords.[208] The CPRA is scheduled to take effect on January 1, 2023.[209]

---

[202] *Id.* at 46.
[203] *Id.*
[204] *Id.* at 47.
[205] *Id.*
[206] *California Privacy Rights Act: An Overview*, PRIVACY RIGHTS CLEARINGHOUSE (December 10, 2020), https://privacyrights.org/resources/california-privacy-rights-act-overview#:~:text=The%20California%20Privacy%20Rights%20Act%20clarifies%20that%20people%20can%20opt,personal%20information%20to%20third%20parties.&text=The%20California%20Privacy%20Rights%20Act%20expands%20this%20to%20cover%20data,includes%20a%20username%20and%20password.
[207] *Id.*
[208] *Id.*
[209] *Id.*

The CPRA consists of a fair number of enhancements to the CCPA.[210] The CPRA changed the threshold for the number of consumers or households to 100,000 and now applies to businesses that receive 50 percent or more of their annual revenue from selling or sharing consumer personal information.[211] The CPRA gives California consumers the right to opt-out of automated decision-making technology associated with a consumer's economic situation, health and personal preferences, location or movements, and work performance while strengthening the opt-out rights for minors.[212] The CPRA introduced the notion of *sensitive personal information*, such as *biometric or health information*, the content of non-public information (i.e., email and text messages), ethnicity, *genetic data*, race, religious or philosophical beliefs, sex life or sexual orientation information, and union membership, where sensitive personal information now possesses stringent consent, disclosure, opt-out requirements, and purpose limitation requirements.[213]

Under the CPRA, consumers have the right, subject to some exceptions, to demand the deletion of any consumer personal information purchase or sold.[214] Suppose consumer personal information is inaccurate. With the passage of the CPRA, California consumers now have the right to correct erroneous information along with the right to restrict the use and disclosure of sensitive personal information.[215] The CPRA distinguishes between requests for specific information from requests for general personal information. Under the CPRA, consumers have the right to access meaningful information regarding the decision-making logic used in collecting, using, storing, disseminating information, and describing the likely outcomes of the process.[216] Under the CPRA, consumers may request the business transmit specific personal information, when technically feasible, to third parties.[217] The CPRA requires a company to perform an annual

---

[210] *CPRA vs. CCPA vs. GDPR: How the Difference Impacts Your Data Privacy Operations*, WIREWHEEL, INC., 2 (2020), https://wirewheel.io/resources/cpra-ccpa-gdpr-impact-on-data-privacy-operations/.
[211] *Id.*
[212] *Id.* at 3.
[213] *Id.* at 4.
[214] *Id.* at 5.
[215] *Id.*
[216] *Id.* at 6.
[217] *Id.* at 7.

cybersecurity audit and submit a personal information processing risk assessment to the California Privacy Protection Agency.[218]

The CPRA places limits on the collection, storage, use, and retention of personal information that is reasonably necessary and proportionate to achieve the desired end of collecting the personal information in the first place.[219] The CPRA increased the fine to $7,500 per violation involving individuals under 16 years of age.[220] There is no longer a 30-day cure period following notice of a breach.[221] Finally, the CPRA expanded the scope of a consumer privacy right of action so that violations of email accounts are now covered.[222] Thus, the CCPA, together with the CPRA, is currently looking a lot like the GDPR in terms of enforcement, opt-in and opt-out restrictions, scope, the meaning of personal information, and the rights of access, correction, deletion, disclosure, erasure, as well as portability, penalties, and verification.[223]

C. Nevada's Privacy Law

On May 29, 2019, the Nevada Senate approved Senate Bill (SB-220), which amended Nevada's existing privacy law from 2017 or NRS 603A.300 – 603A.360 and became effective on October 1, 2019.[224] SB-220 gave consumers the right to opt out to sell their personal information.[225]

The Nevada privacy law concerns "operators" who are defined as any person that meets the following criteria: (1) owns and operates a website or online service as a business, (2) collects and maintains personal information from consumers who reside in Nevada and who access the website or online service, and (3) focuses its activities on Nevada, conducts a transaction in Nevada, or purposefully avails itself of performing its activities in Nevada.[226] In terms of the Nevada privacy

---

[218] *Id.* at 8.
[219] *Id.*
[220] *Id.* at 9.
[221] *Id.*
[222] *Id.*
[223] *See id*.
[224] OneTrust, *The Nevada Privacy Law (SB-220) vs. The California Consumer Privacy Act (CCPA)*, ONETRUST, (Sept. 17, 2019), https://www.onetrust.com/blog/the-nevada-privacy-law-sb-220-vs-the-california-consumer-privacy-act-ccpa/.
[225] *Id.*
[226] Hans Skillrud, & Donata K. Stroink-Skillrud, *Nevada Privacy Law Compliance Guide.* TERMAGEDDON.COM, (May 22, 2020), https://termageddon.com/nevada-revised-statutes-chapter-603a/.

law, personal information consists of a person's first and last name, social security number, driver's license number or identification card number, account number, credit card number, debit card number, or any other identifier that permits an individual to be contacted either physically or online.[227]

The Nevada privacy law applies to persons that (1) advertise their products or services in Nevada, (2) ship their products or services to Nevada, or (3) sell their products or services to Nevada citizens.[228] The Nevada privacy law does not apply if (1) a person or entity is located in Nevada, (2) the revenue of the person or entity primarily comes from a source other than selling goods or services on its website or online service, and (3) the website or online service has less than 20,000 unique visitors per year.[229]

Companies that satisfy the Nevada privacy law must create and maintain an expressed privacy policy document that (1) categorizes the personal information that is collected and the third parties to whom such information is shared, (2) describes the process, if it exists, for a user to be notified and to review and request changes to the collected personal information, (3) informs a user whether a third party is collecting personal information through different websites, (4) lists the effective date of the privacy policy.[230] SB-220 requires a person or an entity to create a designated request address, either a physical address, email address, toll-free telephone number, or website where an individual can submit a request.[231] This information must be published on the website's privacy policy statement, and a person or entity must respond to the request within 60 days of receiving the request.[232] The penalty for non-compliance is at most $5,000 per violation.[233] According to Jordan, although SB-220 covers a wide range of information, the scope of Nevada's privacy law is much narrower than the GDPR and the CCPA.[234] SB-220 does provide consumers with the right to request that their personal information not be sold to third parties.[235]

---

[227] *Id.*
[228] *See generally id.*
[229] *Id.*
[230] *Id.*
[231] *Id.*
[232] *Id.*
[233] *Id.*
[234] Zaniah Jordan, *The Effect of the European Union (EU) General Data Protection Regulation (GDPR) on the Gaming Industry*, 10 UNLV GAMING L.J., 260, 274 (2020), https://scholars.law.unlv.edu/glj/vol10/iss2/6.
[235] *Id.*

