PEPPERDINE UNIVERSITY

The Journal of Business, Entrepreneurship & the Law

Volume 16 | Issue 1 Article 7

5-15-2023

Complying with New and Existing Biometric Data Privacy Laws

Ariel Latzer

COMPLYING WITH NEW AND EXISTING BIOMETRIC DATA PRIVACY LAWS

Ariel Latzer*

* J.D. 2023, Pepperdine Caruso School of Law; B.A. 2019, San Diego State University. I would like to thank my amazing parents, Keren and Michael, and my incredible siblings, Maya and Adam, for your endless love and support. You are my biggest blessing and I am forever grateful for you.

I. INTRODUCTION

Biometrics have become an inescapable part of today's society as Global Markets Insight projects a fifty billion dollar valuation of the global biometric market by 2024,[1] with over thirty percent of the biometric industry coming from North America alone by that time.[2] The term "biometric" encompasses various forms of personal data which can be either morphological—consisting of features such as vein pattern, hand shape, and fingerprints—or biological—consisting of DNA information like blood and urine samples.[3] Because this type of information is specific to each person, biometric data allows the potential for various types of identification systems.[4] For example, India implemented the Aadhaar project, a biometric system that issues all residents a personalized twelve-digit identification number "based on their biographic and biometric data (a photograph, ten fingerprints, [and] two iris scans)" as a form of identification.[5]

However, the use of biometric information has expanded beyond the scope of a pure identification system and become widely used in a variety of ways which are now considered routine aspects of people's lives.[6] While some have accepted and welcomed this new technology, others have found it more concerning, evidenced by the actions of certain people and companies, such as Unlabeled, a Japanese textile brand that designs clothes to prevent people from being detected by artificial intelligence, or "camouflage against the machines."[7] Conversely, other

---

[1] Aditya Sharma, *5 Industries Getting Disrupted by Biometric Technologies*, M2SYS (Feb. 14, 2020), https://www.m2sys.com/blog/guest-blog-posts/5-industries-getting-disrupted-by-biometric-technologies/.

[2] *Biometrics: Definition, Use Cases and Latest News*, THALES (last updated June 2, 2021), https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/biometrics.

[3] *Id.* (noting how physiological readings are more accurate and consistent than behavioral measures, which may change based on the situation).

[4] *Id.*

[5] *Id.*

[6] *Id.*

[7] *See* Monica Athnasious, *How Fashion Brand UNLABELED's Wearable Technology Prevents AI from Detecting Humans*, SCREEN SHOT (Oct. 30, 2021), https://screenshot-media.com/technology/ai/hide-from-surveillance-ai/.

companies have been quick to embrace this advancing field's potential, such as Disney.[8] According to Disney's website, Disney World visitors can now scan their fingerprint through its Ticket Tag program, which converts the fingerprint into a numerical value that is later recalled when the visitor re-enters or visits another park.[9]

While there is no doubt that the use of biometric information as a form of identification brings a new sense of ease and convenience to users—since it cannot be forgotten like a normal password—there is also a great deal of criticism surrounding the field because of how personal and invasive the information truly is; there is no way of changing it if it ever gets compromised.[10] With a growing number of businesses now using biometric information in the course of everyday business and with no enacted federal law on the matter,[11] some state governments have taken it

---

[8] *Privacy at the Walt Disney World Resort, the Disneyland Resort, and Aulani, a Disney Resort & Spa – Frequently Asked Questions*, THE WALT DISNEY CO., https://disneyworld.disney.go.com/faq/my-disney-experience/my-magic-plus-privacy/ (last visited Nov. 5, 2021).

[9] *Id.* While a visitor's fingerprint is not stored, visitors who do not wish to participate in the Ticket Tag program can opt to use a photo ID to verify his or her ticket upon re-entrance or change of park. *Id.* Disney further notes that "no security measures are perfect or impenetrable," despite asserting its implementation of security measures. *Id.*

[10] *See* Tracy Lindeman, *Can Biometrics Make Your Life Easier?*, IG WEALTH MGMT. (Feb. 2018), https://www.ig.ca/en/articles/2018/02/can-biometrics-will-make-your-life-easier- (mentioning how in 2016 the United States lost $16 billion to identity theft and fraud).

[11] Jonathan M. Crotty, *Increasing Use of Biometric Information Raises Legal Issues for Employers*, PARKER POE (Nov. 11, 2022), https://www.parkerpoe.com/news/2022/11/increasing-use-of-biometric-information-raises-legal-issues. The National Biometric Information Privacy Act of 2020 (NBIPA), sponsored by Senators Jeff Merkley and Bernie Sanders, was introduced in the Senate on August 8, 2020, and referred to the Committee on the Judiciary to "regulate the collection, retention, disclosure, and destruction of biometric information, and for other purposes" but has not been passed as of February 2022. *See S.4400 – National Biometric Information Privacy Act of 2020*, CONGRESS.GOV, https://www.congress.gov/bill/116th-congress/senate-bill/4400?overview=closed (last visited Feb. 10, 2022). Instead of having a single law whose scope encompasses all types of data, the United States has many different laws—such as the Health Insurance Portability and Accountability Act (HIPAA), the Family Educational Rights and Privacy Act (FERPA), and the Children's Online Privacy Protections Rule (COPPA), which each protect a specific form of privacy. *See* Thorin Klosowski, *The State of Consumer Data Privacy Laws in the US (And Why it Matters)*, WIRECUTTER (Sept. 6, 2021), https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/.

into their own hands to create legislation imposing restrictions and guidelines for businesses in order to protect their state's residents' biometric information.[12] After providing an overview of the history behind biometric information, this article will discuss the Illinois Biometric Privacy Act (BIPA)—which laid the foundation for biometric privacy regulations in the United States—and then discuss the California Consumer Privacy Act (CCPA) and its amendments in the California Privacy Rights Act (CPRA). It will also briefly touch on biometric information regulations in other states and then delve into how some notable companies are currently using individuals' biometric information to give readers a general idea of what is happening to their personal information and highlight areas businesses should take note of in order to comply with the aforementioned Acts.

II. HISTORY OF BIOMETRICS

The use of biometric information as a form of identification is not new, in fact, there is evidence dating back as early as 500 B.C. of the Babylonians recording fingerprints in clay tablets for business transactions.[13] Fingerprinting as a form of identification was used cross-culturally and was not exclusive to the Babylonians—the Chinese used it in business transactions and to differentiate children and the Persians used it in the fourteenth century.[14] Fingerprints were first identified as being unique in 1788 by J.C.A Mayer, a German anatomist and doctor, with Sir Francis Galton developing the first classification system in 1892—the "details" Galton discovered in his identification system are still in use today.[15] Biometric identification later expanded from fingerprinting to using an individual's full handprint, with hand printing first being used in India in 1858 to distinguish employees from nonemployees on payday.[16] Not before long, biometric identification became commonplace not only within the public sector but within the prison system as well.[17] Prisons began to use fingerprints to track inmates, differentiate between first-time

---

[12] *See also* Klosowski, *supra* note 11 (listing several states which imposed their own data privacy laws, namely California, Virginia, and Colorado).

[13] Stephen Mayhew, *History of Biometrics*, BIOMETRIC UPDATE (Feb. 1, 2018, 11:43 AM), https://www.biometricupdate.com/201802/history-of-biometrics-2.

[14] *See id.*

[15] *See id.*; *Biometrics*, DEP'T OF HOMELAND SEC., https://www.dhs.gov/biometrics (last updated Dec. 14, 2021).

[16] *See* Mayhew, *supra* note 13.

[17] *Id.*

and repeat offenders and punish them differently.[18] Recognizing the usefulness of fingerprint identification adopted by several police departments across the United States, Congress officially established the FBI's Identification Division on July 1, 1921, to meet the country's need for fingerprint identification by the police.[19] The type of biometric data collected and used for identification became increasingly more sophisticated and complex, with the idea of using the iris as a form of identification first conceived in 1936, a patent for the concept issued in 1986, and a patent for the algorithm issued in 1994.[20] Biometric data tracking increased in sophistication again in the 1960s when the first semi-automatic facial recognition system was developed.[21] More recently, the use of biometric information became significantly more popular and commonplace in 2013 when Apple began using fingerprint identification with its iPhones and iPads, allowing users to unlock their devices and make purchases with the touch of a finger.[22]

III. BIOMETRIC USAGE

A. *Benefits of Biometric Information*

Both the government and private businesses now capitalize on the use of biometric data in the everyday course of business because of how invaluable this form of identification is.[23] To begin, the Department of Homeland Security uses biometrics data "to detect and prevent illegal entry into the U.S., grant and administer proper immigration benefits, vetting and credentialing, facilitating legitimate travel and trade, enforcing federal laws, and enabling verification for visa applications to the U.S."[24] Additionally, as of June 2021, the Automated Biometric Identification System (IDENT)—a Department of Homeland Security biometric storage and processing system used for national security and other related

---

[18] *See id.* Fingerprinting became the more used approach to tracking offenders over the French, Bertillon system which used the measurements of various body dimensions, physical descriptions, and photographs. *Id.*

[19] *See id.*

[20] *See id*.

[21] *Id.*

[22] *Id.*

[23] *Id.*

[24] DEP'T OF HOMELAND SEC., *supra* note 15. The Department of Defense and the Department of Justice also use biometrics. *Id.*

purposes[25]—"holds more than 260 million unique identities and processes more than 350,000 biometric transactions per day."[26] Furthermore, the Office of Biometric Identity Management (OBIM) specifically notes that an individual's biometric data will only be used for the purpose for which it is collected unless another purpose is explicitly authorized or mandated by law.[27] Moreover, technology now allows for live facial recognition that works in real-time, which can be used as a tool for public security in institutions, such as at airports and borders.[28] The U.S. Customs and Border Protection agency (CBP) is using facial recognition at border checkpoints to "automate[] a[n] [otherwise] manual process" for travelers and officers; however, the CBP still provides travelers the option to proceed with the manual process by notifying the officers at inspection that they would like to opt out.[29] Additionally, the CBP makes sure to encrypt the biometric data it collects, explaining that "[w]hen a gallery is created, that photo isn't attached to any information and can't be reverse engineered to be compromised."[30] The United States military has also collected biometric information since January 2009—namely face, iris, and fingerprint scans—which it used to identify foreign individuals on the battlefield.[31] In fact, between 2008 and 2017, the Department of Defense (DOD) "used biometric and forensic capabilities to capture or kill 1,700 individuals and deny 92,000 individuals access to military bases."[32] In addition to being used by the military, the Internal Revenue Service (IRS) announced it would use ID.me, a third-party facial recognition software company, to verify the identity of individuals using its website by comparing a picture of the user's photo ID, such as a driver's license or passport, with a video selfie of the user.[33] However, the IRS quickly

---

[25] *DHS/OBIM/PIA-001 Automated Biometric Identification System*, DEP'T OF HOMELAND SEC., https://www.dhs.gov/publication/dhsnppdpia-002-automated-biometric-identification-system (Sept. 7, 2022).

[26] DEP'T OF HOMELAND SEC., *supra* note 15.

[27] *Office of Biometric Identity Management Privacy Information*, DEP'T OF HOMELAND SEC., https://www.dhs.gov/privacy-information (Dec. 17, 2021).

[28] *Biometrics: Definition, Use Cases and Latest News*, *supra* note 2.

[29] Elaine Glusac, *What You Need to Know About Facial Recognition at Airports*, N.Y. TIMES (Feb. 26, 2022), https://www.nytimes.com/2022/02/26/travel/facial-recognition-airports-customs.html.

[30] *Id.*

[31] *Biometrics: Definition, Use Cases and Latest News*, *supra* note 2.

[32] *DOD Biometrics and Forensics: Progress Made in Establishing Long-Term Deployable Capabilities, but Further Actions are Needed Accessible Version*, U.S. GOV'T ACCOUNTABILITY OFF. (Aug. 7, 2017), https://www.gao.gov/assets/690/687207.pdf.