D. Maine's Act to Protect the Privacy of Online Customer Information

On July 1, 2020, Maine became the next state to regulate online data.[236] Like the Nevada privacy law, the Maine privacy law is not a comprehensive privacy law like the CCPA.[237] However, in contrast to the California and Nevada privacy laws, the Maine law focuses exclusively on data collected by Internet Service Providers (ISPs).[238] The Maine law prevents ISPs from disclosing, selling, or permitting access to customer personal information.[239] According to the Maine privacy law, customers include applicants for service, current subscribers, and former subscribers of ISPs.[240] The law protects a customer's name, address, social security number, billing address, and demographic data.[241] It also safeguards web browsing history, application use history, precise geolocation data, financial data, health data, information on the customer's children, the customer's device identifiers, the content of customer communications, and origin and destination IP addresses.[242] An ISP may use, disclose, sell, or allow access to personal information only if a customer consents.[243] A consumer may withdraw their consent at any time.[244]

An ISP is not permitted to refuse service to a customer when the customer does not consent, charge a customer for not providing consent, or give a customer a discount for consenting.[245] As for information that is not personal information, an ISP may use, disclose, sell, or allow access, provided that a customer does not give written notice to the ISP that they do not agree to such actions.[246] Even so, an ISP may collect, retain, use, disclose, sell, or allow access to customer information to provide Internet service, to advertise or market services, to comply with a legal court order, to bill and collect payment, to protect customers from fraud and other abuses, and to provide

---

[236] Barry Levine, *What's the Impact of Maine's New Privacy Law?*, RAMPUP (Dec. 17, 2019), https://rampedup.us/maine-privacy-law-impact/.
[237] *See generally* Donata Kaleneaite, *Maine Privacy Law Guide*, TERMAGEDDON.COM (2019), https://iapp.org/media/pdf/resource_center/MainePrivacyLawGuide.pdf.
[238] Levine, supra, note 235.
[239] *Id.*
[240] Kaleneaite, *supra*, note 236.
[241] *Id.*
[242] *Id.*
[243] *Id.*
[244] *Id.*
[245] *Id.*
[246] *Id.*

geolocation data in an emergency to law enforcement, a customer's legal guardian or family member, or for assisting in an emergency response.[247]

E. Virginia's Consumer Data Protection Act

On March 2, 2021, Governor Ralph Northam signed the Virginia Consumer Data Protection Act (CDPA) into law.[248] According to Horner, the CDPA establishes a framework for controlling and processing personal data in Virginia.[249] The law applies to all persons that conduct business in the state, and either (1) control or process personal data of at least 100,000 consumers or (2) obtain over 50 percent of gross revenue from the sale of personal data and control or process personal data of more than 25,000 consumers.[250] The law does not apply to state or local government entities and possesses exceptions for specific types of data or information that are governed by federal law.[251] The law gives consumers the rights to access, correct, delete, and copy personal data.[252] Under Virginia law, a consumer has the right to opt-out of the processing of personal data for targeted advertising, the sale of personal data, or the profiling of the consumer and the right to appeal the decision of an entity's data controller.[253] The CDPA states that the Virginia Attorney General possesses the exclusive authority to enforce any violations of the law.[254] The CDPA established the Virginia Joint Commission on Technology and Science (VJCTS) to support the Virginia Attorney General's efforts.[255] The Virginia legislature charged the VJCTS with reviewing the act's provisions,.[256] The effective date of the CDPA is January 1, 2023.[257]

According to Rippy, the scope of the CDPA is controlled by the definitions of the terms "consumer," "sale of personal information,"

---

[247] *Id.*
[248] Sarah Rippy, *Virginia Passes the Consumer Data Protection Act*, INT'L. ASS'N. OF PRIV. PROF., (Mar. 3, 2021), https://iapp.org/news/a/virginia-passes-the-consumer-data-protection-act/.
[249] Rick Horner, *Gov. Northam Signs Data Protection Law*, FAIRFAX COUNTY TIMES, (Mar. 19, 2021), http://www.fairfaxtimes.com/articles/gov-northam-signs-data-protection-law/article_54a4dc38-8809-11eb-ac65-ab6d12c38118.html.
[250] *Id.*
[251] *Id.*
[252] *Id.*
[253] *Id.; see also* Rippy, *supra* note 247.
[254] Horner, *supra* note 248.
[255] *Id.*
[256] *Id.*
[257] *Id.*

and "monetary and other valuable consideration."[258] According to the CDPA, a consumer is a natural person that resides in Virginia that acts as an individual or in the context of a household.[259] In contrast to the CCPA, the CDPA does not include employee data that may be collected by businesses.[260] The CDPA defines valuable consideration strictly as money exchanged when data is sold with the following exceptions: (1) disclosures to processors, (2) disclosures to third parties where a consumer requested a product or service, (3) disclosures to an affiliate of a controller, (4) unrestricted disclosures by consumers to the public via mass media, and (5) disclosures due to mergers, acquisitions, etc.[261] The entity exemptions include (1) a Virginia agency, board, bureau, commission, district, or political subdivision, (2) a financial institution that is subject to the Gramm-Leach-Bliley Act, (3) an entity subject to the Health Insurance Portability and Accountability Act and the Health Information Technology for Economic and Clinical Health Act, (4) a nonprofit organization, and (5) an institution of higher learning such as a college or university.[262] Much like the GDPR and the CCPA, the CDPA has provisions that limit the collection and use of data, mandates technical safeguards, and require data protection assessments, data processing agreements, and a privacy policy.[263]

Unfortunately, the CDPA has specified neither a time requirement regarding disclosures of personal information to a consumer nor the format used in disclosing personal information to a consumer.[264] The CDPA does not provide for a private right of action.[265] Even so, when the Virginia Attorney General chooses to take legal action against an entity, the entity's data controller has 30 days to either cure the violation and provide the Attorney General with a written statement that the breach has been fixed.[266] If an entity selects not to cure a violation, the Virginia Attorney General may fine the entity up to $7,500 per violation.[267]

---

[258] Rippy, *supra* note 247.
[259] *Id.*
[260] *Id.*
[261] *Id.*
[262] *Id.*
[263] *Id.*
[264] *Id.*
[265] *Id.*
[266] *Id.*
[267] *Id.*

F. Colorado's Privacy Act

On July 8, 2021, the Colorado Privacy Act (CPA) officially became law.[268] According to Rippy, the CPA is similar to the CCPA and the CDPA but with some distinct differences.[269] The CPA pertains to any controller that conducts business in Colorado, produces products or services for Colorado residents, controls data for at least 100,000 customers annually, or obtains revenue or a discount on the price of goods or services from selling personal customer data.[270] According to the CPA, there are no revenue minimums, but the law does concern companies that process the personal information of 25,000 or more customers and gets revenue or a discount from the sale of that data.[271] Also, the CPA defined a consumer as a Colorado resident that acts as an individual or in the context of a household but omitted peopled acting in a commercial or employment context such as a job applicant.[272]

The CPA defines a sale of personal information as an exchange of personal data for money or other valuable consideration.[273] However, a sale does not include the (1) disclosure of personal data to a processor that processes personal data for the processor, (2) disclosure of personal data to a third party for delivering a product or service that a consumer asks for, (3) disclosure or transfer of personal data to a controller's affiliate, (4) disclosure or transfer of personal data that is part of a merger or bankruptcy, or (5) disclosure of personal data where the controller is directed by the consumer to make the personal data available to a third party or the general public.[274]