[33] Rachel Metz, *The IRS Website Will Soon Require Facial Recognition to Log in to Your Account*, CNN BUS.,

changed its policy providing users the option to alternatively verify their identity through a live, virtual interview with an agent without the need for any biometric information.[34]

Outside of government use, mass-scale implementation of biometric data has also ensured a higher degree of safety at large events, such as the Super Bowl, which attracts over 65,000 fans, by running face scans of attendees against a set of face scans from a watch list.[35] Casinos also use facial recognition from live video streams to identify banned individuals and alert security of their presence.[36] The Covid-19 pandemic accelerated the use and acceptance level of biometric information being used in people's everyday lives.[37] Not only is the use of biometrics a cost-saving mechanism for businesses struggling financially amid the many closures and other repercussions of the pandemic, but it also provides a quick, contactless method of identification.[38] In fact, the International Air Transport Association's (IATA) 2021 Global Passenger Survey found "73% of passengers are willing to share their biometric data to improve airport processes," a 27% increase since 2019.[39] E-passports, consisting of two

---

https://www.cnn.com/2022/01/27/tech/facial-recognition-irs-idme/index.html (Jan. 28, 2022, 4:38 PM).

[34] *See IRS Statement — New Features Put in Place for IRS Online Account Registration; Process Strengthened to Ensure Privacy and Security*, IRS (Feb. 21, 2022), https://www.irs.gov/newsroom/irs-statement-new-features-put-in-place-for-irs-online-account-registration-process-strengthened-to-ensure-privacy-and-security.

[35] Kevin Freiburger, *Biometric Security Technology at the Super Bowl is a Big Win for Public Safety*, BIOMETRIC UPDATE (Jan. 29, 2020, 12:50 PM), https://www.biometricupdate.com/202001/biometric-security-technology-at-the-super-bowl-is-a-big-win-for-public-safety (noting the increase in efficiency and admission protocol biometrics can have on sporting events, improving overall event experience).

[36] Alex Perala, *Cognitec Solution Helps Secure Macau Casinos*, FINDBIOMETRICS (Feb. 8, 2016), https://findbiometrics.com/cognitec-solution-helps-secure-macau-casinos-302082/.

[37] Elaine Glusac, *Your Face Is, or Will Be, Your Boarding Pass*, N.Y. TIMES, https://www.nytimes.com/2021/12/07/travel/biometrics-airports-security.html (Jan. 11, 2022) (suggesting how prior commonly used forms of using biometric information, such as unlocking one's phone or accessing one's bank account with facial recognition, may have helped ease the transition of using biometric information in other forms).

[38] *Id.*

[39] *Passengers Want to Use Biometrics to Eliminate Queuing Post Pandemic*, INT'L AIR TRANSP. ASS'N (Nov. 15, 2021), https://www.iata.org/en/pressroom/pressroom-archive/2021-releases/2021-11-15-01/ .

fingerprints and a photograph, are used by over 1.2 billion people as of 2021 and help speed up and secure interactions at airports and borders.[40] Furthermore, in addition to ease and efficiency, biometric identification systems also helped identify 252 people who used another's passport at a land border.[41] The ease and convenience of biometric information are causing it to replace passwords as a form of digital authentication in areas requiring high levels of security because passwords are susceptible to being stolen, especially with the increase in sophistication of cyberattacks.[42] Switching to a biometric identification system can also be more efficient and convenient for many users who want to leave passwords and PIN numbers in the past.[43] However, the use of biometric information is not without risk.

Unlike other forms of identification, such as an individual's social security number, name, password, etc., which can be changed with varying degrees of difficulty, biometric information is permanent, making it far more invasive than other forms of data collection.[44] And unfortunately, breaches of biometric data are not unheard of.[45] In 2019, security researchers found that the security company Suprema's Biostar 2's database made "27.8 [million] records[] and 23 gigabytes-worth of data" including individual's biometric information, such as fingerprints and facial recognition data, discoverable on a "publicly accessible database."[46] The "unprotected and mostly unencrypted" database resulted in an information leak reaching 1.5 million locations around the world.[47] But potentially even more concerning than this large-scale exposure is the fact that the researchers noted, "the problem wasn't unique to Suprema."[48] Part of the problem the researchers found with Suprema's data storage was the

---

[40] *Biometrics: Definition, Use Cases and Latest News*, *supra* note 2.

[41] Kyle Wiggers, *U.S. Homeland Security Has Used Facial Recognition on over 43.7 Million People*, VENTUREBEAT (Feb. 6, 2020, 2:15 PM), https://venturebeat.com/2020/02/06/u-s-homeland-security-has-used-facial-recognition-on-over-43-7-million-people/.

[42] *See* Danny Thakkar, *Biometrics in Social Media Apps: Opportunities and Risks*, BAYOMETRIC, https://www.bayometric.com/biometrics-in-social-media-apps/ (last visited Dec. 24, 2021).

[43] *See id.*

[44] *See id.* (comparing how some forms of non-biometric data, such as IP addresses, can become obsolete over time rendering them useless).

[45] *See, e.g.*, Josh Taylor, *Major Breach Found in Biometrics System Used by Banks, UK Police and Defence Firms*, THE GUARDIAN (Aug. 14, 2019, 3:11 EDT), https://www.theguardian.com/technology/2019/aug/14/major-breach-found-in-biometrics-system-used-by-banks-uk-police-and-defence-firms.

[46] *Id.*

[47] *Id.*

[48] *See id.*

fact that the company stored individuals' actual fingerprints, which could be copied, as opposed to hashing[49] the fingerprints, which cannot be reverse engineered if stolen.[50] Nevada Restaurant Services, the parent company to national gambling chain Dotty's, experienced a breach on or before January 16, 2021 due to malware found on certain computer systems resulting in some customers' personal information, including their biometric data, being leaked.[51] The company announced it would provide complementary identity protection services—as is customary in this circumstance—and increase its security; however, when it comes to any compromised biometric data, it may be too little too late.[52]

B. *Need for Restrictions*

Having restrictions with legal consequences on a company's inappropriate use of individuals' biometric information is imperative because large corporations and the like tend to understand hefty fines better than they do respecting the personal privacy of others simply because it is the right thing to do.[53] TikTok is one of the companies that needed a monetary wake-up call to respect these privacy boundaries.[54] More specifically, it needed a $92 million class action lawsuit settlement against it for violating the BIPA where claimants "alleged the app captured biometric and private data from users in the U[.]S[.] and passed private

[49] *Id.* Hashing is "a one-way function" allowing information, such as biometric data, to be converted "into a non-reversible cryptographic hash rather than a template" thereby promoting security by only giving the hacker access to the hashed version of the sensitive information and not its plaintext. *ID R&D Partners with Infinity Optics to Bring Passive Liveness Detection to Privacy Biometric Trust Platform*, ID R&D, https://www.idrnd.ai/id-rd-partners-with-infinity-optics-to-bring-passive-liveness-detection-to-privacy-biometric-trust-platform/ (last visited Jan. 1, 2022).