The CPA excuses the entity-level exemptions and data-level exemptions.[275] For example, an entity-level exemption would consist of entities that are subject to the Gramm-Leach-Bliley Act, but did not fully exempt entities that are covered by the Health Insurance Portability and Accountability Act (HIPPA).[276] Furthermore, under the CPA, the six primary consumer rights include the right of access, the right to correct data inaccuracies, the right to delete personal data, the right to obtain personal information in a portable format, the right to

---

[268] Sarah Rippy, *Colorado Privacy Act Becomes Law*, THE PRIVACY ADVISER (Jul. 8, 2021), https://iapp.org/news/a/colorado-privacy-act-becomes-law/.
[269] *Id.*
[270] *Id.*
[271] *Id.*
[272] *Id.*
[273] Colorado Privacy Act, Colo. Rev. Stat. 6-1-1303 (23)(a).
[274] Colo. Rev. Stat. § (23)(b).
[275] Rippy, *supra* note 267.
[276] *Id.*

opt-out of processing of personal customer data, and the right to appeal with a reasonable time when a business denies a customer's request.[277] The law demands that the Colorado attorney general establish technical standards before July 1, 2023.[278]

A data controller has the duty (1) to expressly specify why personal information is being collected, (20 to avoid the secondary use of personal data, (3) of care that is appropriate to the volume, scope, and nature of the personal information being collected, (4) to avoid unlawful discrimination, (5) to avert processing sensitive data without customer consent, (6) to assess whether a data processing activity presents a heightened risk of harm to a consumer; and (7) to require that a processor be governed by a contract between a controller and a processor.[279] Unlike the other privacy acts discussed above, the CPA gave the attorney general and district attorneys the authority to enforce the Colorado privacy law.[280] Once legal action is initiated, a controller has 60 to cure a violation, which is twice the time allotted by the California and Virginia cure period.[281] The 60-day cure period will cease beginning January 1, 2025.[282] There are no penalties in the CPA because a violation of the law is considered to be deceptive trade practice, where the Colorado Consumer Protection Act ensures that the maximum is $20,000 per violation.[283]

G. Status of Privacy Bills in the Several States

As one can see from the discussion above, there are as of this writing five states, California, Nevada, Maine, Virginia, and Colorado, that have passed privacy laws. According to Rippy, six states are currently in the process of legislating privacy laws.[284] Also, sixteen states have had privacy bills that failed to be passed by their respective legislatures.[285] By implication, as of September 1, 2021, the legislatures of 23 states are not currently considering a privacy bill. This information implies that privacy legislation may be quickly becoming a serious issue in the United States.

---

[277] *Id.*
[278] *Id.*
[279] *Id.*
[280] *Id.*
[281] *Id.*
[282] *Id.*
[283] *Id.*
[284] Sarah Rippy, *US State Comprehensive Law Comparison*, INT'L. ASS'N. OF PRIV. PROF., (as of Sep. 1, 2021), https://iapp.org/resources/article/state-comparison-table/.
[285] *Id.*

IV. BIOMETRIC PRIVACY LAWS IN THE SEVERAL STATES

In this section of this essay, Illinois' Biometric Information Privacy Act, Texas' Capture or Use of Biometric Identifier Act, and Washington's Biometric Identifiers Act will be discussed in turn. The states with minor changes in existing law to accommodate the protection of biometric identifiers and states where biometric privacy bills are under legislative review will also be examined.

A. Illinois' Biometric Information Privacy Act

In 2008, the Biometric Information Privacy Act became law in the State of Illinois. It was a comprehensive law that more or less laid dormant until the Illinois Supreme Court opined in *Rosenbach*.[286] An example of a case involving BIPA before *Rosenbach* is *Rivera*. The Court held that Google's retention of unique face templates did not cause the type of concrete injury to individuals required to establish standing.[287] The Court observed that Google, Inc.'s creation, without consent, of unique face templates did not cause a concrete injury as required for standing.[288] Thus, there was no BIPA violation.

With the Illinois Supreme Court's decision in *Rosenbach*, a proliferation of cases occurred.[289] *Rosenbach* originated when a fourteen-year-old boy, Alexander Rosenbach, went on a field trip to Six Flags Great America in Gurnee, Illinois.[290] His mother, Stacy Rosenbach, purchased a ticket for her son online.[291] When entering Six Flags, Alexander was required to scan his thumbprint to verify his identity and activate his season pass.[292] Alexander did not receive any paperwork describing either the reasons for why the thumbprint scan was taken or how the biometric data would be stored, used, or disseminated.[293] When Alexander returned home, he told his mother about the scan print.[294] Six Flags did not send Alexander or his mother

---

[286] Rosenbach v. Six Flags Entertainment Corp., 129 N.E.3d 1197 (Ill. 2019); *see also* Chloe Stepney, *Actual Harm Means It Is Too Late: How Rosenbach v. Six Flags Demonstrates Effective Biometric Information Privacy Law*, 40 LOY. LOS ANGELES ENT. L. REV. 51 (2019).
[287] Rivera v. Google, Inc., 366 F. Supp. 3d 998 (N.D. Ill. 2018).
[288] *Id.* at 1010.
[289] Charles N. Insler, *Understanding the Biometric Information Privacy Act Litigation Explosion*, 106 ILL. B. J. 34, 49 (2018).
[290] *Rosenbach*, 129 N.E.3d at 1200.
[291] *Id.*
[292] *Id.*
[293] *Id.*
[294] *Id.*

a consent form regarding taking a scan of Alexander's thumbprint.[295] Six Flags did not reveal its policy regarding its biometric information storage policies to the plaintiffs.[296]

In *Rosenbach*, the Court reversed the appellate court's ruling, finding a technical violation of BIPA. There was no showing of actual damages in the lower court that gave rise to a cause of action.[297] However, the Court employed the statute's plain meaning to opine that a plaintiff's standing under BIPA is not controlled by actual harm but rather by an invasion and infringement of a statutory right, which in turn gave rise to the cause of action.[298] The decision of the Court was unanimous.[299]

Rosenbach resulted in an increase in biometric litigation in Illinois.[300] In *Rogers,* the plaintiffs were an "aggrieved person" within the meaning of BIPA.[301] The plaintiffs adequately stated a claim for violations of the Illinois law.[302] However, the plaintiffs failed to allege that the defendant's actions were intentional and reckless, as required for heightened damages.[303] In *Namuwonge*, the plaintiffs sufficiently alleged that Kronos, Inc. possessed fingerprint data collected by the company within the meaning of BIPA.[304] The plaintiffs stated a claim against Kronos for the violation of BIPA that required Kronos to develop a written policy when in possession of biometric identifiers.[305] The plaintiffs did not state a claim against Kronos for a violation of BIPA, which limited transfers of biometric information.[306] The plaintiffs did not state a claim against Kronos, Inc. for a violation of BIPA that required a company collecting or capturing a person's biometric information to inform the individual in writing.[307] Finally,

---

[295] *Rosenbach*, 129 N.E.3d at 1200.
[296] *Id.*
[297] *Id.* at 1202.
[298] *Id.* at 1206.
[299] *Id.* at 1207.
[300] Chloe Stepney, *Actual Harm Means It Is too Late: How Rosenbach v. Six Flags Demonstrates Effective Biometric Information Privacy Law*, 40 LOYOLA OF LOS ANGELES ENT. L. REV. 1 61, (Dec. 4, 2019), *available at* https://digitalcommons.lmu.edu/cgi/viewcontent.cgi?article=1630&context=elr.
[301] Rogers v. CSX Intermodal Terminals, Inc., 409 F. Supp. 3d 612, 617 (N.D. Ill. 2019).
[302] *Id.*
[303] *Id.* at 619.
[304] Namuwonge v. Kronos, Inc., 418 F. Supp. 3d 279, 284 (N.D. Ill. 2019).
[305] *Id.*
[306] *Id.* at 284-85.
[307] *Id.* at 286.

the plaintiffs' abstract statements regarding damages were insufficient for the federal district court to infer that the company acted recklessly or intentionally.[308]

In *Bryant*, the Seventh Circuit ruled that the collection of customer fingerprints without first obtaining written consent, which BIPA required, was an injury that was sufficient to satisfy the injury-in-fact requirement for standing.[309] According to the Court, the failure to disclose a written retention schedule and destruction guidelines publicly violated BIPA, whereas no injury was sufficient to confer standing before collecting fingerprints.[310]

In *Snider*, Snider had the standing to bring BIPA claims for Heartland Beef's failure to inform and failure to obtain written consent.[311] However, Snider lacked standing to assert a claim that Heartland Beef was unable to create and publicize its policy regarding retention and destruction of its biometric identifiers defense.[312] The Illinois Workers' Compensation Act did not preempt Snider's BIPA claims because Snider pled a plausible BIPA claim against the Heartland Beef defense.[313] Finally, Snider sufficiently alleged Heartland Beef's negligence, where an implied assumption of risk was not an applicable defense.[314] In *Campbell*, the Ninth Circuit opined that the plaintiffs in the class-action suit had sufficiently alleged concrete injury-in-fact to satisfy standing.[315] The federal district court did not abuse its discretion when it determined that class certification's predominant requirement was met.[316] Finally, the federal district court did not abuse its discretion when it opined that class certification's superiority requirement was met.[317]

In *Fox*, the Seventh Circuit held that the federal district court's remand order back to state court was appealable.[318] Dakkota Integrated Systems' alleged violation of BIPA was an injury-in-fact that

---

[308] *Id.*
[309] Bryant v. Compass Grp. USA, Inc., 958 F.3d 617, 619 (7th Cir. 2020), as amended on denial of reh'g en banc (June 30, 2020).
[310] *Id.* at 626.
[311] Snider v. Heartland Beef, Inc., 479 F. Supp. 3d 762, 767 (C.D. Ill. 2020).
[312] *Id.*
[313] *Id.* at 770.
[314] *Id.* at 771.
[315] Campbell v. Facebook, Inc., 951 F.3d 1106, 1116 (9th Cir. 2020).
[316] *Id.* at 1127.
[317] *Id.*
[318] Fox v. Dakkota Integrated Systems, LLC, 980 F.3d 1146, 1151 (7th Cir. 2020).

supported Fox's claim for standing under Article III.[319] The alleged violation consisted of failing to develop, publicly disclose, and comply with a data-retention schedule and guidelines for the permanent destruction of biometric data after the initial purpose for collection ended.[320]

In *Figueroa*, the plaintiffs sufficiently alleged a concrete informational injury to confer Article III standing.[321] Kronos was obliged to obtain a written release from its employees before acquiring biometric data.[322] The plaintiffs claimed that Kronos violated the BIPA section that required private organizations who obtained biometric data to inform its employees that the company was collecting biometric data without receiving a written release.[323] The Court noted that Kronos disseminated employee biometric data without the plaintiffs' knowledge or consent.[324] The plaintiffs adequately alleged negligence required to state a claim for statutory damages under BIPA.[325] Finally, potential fact questions concerning various timekeeping practices of Kronos did not warrant striking the class allegations at the pleading stage.[326] It was premature at the pleading stage to strike class allegations based on the vendor's claim that named plaintiffs were inadequate class representatives.[327]

In *Cothron*, the plaintiffs' alleged injury was caused by White Castle's violation of BIPA, which requires an organization, before collecting biometric data, to inform an employee in writing that the information is being collected or stored.[328] The organization must also state the specific purpose and length of term for collecting, storing, and using the data.[329] An employer must receive a written release from the individual.[330] In other words, the plaintiffs had Article III standing.[331] The plaintiffs did not allege a violation or suffer an injury under BIPA that required the defendant that possessed the biometric data to delete

---

[319] *Id.*
[320] *Id.* at 1154.
[321] Figueroa v. Kronos, Inc., 454 F. Supp. 3d 772, 781 (N.D. Illl. 2020).
[322] *Id.* at 783.
[323] *Id.*
[324] *Id.* at 785.
[325] *Id.* at 786.
[326] *Id.* at 789
[327] Figueroa, 454 F. Supp. 3d at 782.
[328] Cothron v. White Castle Sys., Inc., 476 F. Supp. 3d 604, 611 (N.D. Ill. 2020).
[329] *Id.* at 610.
[330] *Id.*
[331] *Id.* at 613.

that data as soon as the purpose of the collection was satisfied or within three years after the last interaction with the relevant person.[332] This meant that the plaintiffs did not have Article III standing to bring a claim based on this provision of BIPA.[333]

The plaintiffs' alleged injury, which was caused by the defendant's violation of a provision of BIPA that states that an organization in possession of biometric data may only disclose or otherwise disseminate an individual's data on obtaining the person's consent or in limited other circumstances, was concrete and particularized.[334] This means that the plaintiffs possess Article III standing to sue for such alleged violation.[335] The consent form that the plaintiffs signed did not equitably estop the plaintiffs, under Illinois law, from bringing this action.[336] The plaintiffs' failure to specifically allege the defendant's mental state did not require dismissal.[337] It did not matter the time at which consent was statutorily required under the provision of BIPA, which states that an organization that possesses biometric data may only disclose or otherwise disseminate a person's data upon obtaining the person's consent or in limited other circumstances.[338] The plaintiffs pleaded information that triggered his or her suspicion of disseminating their biometric data without consent.[339] Thus, the plaintiffs stated a plausible claim, even though some of the allegations were alleged upon information and belief.[340]

In *Sherman*, the plaintiffs alleged a concrete injury sufficient to establish Article III standing because Brandt Industries failed to institute, maintain, and adhere to a publicly available retention schedule and failed to obtain informed written consent before collecting biometric information.[341] The plaintiffs could seek liquidated damages under BIPA.[342] The Illinois Workers' Compensation Act did not preempt the plaintiffs' suit.[343]

---

[332] *Id.* at 612.
[333] *Id.* at 613.
[334] *Cothron* 476 F. Supp. 3d at 612.
[335] *Id.* at 613.
[336] *Id.* at 614.
[337] *Id.* at 615.
[338] *Id.* at 617.
[339] *Id.* at 618.
[340] *Cothron*, 476 F. Supp. 3d at 618.
[341] Sherman v. Brandt Indus. USA Ltd., No. 20-CV-1185 (C. D. Ill. Peoria Div. Nov. 12, 2020).
[342] *Id.*
[343] *Id.*