[50] Taylor, *supra* note 45.

[51] Jonathan Greig, *Popular Slot Machine Chain Dotty's Reveals Data Breach Exposing SSNs, Financial Account Numbers, Biometric Data, Medical Records and More*, ZDNET (Sept. 16, 2021), https://www.zdnet.com/article/popular-slot-machine-chain-dottys-reveals-data-breach-exposing-ssns-financial-account-numbers-biometric-data-medical-records-and-more/.

[52] *See id.*

[53] *See, e.g.*, Sarah Perez, *TikTok Just Gave Itself Permission to Collect Biometric Data on US Users, Including 'Faceprints and Voiceprints'*, TECHCRUNCH (June 3, 2021, 3:57 PM PDT), https://techcrunch.com/2021/06/03/tiktok-just-gave-itself-permission-to-collect-biometric-data-on-u-s-users-including-faceprints-and-voiceprints/.

[54] *See id.*

user data on to third parties"[55] in order to incentivize the company to create its new biometric data collection disclosure policy.[56] As of its most recent Privacy Policy, TikTok states that for users over the age of thirteen, the app may automatically collect "biometric identifiers and biometric information as defined under U.S. laws, such as faceprints and voiceprints, from [a user's] User Content."[57] Additionally, the app's updated Privacy Policy states that where required by law, it will get any required permissions it needs for that collection from the user before getting a user's biometric information.[58] However, to avoid imposing too many restrictions on itself, TikTok also added its ability to de-identify or aggregate the data that is not subject to that Privacy Policy.[59] Also, while TikTok does not sell users' information, it added its ability to share that information for business purposes.[60] The Privacy Policy also allows TikTok to share the information it collects in response to law enforcement requests and government inquiries, potentially funneling biometric information from the private sector into the public sector.[61]

C. *Biometrics in Other Countries*

The United States is not alone in developing regulations surrounding biometric data and determining how companies can use it.[62]

---

[55] Sean Keane, *TikTok is Letting Itself Collect Your Biometric Data*, CNET (June 4, 2021, 7:59 a.m. PDT), https://www.cnet.com/tech/services-and-software/tiktok-is-letting-itself-collect-your-biometric-data/.

[56] Perez, *supra* note 53. The lawsuit was originally filed in May 2020. *Id.*

[57] *Privacy Policy*, TIKTOK, https://www.tiktok.com/legal/privacy-policy-us?lang=en (last updated Jan. 1, 2023). Furthermore, in its Privacy Policy, TikTok defines "User Content" as information a user voluntarily provides to the app by either creating or uploading the "[u]ser-generated content, including comments, photographs, livestreams, audio recordings, videos, text hashtags, and virtual item videos," to the app. *Id.*

[58] *Id.* Although it sounds comforting that TikTok will seek a user's permission where required by law, the policy does not concretely outline how it plans to get the permissions it mentions or what law it is referring to—federal, state, or both—which is important because only a few states currently have biometric privacy laws that would give this statement any weight. *See* Perez, *supra* note 53.

[59] *See Privacy Policy*, *supra* note 57.

[60] *See id.* TikTok includes advertising, marketing, and analytics vendors as examples of business partners who may receive information TikTok automatically collects, such as biometric information, from its users. *See id.*

[61] *See id.*

[62] *See Biometric Data and Privacy Laws (GDPR, CCPA/CPRA)*, THALES, https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/biometric-data.

Because these regulations vary in protection level, sometimes companies have different policies in one country than they do in another.[63] This is the case with TikTok, which updated its United States privacy policy to include a disclaimer about biometric data collection that was unnecessary in the European Union, whose "stricter data protection and privacy laws" eliminated the need for such a disclaimer."[64] Although there is a range of biometric privacy laws, something all regions seemingly share is the steep fines companies pay for breaching them.[65] An English lawsuit against YouTube sought £2.5 billion, or roughly $3.1 billion, in damages for knowingly violating the country's children's privacy laws.[66] In the United States, Google agreed to settle with the Federal Trade Commission for $170 million—paling in comparison to the $38.9 billion reported revenue its parent company, Alphabet Inc., made during the most recent financial quarter at that time—"over allegations that it violated the Children's Online Privacy Protection Act or COPPA."[67] Likewise, in 2020, Facebook agreed to pay a $550 million settlement for a 2015 class action suit over its facial recognition software that "suggested tags for people it identified in users' photos," which potentially violated BIPA.[68] Similarly, Australia held Clearview AI's[69] facial recognition violated the country's Privacy Act of 1988 when it "covertly collected citizens' facial biometrics and incorporated them into its AI-powered identity matching service — which

[63] *See* Perez, *supra* note 53.

[64] *See id.*

[65] Kate Cox, *YouTube Unlawfully Violates Kids' Privacy, New $3.2B Lawsuit Claims*, ARS TECHNIA (Sept. 14, 2020, 10:51 AM), https://arstechnica.com/tech-policy/2020/09/google-faces-3-2b-lawsuit-over-claims-it-violated-childrens-privacy.

[66] *Id.*

[67] *Id.* Of the $170 million settlement, $136 million went to the FTC and the remaining $34 million went to the New York Attorney General's Office. Kate Cox, *YouTube fined $170 million for violations of children's privacy*, ARS TECHNICA (Sept. 4, 2019, 7:53 AM), https://arstechnica.com/tech-policy/2019/09/youtube-fined-170-million-for-violations-of-childrens-privacy/.

[68] Sara Morrison, *don't expect a $550 million settlement to stop Facebook from scanning your face*, VOX (Jan. 30, 2020, 3:40 PM), https://www.vox.com/recode/2020/1/30/21115260/facebook-facial-recognition-scan-face.

[69] Clearview AI says it is a platform that is "powered by facial recognition technology" containing over 10 billion facial images "sourced from public-only web sources, including news media, mugshot websites, public social media, and other open sources"—that it claims is the largest known database of this information. CLEARVIEW AI, https://www.clearview.ai/ (last visited Jan. 2, 2022).

it sells to law enforcement agencies and others."[70] Clearview is now under order to "stop collecting facial biometrics and biometric templates from Australians" and to "destroy all existing images and templates that it holds."[71] Sweden also held that Clearview AI violated its Criminal Data Act and fined local police €250,000 for using the program.[72] Moreover, on its own terms, Clearview "withdrew from the Canadian market after that country's privacy commissioner found that the company used personal photos without consent, in violation of the country's laws."[73]

IV. STATE LAWS SURROUNDING BIOMETRIC INFORMATION

A. *Illinois Biometric Information Privacy Act (BIPA)*

Illinois was the first state to issue a Biometric Information Privacy Act (BIPA) in 2008.[74] It represents the "gold standard" for biometric litigation matters.[75] The BIPA contains the broadest private right of action,[76] making it easier for individuals to successfully bring suit against those who violate their rights under it.[77] The BIPA defines a biometric identifier as "a retina or iris scan, fingerprint, voiceprint, or scan of hand

---

[70] Natasha Lomas, *Clearview AI told it broke Australia's privacy law, ordered to delete data*, TECHCRUNCH (Nov. 3, 2021, 8:36 AM), https://techcrunch.com/2021/11/03/clearview-ai-australia-privacy-breach/.

[71] *Id.*

[72] *Id.*

[73] J.D. Tuccille, *Lawsuit Challenges Clearview's Use of Scraped Social Media Images for Facial Recognition*, REASON (Mar. 15, 2021, 8:45 AM), https://reason.com/2021/03/15/lawsuit-challenges-clearview-use-of-scraped-social-media-images-for-facial-recognition/.

[74] Christopher Ward & Kelsey C. Boehm, *Developments in Biometric Information Privacy Laws*, FOLEY & LARDNER LLP (June 17, 2021), https://www.foley.com/en/insights/publications/2021/06/developments-biometric-information-privacy-laws. Arkansas, California, Texas, and Washington have BIPA-based legislation and another twenty-seven states have pending legislation on the matter as of June 2021—the only states that regulate biometric privacy using measures other than enacted or pending legislation based on BIPA are Georgia, Kansas, Michigan, Missouri, and South Dakota. *Id.*

[75] *See* Molly DiRago, *The Litigation Landscape of Illinois' Biometric Information Privacy Act*, A.B.A. (Aug. 20, 2021), https://www.americanbar.org/groups/tort_trial_insurance_practice/committees/cyber-data-privacy/the-litigation-landscape/.

[76] A private right of action allows a private citizen, as opposed to the government, to bring forth a civil lawsuit either by express or implied permission. *See* Mariia Synytska, *Private Right of Action*, LAWRINA (Sept. 28, 2021), https://lawrina.com/blog/private-right-of-action/.

[77] *See* DiRago, *supra* note 75.

or face geometry" and biometric information as "any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual," and both receive protection under the Act.[78] To collect individuals' biometric identifiers or biometric information under this Act, private businesses are required to: (1) provide them with written notification of its collection and storage, (2) along with the purpose of its collection and the period of time it will be stored, (3) and must receive written release from that individual.[79] Furthermore, to retain individuals' biometric information or biometric identifiers, private entities must have a publicly available written policy outlining how to retain the data and later permanently destroy it.[80] However, even if a private business meets the requirements to validly collect biometric information and biometric identifiers, the BIPA prohibits it to "sell, lease, trade, or otherwise profit from a person's or a customer's biometric identifier or biometric information."[81] Similarly, the BIPA prohibits private entities from disseminating an individual's biometric information or biometric identifier unless: (1) the individual consents, (2) it is to complete a financial transaction the individual requested or authorized, (3) a state or federal law or municipal ordinance requires disclosure, or (4) a valid court issued warrant or subpoena requires disclosure.[82] Additionally, while businesses cannot sell their employees' or customers' biometric information, they may collect and store it as long as they: (1) provide notice; (2) have policy guidelines outlining its collection, use, and storage of information; and (3) use a "commercial standard of care" to protect sensitive information.[83]

Businesses operating under the terms of the BIPA should be wary to ensure compliance because of how low the bar is to raise a valid claim under the Act.[84] In 2019, the Illinois Supreme Court held in *Rosenbach v.*

---

[78] 740 ILL. COMP. STAT. ANN. 14/10. (2008).

[79] *Id.* at 14/15.

[80] *Id.* at 14/15(a) (explaining that permanent destruction of biometric information and biometric identifiers must occur either once the reason for their collection has occurred or within three years of the individuals last encounter with the private entity, whichever occurs sooner).

[81] *Id.* at 14/15(c).

[82] *Id.* at 14/15(d) (1-4).

[83] Jonathan Herpy, *Staying in Compliance with Biometric Privacy Laws as a Business*, FORBES (Apr. 5, 2021, 9:00 AM), https://www.forbes.com/sites/forbesbusinesscouncil/2021/04/05/staying-in-compliance-with-biometric-privacy-laws-as-a-business/?sh=3d244d973123.

[84] *See, e.g.*, Rosenbach v. Six Flags Ent. Corp., 129 N.E.3d 1197 (Ill. 2019).