Finally, in *Thornley*, the defendant collected Thornley's biometric data via photographs and metadata that were procured using social media websites such as Facebook, Venmo, and YouTube.[344] Clearview proceeded to compile the biometric data and then sold it to third parties.[345] Thornley contended that Clearview violated Section 15(c) of BIPA, prohibiting private organizations from selling, leasing, trading, or profiting from an individual's biometric identifiers.[346] The Seventh Circuit opined that Thornley did not experience an Article III injury from the sale of his biometric data.[347] The Court concluded that by ensuring that the supply of biometric identifiers is illegal, Section 15(c) prevented a market for biometric identifiers from existing.[348] The Court likened Section 15(c) to Section 15(a), which prohibited entities from collecting biometric identifiers without issuing data retention and destruction policies.[349] In other words, a defendant owed a duty to the public-at-large rather than to an individual plaintiff, absent a positive allegation of a specific injury.[350]

B. Texas' Capture or Use of Biometric Identifier Act

In 2009, one year after BIPA was passed, the Texas legislature passed Chapter 503 of Title 11, Subtitle A as amended, the Texas biometric privacy law, also known as the Capture or Use of Biometric Identifier (CUBI) Act.[351] The law is approximately one and one-half pages long.[352] The law protects the confidentiality of biometric identifiers by restricting their collection, sale, lease, or disclosure but does not contain a broader definition of biometric information.[353]

---

[344] Thornley v. Clearview AI, Inc., 984 F.3d 1241, 1242-43 (7th Cir. 2021).
[345] *Id.* at 1243.
[346] *Id.* at 1246.
[347] *Id.* at 1249.
[348] *Id.* at 1247.
[349] *Id.*
[350] *Thornley*, 984 F.3d at 1247.
[351] Capture or Use of Biometric Identifier Act, Tex. Bus. & Com. Code §503.001 (2009), https://statutes.capitol.texas.gov/Docs/BC/htm/BC.503.htm.
[352] *See generally id.*
[353] David E. Keltner, *§ 3:162. Federal Wiretap Law and Electronic Communications—Telephone Conversations—Employee Email, Voice Mail Compared*, TEXAS PRACTICE GUIDE: DISCOVERY (2020 ED.), (Apr. 2020), https://1.next.westlaw.com/Document/If936e411b1a311d99ff5ef8e306d2857/View/FullText.html; *see also,* John G. Browning, *The Battle over Biometrics*, TEXAS BAR J., 674, 676 (2018), https://www.texasbar.com/AM/Template.cfm?ection=Content_Folders&ContentID=42128&Template=/CM/ContentDisplay.cfm.

According to Section 503.001, a biometric identifier means a retina or iris scan, fingerprint, voiceprint, or a record of the geometry of a face or hand.[354] The Texas law does not cover a voiceprint if a financial institution or an affiliate retains it because 15 U.S.C. Section 6809 defines those terms.[355] CUBI does not require a written release, but does demand that firms destroy data that are no longer needed, and compels businesses to destroy that data "no later than the first anniversary of the data the purpose for collecting the identifier expires, except as provided by Subsection (c-1)".[356] CUBI does not permit a private cause of action but only allows the Texas Attorney General to begin legal proceedings.[357]

C. Washington's Biometric Identifiers Act

On July 23, 2017, Washington became the third state to pass a biometric privacy law called the Biometric Identifiers Act (BIA).[358] Under the Washington law, a biometric identifier is similar to the Texas definition of a biometric identifier, but BIA does not possess an express definition of biometric information.[359] In contrast to BIPA and CUBI, the Washington law does have a security clause where biometric identifiers may be collected for 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."[360]

Like Texas, the BIA does not require that consent be in writing, nor does the law create a private cause of action, but only permits the Washington Attorney General to instigate legal proceedings.[361] Finally, the Washington biometric privacy law does allow businesses to sell biometric identifiers except under seven specific circumstances that, under a careful reading, appear to subsume the rule.[362]

---

[354] Capture or Use of Biometric Identifier Act §503.001; *see also* Keltner, *supra* note 352.
[355] Capture or Use of Biometric Identifier Act §503.001.
[356] *Id.*
[357] *See* Browning, *supra* note 352, at 676.
[358] *Id.*
[359] *Id.*; *see also* Biometric Identifiers Act, RCW § 19.375.010 (2017).
[360] Biometric Identifiers Act § 19.375.010(8).
[361] Biometric Identifiers Act § 19.375.040; *see also* Browning, *supra* note 352.
[362] Biometric Identifiers Act § 19.375.020.

D. Amendments to Existing Arkansas and New York State Laws

Zych and his colleagues wrote that on August 9, 2019, Arkansas amended its definition of the personal information contained in its data breach response law to encompass biometric data, such as voiceprint, handprint, fingerprint, DNA, a retina or iris scan, hand geometry, faceprint, or another unique biological characteristic.[363] Accordingly, Arkansas businesses that acquire, own, or license personal information are now required to implement and maintain "reasonable and appropriate security practices to protect data from unauthorized access or disclosure."[364] In February 2020, the State of New York revised its definition of personal information in its Stop Hacks and Improve Electronic Data Security Act to include biometric data that may be employed to authenticate or ascertain a person's identity.[365]

E. Pending Biometric Privacy Bills in New York and Maryland

According to Lust and his colleagues, on January 6, 2021, the first day of the New York legislature's 2021 session, New York state representatives proposed Assembly Bill 27 (AB 27), the New York Biometric Privacy Act.[366]They reported that the bill's purpose is to ensure that companies have a written biometric retention policy.[367] The bill would require that non-governmental organizations with biometric information generate a written retention policy that specifies the initial purpose of acquiring personal information and when this purpose has been satisfied.[368] According to the New York bill, a private entity must destroy that biometric information within three years of last interacting with an individual.[369]

---

[363] Thomas F. Zych, Steven G. Stransky, & Brian Doyle-Wegner, *State Biometric Privacy Legislation: What You Need to Know*, THOMPSON HINE (Sept. 5, 2019), https://www.thompsonhine.com/publications/state-biometric-privacy-legislation-what-you-need-to-know.
[364] *Id.*
[365] *Id.*
[366] Karen Lee Lust, Michael Galibois, & Jacqueline Lefebvre, *New York Proposes a New Biometric Privacy Act*, TECHNOLOGY LAW DISPATCH (Jan. 21, 2021), https://www.technologylawdispatch.com/2021/01/privacy-data-protection/new-york-proposes-a-new-biometric-privacy-act/.
[367] *Id.*
[368] *Id.*
[369] *Id.*

Shortly after New York state representatives proposed Assembly Bill 27 (AB 27), Maryland introduced House Bill 218, a bill that seemingly cloned the Illinois Biometric Privacy Act.[370] Like Illinois' BIPA, the Maryland bill assures that individuals have a private right of action, statutory penalties and that plaintiffs can recover attorney fees when the litigation is successful.[371] Given the tidal wave of class action suits in Illinois, the modeling of Maryland's biometric bill on Illinois' BIPA demonstrates that Maryland employers must scrutinize biometric technology and litigation to avoid possible class action suits in the future.[372]