Six Flags Entertainment Corporation that individuals can successfully bring action as an "aggrieved" person under the BIPA against an entity for simply violating the terms of the BIPA without having sustained any actual damages.[85] This should be especially concerning for businesses because the BIPA allows for a private right of action for any person "aggrieved" by a BIPA violation granting the prevailing party relief for each statutory violation.[86] Where the private entity negligently violates the BIPA, the prevailing party may receive either $1,000 in liquidated damages or actual damages, whichever amount is greater.[87] However, in cases of reckless or intentional violations of the Act, the prevailing party may receive up to $5,000 in liquidated damages or actual damages, whichever is greater.[88] Furthermore, the court can award attorneys' fees, costs, and other relief as the court deems fit.[89]

B. *California Consumer Privacy Act of 2018 (CCPA)*

While California does not currently have an act specifically protecting biometric information, on June 28, 2018 it passed the California Consumer Privacy Act (CCPA) which took effect on January 1, 2020, giving consumer's greater rights and protection over their biometric data.[90] Furthermore, although both the CCPA and the BIPA address biometric data privacy, the CCPA is broader in scope and affects more businesses.[91] More specifically, the CCPA protects any consumer, defined as "a natural person who is a resident of California."[92] The Act further defines "biometric information" as meaning:

---

[85] *Id.* at 1206.

[86] *See* 740 ILL. COMP. STAT. ANN. 14/20.

[87] *See id.* at 14/20 (1).

[88] *See id.* at 14/20 (2).

[89] *See id.* Injunctions are an example of other relief the court may award. *See id.*

[90] Robert Bateman, *What is the California Consumer Privacy Act (CCPA)?*, TERMSFEED, https://www.termsfeed.com/blog/ccpa/ (last updated on Jan. 27, 2023).

[91] Lori Tripoli, *Resurgent BIPA More Than Second Fiddle to CCPA?*, COMPLIANCE WEEK (Feb. 21, 2020, 8:36 AM), https://www.complianceweek.com/data-privacy/resurgent-bipa-more-than-second-fiddle-to-ccpa/28481.article.

[92] CAL. CIV. CODE § 1798.140(i) (West 2020); *see* Brooks v. Thomson Reuters Corp., No. 21-CV-01418-EMC, 2021 WL 3621837, at *6, *50 n.4 (N.D. Cal. Aug. 16, 2021). In *Brooks v. Thomson Reuters Corp.*, plaintiffs qualified for protection under the CCPA despite not actually having purchased any of defendant's products or services and qualified as "consumers" under the Act based on meeting its definition for "consumer,"—"a natural person who is a California resident." *Brooks*, 2021 WL 3621837, at *6, *50 n.4.

> [A]n individual's physiological, biological, or behavioral characteristics, including an individual's deoxyribonucleic acid (DNA), that can be used, singly or in combination with each other or with other identifying data, to establish individual identity. Biometric information includes, but is not limited to, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information.[93]

Biometric information is one of the many types of identifying data the Act explicitly defines as being "personal information."[94] However, deidentified or aggregate consumer information, or publicly available" information—information lawfully obtained from the government, not "biometric information collected by a business about a consumer without the consumer's knowledge"—is not personal information."[95]

Although implemented by the state of California, businesses operating outside of the State must also take note of the effects of the CCPA because it "directly implicates a wide swath of entities collecting/using the biometric data of California residents—even if the entity does not maintain any physical presence in the state"[96]—or roughly

---

[93] CAL. CIV. CODE § 1798.140(c) (West 2020). Note that beginning January 1, 2023, the CPRA will amend the definition of "biometric information" to include "*information pertaining to* an individual's deoxyribonucleic acid (DNA), that *is used or is intended to* be used" to establish that individual's identity in some manner. CAL. CIV. CODE § 1798.140(c) (West 2020) (effective Jan. 1, 2023) (emphasis added).

[94] CAL. CIV. CODE § 1798.140(v)(1)(E) (West 2020).

[95] *Id.* at § 1798.140(v)(2)-(3) (West 2020).

[96] Jeffrey N. Rosenthal, David J. Oberly & Harrison M. Brown, *Analyzing the CCPA's Impact on the Biometric Privacy Landscape*, LAW.COM (Oct. 14, 2020, 7:00 AM), https://www.law.com/legaltechnews/2020/10/14/analyzing-the-ccpas-impact-on-the-biometric-privacy-landscape/?slreturn=20211009225037; *see also* CAL. CODE REGS. TIT. 18, § 17014 (defining "resident" as "(1) every individual who is in the State for other than a temporary or transitory purpose, and (2) every individual who is domiciled in the State who is outside the State for a temporary or transitory purpose. All other individuals are nonresidents").

39.1 million people as of July 2021.[97] That being said, this Act only regulates for-profit companies doing business in California that either: (1) have an annual revenue greater than $25 million; (2) "[b]uys, receives for the business' commercial purposes, sells, or shares . . . the personal information of 50,000 or more consumers, households, or devices;" or (3) make at least half of its annual revenue through selling the personal information of California residents.[98] Consequently, nonprofit organizations and government agencies are not required to comply with the terms of the CCPA since they fall outside the scope of entities the Act protects consumers from.[99]

When determining if an entity is bound by the CCPA, not only does it have to be the correct type of entity—a for-profit operation meeting one of the three requirements listed above—it also has to meet the broader requirement of being a business.[100] The CCPA protects consumer's from a business's violation of the Act; however, if the defendant entity successfully shows it is a service provider[101] and not a business, the resulting course of action differs.[102] Furthermore, along with the increase in protection for California consumers, the "CCPA also poses a significant

---

[97] *Quick Facts California*, U.S. CENSUS BUREAU, https://www.census.gov/quickfacts/fact/table/CA# (last visited Jan. 7, 2021).

[98] California Consumer Privacy Act, OFF. OF THE ATT'Y GEN. CAL. DEP'T OF JUST., https://oag.ca.gov/privacy/ccpa, (last visited Jan. 7, 2021); *see* CAL. CIV. CODE § 1798.140 (West 2020) (stating an entity needs to fall within one of the three listed categories in order to be bound by the CPRA, which is why all business, not just large companies, should take note of Act's requirements).

[99] *See generally* CAL. CIV. CODE § 1798.140. However, data brokers should take note of the CCPA as well because section 1798.99.80 of the California Civil Code defines data broker as "a *business* that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship" with the exception of consumer reporting agencies and certain financial institutions and insurance companies. *See* CAL. CIV. CODE § 1798.99.80 (West 2020) (emphasis added).