The Maryland bill title is entitled "Commercial Law – Consumer Protection – Biometric Identifiers and Biometric Information Privacy."[373] The Maryland bill forbids private organizations from capturing, collecting, or storing an individual's biometric information without first having a biometric policy document and acquiring written consent, implements standards of care, and prohibits biometric information disclosure without consent.[374] Under the Maryland bill, the available remedies are similar to the remedies contained in Illinois' BIPA.[375] An individual can recover $1,000 for each negligent violation and $5,00 for each intentional or reckless violation, including reasonable attorneys' fees and costs.[376]

The difference between Illinois' BIPA and the Maryland bill is that biometric identifiers under the Maryland law extend to data about an individual that is created by automatic measurements of that person's biological characteristics, including fingerprints, genetic print, iris, or retina scan, voiceprint, etc.[377] The Maryland bill possesses a broader definition of biometric information.[378] It includes *any information* that can be used to identify an individual, regardless of how it is obtained, converted, stored, or shared.[379] However, under the

---

[370] Thomas Ahlering & Gerald Maatman Jr., *Maryland Joins Growing Number of States Introducing Biometric Information Privacy Bills with Potential to Spur Class Action Litigation*, JDSUPRA, (Feb. 24, 2021), https://www.jdsupra.com/legalnews/maryland-joins-growing-number-of-states-3182422/.
[371] *Id.*
[372] *Id.*
[373] *Id.*
[374] *Id.*
[375] *Id.*
[376] *Id.*
[377] *Id.*
[378] *Id.*
[379] *Id.*

Maryland bill, biometric information does not include any information that is excluded under its definition of a biometric identifier, such as photographs, information captured from a health care setting, operations, payment, or treatment under HIPAA.[380] Finally, under the Maryland bill, a company's policy regarding the retention and destruction of biometric information does not need to see the light of day if the policy applies only to the employees of a private organization and is employed only for internal use.[381] If Maryland passes its biometric privacy bill, it remains to be seen whether Maryland will experience a similar cascade of class action suits like those currently being filed in Illinois.[382]

Finally, based on the experiences of Illinois' BIPA and the New York and Maryland legislators, it can be expected that other states may soon follow the lead of Illinois, New York, and Maryland.

F. Summary of the Literature Reviewed

The first privacy test originated in Justice Harlan's concurrence in *Katz*.[383] The General Data Protection Regulation became law in 2018.[384] It is a comprehensive law that includes biometric privacy. The principal case that tested the EU Directive was *Costeja González*.[385] The CJEU held that Google Spain and Google, Inc. must eradicate links to web pages that are freely accessible worldwide when individuals whose personal information is contained therein demand that the links be removed.[386] For the United States, the California Consumer Privacy Act is a comprehensive privacy law as amended by the California Privacy Rights Act.[387] Several states are creating their versions of the CCPA, much like how the Virginia law was modeled after the CCPA as amended.[388] Currently, there is no comprehensive federal privacy law in the United States.[389]

The first state in the United States to pass a comprehensive biometric privacy law was Illinois.[390] The law was entitled the

---

[380] *Id.*
[381] *Id.*
[382] *Id.*
[383] *See generally* Katz v. United States, 389 U.S. 347 (1967).
[384] Frankenfield, *supra* note 113; *see also* IT Governance Privacy Team, *supra* note 113.
[385] Press Release, No. 70/14 *supra* note 141.
[386] *Id.*
[387] *See generally* Buresh, *supra* note 118.
[388] Rippy, *supra* note 247.
[389] *See generally* Buresh, *supra* note 118.
[390] Stepney, *supra* note 299, at 59.

Biometric Information Privacy Act (BIPA).[391] One of the consequences of BIPA has been a tidal wave of suits because BIPA permits private action rather than limiting actions to be filed only by the Illinois Attorney General.[392] Texas and Washington have their biometric privacy law versions, but the laws in these states are by no means as all-inclusive as the Illinois law.[393] Arkansas and New York recently amended their existing state laws to protect biometric information.[394] Finally, as of this writing, the legislatures of both New York and Maryland are in the process of evaluating their renderings of biometric privacy law.[395]

V. DISCUSSION OF THE FINDINGS

The purpose of this study was to understand and evaluate the privacy and property issues that states confront that are inherent from the use of biometrics to enhance corporate security in their efforts to protect individual privacy. The research examined the historical legal foundations of privacy, focusing on the GDPR, the CCPA as amended by the CPRA, and Illinois' BIPA. The research also discussed the existing privacy and biometric privacy laws by indicating the states where privacy and biometric privacy legislation are under review by various state legislatures. The research addressed the following questions: (1) What are the biometric privacy issues that states face regarding individual and corporate needs for security and privacy?; (2) Why do several states continue to be vulnerable to litigation regarding biometric privacy issues?; (3) How does the State of Illinois address biometric privacy issues in its statutory effort to protect the individuals against organizations that employ biometric cybersecurity procedures?; and (4) How does the Illinois Biometric Information Privacy Act benefit the federal government and other states in their efforts to create and pass biometric privacy laws that protect the privacy rights of their citizens?

The research described the history of privacy, why it is important, and what harms individuals experience when their privacy is violated. The research also described the content of the GDPR and the content of the CCPA as amended by the CPRA. The study outlined Illinois' BIPA, explaining what biometric information is and what it is not. Finally, the essay delineated the privacy and biometric privacy laws in other states and indicated what states were in the process of

---

[391] *Id.*
[392] Insler, *supra* note 288, at 36.
[393] Browning, *supra* note 352, at 676.
[394] Zych et al., *supra* note 362.
[395] Lust et al., *supra* note 365; Ahlering & Maatman Jr., *supra* note 369.

evaluating bills that specifically addressed privacy and biometric privacy.

A. Individual and Corporate Privacy Needs

The fundamental issue that states face regarding individual and corporate needs for security and privacy is how to protect the confidentiality of personal information while ensuring that entities employ their tools appropriately to safeguard corporate tangible and intangible property. In the United States, individuals have a legally recognized reasonable expectation of privacy and specific privacy rights by statute.[396] Companies should be able to buy or sell individual personal information without expressed prior consent. On the other hand, companies need to ensure that their tangible and intangible property is safe from individuals who may misappropriate or misuse corporate assets. Like in *Rosenbach*, firms need to make sure that customers only receive the goods and services they pay for and not for biometric data collection.[397] Once an organization collects personal data, an entity is responsible for ensuring that the personal information is held in privity and not accessible to unauthorized third parties.