[100] *See* CAL. CIV. CODE § 1798.140(d) (West 2020).

[101] A service provider under the CCPA is an entity that "processes personal information on behalf of a business" upon receiving consumers' personal information from the business, which the service provider may only use for the specific business or commercial purposes outlined in the contract between the two or other purposes permitted by the CCPA. *Id.* at § 1798.140(ag)(1).

[102] *See Id.* at § 1798.155(b); Karter v. Epiq Sys., Inc., No. SACV2001385CJCKESX, 2021 WL 4353274, at *2 (C.D. Cal. July 16, 2021) (defendant's argued plaintiff could not sue them under the CCPA because under the Act they are service providers, not businesses). Under the CCPA, claims against service providers "in a civil action brought in the name of the people of the State of California by the Attorney General." CAL. CIV. CODE § 1798.155(b) (West 2020).

risk of class action litigation" which businesses should be aware of.[103] Businesses that violate the Act and fail to cure the alleged violation thirty days after receiving notice of it face a civil penalty of up to $2,500 for each violation or a penalty of up to $7,500 for each intentional violation.[104]

Businesses may still collect consumers' personal information; however, under the CCPA, upon consumer request, a business must disclose (1) the categories of personal information it collected about the consumer, (2) the sources it collected that information from, (3) its purpose in collecting or selling the information, (4) the third parties it shares personal information with, (5) and what "specific pieces of personal information it has collected about that consumer."[105] A business must also inform consumers of the categories of personal information it will collect and its purpose for collecting it at or before the time of collection.[106] If, after consenting that a business or service provider can collect his or her personal information, a consumer changes his or her mind and wishes to revoke his or her consent, the business or service provider is required to delete any information it has on that person upon receipt of a verifiable consumer request unless the information meets one of the nine listed exceptions.[107] Further, while businesses can sell a consumer's personal information or disclose it for business purposes to third parties, third parties are prohibited from further selling that information "unless the consumer has received explicit notice and is provided an opportunity to exercise the right to opt-out pursuant to Section 1798.120."[108] That being

---

[103] Rosenthal, Oberly & Brown, *supra* note 96.

[104] CAL. CIV. CODE § 1798.155(a) (West 2020).

[105] CAL. CIV. CODE § 1798.110 (West 2020) (businesses are only required to disclose a consumer's personal information twice during a twelve-month period, further disclosure is at the business' discretion).

[106] *Id.*

[107] *Id.* at § 1798.105. (Stating a business or service provider does not have to comply with an individual's request to delete his or her personal information if that information is necessary to (1) complete a transaction or perform on a contract the consumer requested, (2) detect security incidents or prosecute those responsible for it, (3) identify and repair errors affecting the business or service provider's existing functionality, (4) exercise free speech on behalf of itself or another consumer, (5) comply with the California Electronic Communications Privacy Act, (6) if the deletion would seriously impair public or peer-reviewed scientific research in the public interest, (7) for strictly internal use the consumer would reasonably expect, (8) comply with legal obligations, or (9) for other internal uses compatible with the content the information was provided).

[108] *Id.* at § 1798.115(d). A consumer may exercise this right, which can be referred to as the right to opt-out, at any point. *See* CAL. CIV. CODE § 1798.120(a) (West 2020).

said, if a business has actual knowledge a consumer is under the age of sixteen, it may not sell his or her personal information without the consumer's consent or without the consent of his or her parent or guardian if the consumer is under the age of thirteen—exhibiting an opt-in as opposed to an opt-out approach to privacy.[109] In addition, businesses must abide by a consumer's request not to sell his or her personal information or the lack of consent to sell personal information in the case of consumers less than sixteen years old.[110] However, businesses can deny a consumer's request to opt-out of data sale under certain circumstances listed in California Civil Code Section 1798.145—such as instances where complying with legal obligations necessitates the sale of a consumer's personal information or if the personal information is of a certain nature, among other exceptions.[111]

Businesses cannot discriminate against consumers who opt-out of data collection under the CCPA by denying them the goods or services the entity provides, charging them different prices or rates for those goods or services, providing them with goods or services of a different quality, or suggesting that any of the above would occur to non-participating customers.[112] However, the CCPA also stipulates that an entity may charge customers who exercise their right to not participate in a business' data collection measures a different rate or provide them with a different quality of goods or services as long as that difference is reasonably related to the value the consumer's data supplies.[113] Although businesses cannot discriminate against those exercising their right under the Act to opt-out of data collection, businesses may encourage customers to voluntarily participate by offering them financial incentives if they provide opt-in consent for the business to collect, sell, or delete their personal information.[114] The CCPA authorizes businesses to provide incentives in

---

[109] CAL. CIV. CODE § 1798.120(c).

[110] *Id.*

[111] *California Consumer Privacy Act*, *supra* note 98.

[112] CAL. CIV. CODE § 1798.125(a)(1) (West 2020). Furthermore, effective January 1, 2023, under the CPRA, businesses will also be prohibited from retaliating against current employees, individuals who applied for employment, or independent contractors who chose not to opt-in to the business's data collection procedures. CAL. CIV. CODE § 1798.125(a)(1)(E) (effective Jan. 1, 2023).

[113] CAL. CIV. CODE § 1798.125(a)(2).