B. Vulnerabilities to Litigation

There are several reasons why states are vulnerable to litigation regarding privacy in general and biometric privacy in particular. For states that have not passed privacy or biometric privacy legislation such as the CCPA or Illinois' BIPA, the following four distinct privacy torts described by Prosser are the unreasonable intrusion upon another's seclusion, public disclosure of private facts, false light invasion of privacy, and appropriation of another's name or likeness.[398] These torts are available for litigants whether the privacy issue at hand deals with personal information or biometric information. For the states that have passed privacy or biometric privacy laws, any vulnerabilities to litigation are expressed in the respective statutes. In particular, for Illinois under BIPA, individuals have the legal right to instigate private

---

[396] *See e.g.,* Americans with Disability Act, 42 U.S.C. § 12101 (2021); *see also* Katz v. United States, 389 U.S. 347, 350 (1967).
[397] Rosenbach v. Six Flags Entertainment Corp., 129 N.E.3d 1197, 1206 (Ill. 2019).
[398] Prosser, *supra* note 67, at 389.

action.[399] In contrast, only the Attorneys General of the respective states can sue private entities in Texas and Washington.[400]

C. Protecting Individual Biometric Privacy

Illinois addresses biometric privacy issues in multiple ways. First, BIPA explicitly defines biometric information as physiological characteristics related to the shape of the body, such as fingerprints, palm veins, face recognition, DNA, palm prints, hand geometry, iris recognition, retina, and odor or scent.[401] BIPA also states what is not biometric information, such as writing samples, photographs, tattoos, height, weight, hair color, X-rays, or mammography.[402] Second, Illinois' BIPA through *Rosenbach* showed that a plaintiff does not have to experience actual damages to sue a defendant to establish a BIPA violation.[403] Finally, instead of giving only a State's Attorney General the legal authority to sue an entity, such as in Texas and Washington, Illinois permits private action.[404]

D. Biometric Privacy and the Federal Government

Based on the research above, it is apparent that the CCPA, as amended by the CPRA, is currently the model privacy law in the United States. It is also evident that Illinois' BIPA is the model biometric privacy law in the country. Both the CCPA, as amended by the CPRA, and BIPA are extensive pieces of legislation that precisely define an individual's privacy and biometric privacy rights. A significant limitation of both laws is that the content of the CCPA as amended by the CPRA does not overlap with the content of Illinois' BIPA. Unlike Article 14(4) of the GDPR, which explicitly covers both Internet and computer-based privacy rights as well as biometric privacy rights.[405] In the text that follows, it is argued that what is needed in the United States is a comprehensive privacy law, much like the GDPR, but tuned to the

---

[399] Biometric Information Privacy Act, 740 ILCS 14/15(c) (2008), https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57.

[400] Capture or Use of Biometric Identifier Act, Tex. Bus. & Com. Code §503.001 (2009), https://statutes.capitol.texas.gov/Docs/BC/htm/BC.503.htm; *see also* Biometric Identifiers Act, RCW § 19.375.010 (2017).

[401] Biometric Information Privacy Act § 15(c); *see also* Alzubaidi & Kalita, *supra* note 49, at 2001.

[402] Biometric Information Privacy Act § 10.

[403] Rosenbach v. Six Flags Entertainment Corp., 129 N.E.3d 1197, 1204 (Ill. 2019).

[404] Insler, *supra* note 288, at 36.

[405] Parliament Regulation 2016/679, 2018, Art. 14(4), *supra* note 140.

political nuances that exist in America. To this end, the CCPA, as amended by the CPRA and Illinois' BIPA, can be employed in the development and passage by Congress of an inclusive and far-reaching federal privacy law.

E. Recommendations

1. First Recommendation

Here are some of the recommendations that come out of the research discussed above. First and foremost is the need for a federal privacy law, much like the CCPA as amended by the CPRA, encompassing biometric privacy. The critical issue is who owns the data collected when an individual provides their data to a corporation or local, state, or federal government. In the law, a person only possesses a reasonable expectation of privacy as defined by Supreme Court case law and by specific statutes, such as the Americans with Disability Act.[406] In *Carpenter* and the preceding cases discussed herein, individuals have a reasonable expectation of privacy when the local, state, and federal government access an individual's cell phone metadata.[407] There were four distinct minority opinions in *Carpenter*, three of whom contended that there is no privacy without property rights.[408] In Justice Gorsuch's dissent, he opined that cell phone providers, the organizations that collect, store, use, and disseminate cell phone metadata, are bailees entrusted by the cell phone owners with the metadata generated by the cell phones that the cell phone owners own.[409]

What is apparent from the case law is that the reasonable expectation of privacy test and the notion that privacy can only exist when property rights are present are antithetical. The first recommendation of this essay is that synthesis must occur, merging one's reasonable expectation of privacy and the privacy is property notion into a cohesive whole so that individual privacy is protected by law. Dialectical reasoning must be employed to achieve this goal, blending the reasonable expectation of privacy thesis and the privacy as property antithesis, creating the synthesis as implied in Justice Gorsuch's dissent in *Carpenter*, where the entities that collect, store, use, and disseminate personal information are bailees.[410] Once this is

---

[406] *See* Katz v. United States, 389 U.S. 347, 350 (1967); *see e.g.,* Americans with Disability Act, 42 U.S.C. § 12101 (2021).
[407] *See generally* Carpenter v. United States, 138 S. Ct. 2206 (2018).
[408] *Id.* at 2223-61 (Kennedy, CJ, Alito & Thomas, JJ., dissenting).
[409] *Id.* at 2268-69 (Gorsuch, J., dissenting).
[410] *Id.*

achieved, biometric privacy loses its importance as an issue in itself but is transformed into a special case of privacy rights in general.

2. Second Recommendation

The second and succeeding recommendations address the mechanics of how a federal privacy law should and ought to function. What is covered under the proposed federal privacy law, and probably more importantly, what is not covered, must be stated explicitly in the proposed rule and not left to the courts' discretion. Presuming that a federal privacy law encompasses biometric privacy, a proposed federal privacy law, like BIPA, should and ought to explicitly state what personal information is protected and what is not. For example, under BIPA, fingerprints, palm veins, face recognition, DNA, palm prints, hand geometry, iris recognition, retina, and odor or scent are all physiological characteristics that are protected.[411] Behavioral factors associated with behavior patterns, including typing rhythm, gait, keystroke, signature, behavioral profiling, and voice, are also protected under BIPA.[412]

The Biometric Information Privacy Act states that biometric information is not "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."[413] Biometric information is also not "donated organs, tissues, or parts, … blood or serum stored on behalf of recipients or potential recipients of living or cadaveric transplants and obtained or stored by a federally designated organ procurement agency."[414] Biometric identifiers are not regulated biological materials (specifically, in Illinois, the Genetic Information Privacy Act of 2020), information captured from a patient in a health care setting, or information collected, used, or stored for health care treatment, payment, or operations under the federal Health Insurance Portability and Accountability Act.[415] Finally, biometric identifiers do not involve "an X-ray, roentgen process, computed tomography, MRI, PET scan, mammography, or other image or film of the human

---

411 Biometric Information Privacy Act, 740 ILCS 14/10 (2008), https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57; *see also* Alzubaidi & Kalita, *supra* note 49, at 2000; *see also* Prescott, *supra* note 52.

412 Alzubaidi & Kalita, *supra* note 49, at 2001; *see also* Biometric Information Privacy Act § 10.

413 Biometric Information Privacy Act § 10.

414 *Id.*

415 *Id.*

anatomy used to diagnose, prognose, or treat an illness or other medical condition or to further validate scientific testing or screening agency."[416]

Illinois' BIPA is quite specific to what constitutes protected biometric information and what information about an individual is not covered. When passing a federal privacy law, it can be expected that legislators will engage in considerable wrangling about what to protect and what not to protect. Such negotiations are an integral part of the negotiation process in voting on a bill to make a law. It is reasonable to expect that such infighting will naturally occur. Although there is a case to be made for the proposed federal law to contain a general definition of personal information, leaving the particulars up to the courts to decide, the risk of having a general definition of what constitutes protected personal information, biometric or otherwise, is that the Supreme Court could rule that the proposed federal privacy law is unconstitutional for vagueness. Thus, the second recommendation is that the proposed federal privacy law specifically describe what is and what is not protected personal and biometric information.

3. Third Recommendation

When a violation occurs of the proposed federal privacy law, damages need to be considered. Currently, in Illinois, when a technical breach of BIPA happens, Illinois courts cite *Rosenbach* to conclude that there is sufficient support for a cause of action, even if an individual has not experienced a loss of biometric privacy.[417] When considering a proposed federal privacy law, the mere presence of a violation could trigger the law, or the law could be invoked when a third party uses personal information for nefarious, presumably illegal ends. This is a difficult question to answer. If the proposed federal privacy law advocates the former, then the consequences may have a significant negative economic impact not foreseen by Congress. On the other hand, if the latter is contained in the proposed federal privacy law, there may be many instances where common sense privacy violations materialize without a legal remedy. Thus, the third recommendation is that a balancing test should be created where an offense transpires only when the harm to an individual outweighs the effect of a technical violation.

---

[416] *Id.*

[417] *See* Rosenbach v. Six Flags Entertainment Corp., 129 N.E.3d 1197 (Ill. 2019).

4. Fourth Recommendation

Next, there is the issue of damages to be addressed. The CCPA specifies two types of non-compliance penalties. According to the CCPA, the damages are at most $750 per violation or the actual damages, whatever is the greater amount.[418] The Attorney General of California may enforce the privacy provision of the CCPA via civil penalties with a maximum of $7,500 per violation.[419] For example, it is not uncommon for a data breach to involve one million individuals. At $750 per violation, the maximum penalty would be $750 million, whereas if the Attorney General of California decides to sue the entity, the maximum penalty would be $7.5 billion.[420] The problem with the massive amount of money that the federal government could extract from a private organization is that few entities could afford to pay the fine and remain in existence. It is quite possible that in the presence of such huge fines, a company would simply declare Chapter 7 bankruptcy. The result would be putting tens of thousands of employees out of work, if not hundreds of thousands. It is apparent that if the proposed federal privacy law were to follow the CCPA's example, one of the economic consequences could be a downturn in the economy or even a recession. Thus, the fourth recommendation is that the proposed federal privacy law employ a sliding scale of damages, where the penalty is directly proportional to the number of individual violations.

5. Final Recommendation

The final recommendation deals with the volume of individual and class action suits that could be filed with the passage of federal privacy law. As was previously observed, the Illinois Supreme Court's decision in *Rosenbach* generated a tidal wave of cases because BIPA permits private action.[421] In contrast, only the states' Attorneys General can begin legal proceedings in both Texas and Washington. Given that the Texas and Washington biometric privacy laws were passed several years after Illinois' BIPA was signed into law, the probable reason that Texas and Washington allow only their Attorneys General to instigate legal proceedings is that the respective state legislators do not want to clog their state judiciary systems with a host of private actions, like what is happening in Illinois. Private action is critical because, without the ability of individuals to sue an offending entity, the proposed

---

[418] Buresh, *supra* note 118, at 276.
[419] *Id.*
[420] Cohen et al., *supra* note 181, at 6.
[421] Insler, *supra* note 288, at 49.

federal privacy law would be a toothless tiger. Suppose individuals must rely exclusively on a federal agency to sue an offending organization. In general, given the limited resources of federal agencies, there is a distinctly significant probability that the proposed federal agency will decide not to pursue litigation, thereby denying justice to aggrieved persons. This would be an untenable situation, leaving wronged individuals without an adequate legal remedy from a civil rights perspective. Thus, a balance must be struck between individual rights of redress and judicial efficiency.

One such solution has its roots in the Civil Rights Act of 1964, as amended, and the Equal Employment Opportunity Commission.[422] It is proposed that the proposed federal privacy law establish a commission responsible for evaluating whether litigation will be filed against an organization that violated an individual's privacy or biometric privacy rights. An individual or a class of individuals could file a complaint with this commission, claiming that a private organization violated an individual's or class of individuals' privacy rights. It is suggested that the commission have 180 days to evaluate whether it will sue the offending entity.

At the end of the 180 days, the commission would release a right-to-sue letter to the complainants(s) if the commission decided not to sue. The claimant(s) would then have 540 days after receiving the right to sue letter to file suit against the offending organization. The statute of limitations would start running for individual lawsuits after the person became knowingly aware that the privacy violation occurred. The statute of limitations for a class action would begin after the class's principal representative became knowingly aware that the privacy violations happened. This final recommendation seemingly balances the rights of individuals to pursue private actions against offending organizations and the likely desire of Congress to ensure that the federal court system is not overly burdened with privacy litigation.

F. Summary

This research summarized the privacy and biometric privacy laws both in the European Union and the United States. The project observed that the United States sorely lacks a federal privacy law that encompasses the handling by companies of personal information and biometric information. It was proposed that the United States pass an all-inclusive privacy law that would act as a floor to the state privacy laws that currently exist and to the privacy bills being considered by

---

[422] C. KERRY FIELDS & HENRY R. CHEESEMAN, CONTEMPORARY EMPLOYMENT LAW, 179-87 & 158-66 (Aspen Publishers 3d ed. 2011).

the legislatures of the several states. Here, the research answered the questions proposed at the beginning of the article. The paper also listed five recommendations that should be considered if and when Congress decides to enact a broad privacy statute. It seems that privacy is becoming a burning issue in America, and that is a good thing.

CONCLUSION

In 1964, Bob Dylan, an iconic folk singer, wrote and recorded the song, *The Times They Are a-Changin'*.[423] It was a song about the turmoil that was altering the face of America in the 1960s. In 2021, in terms of privacy and biometric privacy, the times are also changing, and rapidly at that. Three states have passed general privacy laws protecting personal information, while three other states now have statutes regarding protecting biometric data privacy. Many states are currently considering bills that address the privacy concerns of their constituents. With all of this activity regarding privacy at the state level, what is conspicuous by its absence is a comprehensive federal privacy law that addresses protecting individual personal information and safeguards the privacy of a person's biometric information.

The purpose of this study was to understand and evaluate the privacy and property issues that States confront that are inherent within the use and results of using biometrics to enhance corporate security in their efforts to protect individual privacy. The recommendations from this research indicated that what is needed in the United States is a comprehensive privacy statute that protects personal information and biometric information. The CCPA, as amended by the CPRA, and Illinois' BIPA, can form the basis of a model federal law. Although the path traveled to reach this destination is fraught with crossroads, forks in the road, and the ever-present obstacles, the goal is worth pursuing. For, in the end, the journey will be worth the struggle. Americans want and need a privacy law, for they are the owners of their personal and biometric information, just as Justice Gorsuch opined in *Carpenter*. The world is rapidly changing, and what is all the rage today may be abandoned tomorrow. An inclusive and far-reaching federal privacy law is essential to protect the privacy rights of American citizens. Nothing less will suffice.

---

[423] BOB DYLAN, THE TIMES THEY ARE A-CHANGIN' (Columbia Records 1964).