[114] *See id.* at § 1798.125(b)(1). The CPRA slightly changes what acts businesses can offer customers incentives for, namely adding the sharing of customers personal data and changing deletion of said data to its retention. Additionally, businesses will be required to wait a minimum of twelve months before requesting for a consumer who previously opted-out of data collection to provide opt-in consent. *See* § 1798.125(b)(1), (3).

the form of payment as compensation or a different "price, rate, level, or quality of goods or services" directly related to the value the consumer's data provides the business.[115] However, a financial incentive program may not be "unjust, unreasonable, coercive, or usurious in nature,"[116] and may only allow consumer participation following the consumer's opt-in consent describing the program's material terms and reserving the right to revoke that consent at any time.[117]

C. *California Privacy Rights Act (CPRA)*

Californians voted to amend and expand the CCPA on November 3, 2020, by passing Proposition 24, the California Privacy Rights Act (CPRA).[118] Although officially effective December of 2020, the changes the CPRA makes to the CCPA only became "operative" as of January 1, 2023.[119] Furthermore, the California Privacy Protection Agency and the California Attorney General will only begin enforcement of CPRA violations on July 1, 2023, for incidents occurring on or after that date, providing businesses with time to amend their privacy policies as necessary to comply with the regulations—however, businesses must still comply with the CCPA during this period.[120]

One of the important changes to the CCPA present in the CPRA is the definition of biometric information.[121] While it remains similar to the original definition set out in the CCPA, it also encompasses any information "pertaining to" the information previously included in the definition, expanding the scope of what the CCPA protects.[122] The change also narrows the statute's scope by protecting biometric information that is "used or is intended to be used" to identify an individual, not just information that "can be used" for identification.[123] The CPRA also adds

---

[115] CAL. CIV. CODE § 1798.125(b)(1) (West 2020) (amended 2020).

[116] Id. § 1798.125(b)(4)

[117] *Id.* § 1798.125(b)(3).

[118] *CCPA vs CPRA: What's the Difference?*, BLOOMBERG LAW, https://pro.bloomberglaw.com/brief/the-far-reaching-implications-of-the-california-consumer-privacy-act-ccpa/ (Jan. 23, 2023).

[119] *Id.*

[120] *Id.*

[121] *Compare* CAL. CIV. CODE § 1798.140(b) (West 2020) (amended 2020) (defining "biometric information), *with* CAL. CIV. CODE § 1798.140(c) (West 2020) (operative Jan. 1, 2023) (amending definition of "biometric information").

[122] CAL. CIV. CODE § 1798.140(c) (West 2020) (effective Jan. 1, 2023).

[123] *Compare* CAL. CIV. CODE § 1798.140(b) (West 2020) (amended 2020), *with* CAL. CIV. CODE § 1798.140(c) (West 2020) (effective Jan. 1, 2023).

a definition for "advertising and marketing" used in the context of the statute to mean "a communication by a business or a person acting on the business' behalf in any medium intended to induce a consumer to obtain goods, services, or employment."[124] However, even more importantly, the CPRA changes the definition of what qualifies as a "business," directly changing to what kinds of entities it applies.[125] As of January 1, 2023, the date the CPRA became operative, a "business" now refers to a for-profit entity doing business in California that either (1) has a gross annual revenue over twenty-five million dollars in the prior year; (2) buys, sells, or shares 100,000 or more consumers' or households' personal information alone or in any combination; or (3) makes at least half of its annual revenue by "selling or sharing consumers' personal information."[126] Furthermore, the CPRA expands the scope of what the CCPA defines as a "business purpose," supplementing the existing short-term, transient use provision to include "nonpersonalized advertising shown as part of a consumer's current interaction with the business," provided that the business does not disclose the consumer's personal information to third parties or use it to build that consumer a profile or alter the consumer's experience with the business in other interactions with that business.[127] Another new business purpose added by the CPRA that companies should take note of is providing consumers with marketing and advertising services.[128] More specifically, with the exception of cross-context behavioral advertising, service providers or contractors may not combine the personal information received from the business about consumers who opted-out of data collection with the personal information they receive from another person or collected through that entity's own interactions with the consumer.[129] Moreover, with the implementation of the CPRA, speech that federal and state courts recognize as noncommercial speech—such as political speech and journalism—are no longer expressly listed as acts that are not a "commercial purpose" as it previously was under the CCPA.[130]

---

[124] CAL. CIV. CODE § 1798.140(a) (West 2020) (effective Jan. 1, 2023).

[125] *See id.* § 1798.140(d).

[126] *Id.* § 1798.140(d)(1)(A)–(C). Although the CPRA changes all provisions in this subparagraph, the most notable changes are arguably the amendments to the second and third provisions: increasing the personal information-sharing threshold from 50,000 to 100,000 consumers or households and accounting for revenue derived from "sharing"—not merely "selling"—personal information. *See id.* § 1798.140(d)(1)(B)–(C).

[127] *Id.* § 1798.140(e)(4).

[128] *See id.* § 1798.140(e)(6).

[129] *See id.*

[130] *See id.* § 1798.140(g). Businesses engaging in the type of speech that federal or state courts deem as "noncommercial" should take further precaution

Many privacy issues expressed in both the CCPA and the CPRA revolve around getting the consumer's consent for the collection, storage, etc., of personal information; therefore, businesses should pay special attention to the CPRA's definition of consent.[131] While left unmentioned in the CCPA, the CPRA establishes that consent is

> [A]ny freely given, specific, informed, and unambiguous indication of the consumer's wishes by which the consumer, or the consumer's legal guardian, . . . including by a statement or by a clear affirmative action, signifies agreement to the processing of personal information relating to the consumer for a narrowly defined particular purpose.[132]

The CPRA also expressly states what is not consent.[133] Namely, a consumer accepting "general or broad terms of use, or similar document, that contains descriptions of personal information processing along with other, unrelated information, does not constitute consent."[134] Neither does a consumer "[h]overing over, muting, pausing, or closing a given piece of content" nor an agreement attained via "use of dark patterns" constitute consent.[135] Consequently, businesses should ensure that the agreements they provide consumers with to obtain consent for consumers' personal information are narrowly and concisely defined, without any unnecessary information, to fall within the CPRA's definition of consent.[136]

D. *Other States*

Although Illinois and California are the two main states discussed in this article, they are not the only states with regulations regarding the

---

going into the implementation of the CPRA because they can no longer rely on that type of speech being expressly designated as an act outside the scope of a "commercial purpose." *Compare* CAL. CIV. CODE § 1798.140(f) (West 2020) (amended 2020), *with* CAL. CIV. CODE § 1798.140(g) (West 2020) (effective Jan. 1, 2023).

[131] *See* CAL. CIV. CODE § 1798.140(h) (West 2020) (effective Jan. 1, 2023).

[132] *Id.*

[133] *Id.*

[134] *Id.*

[135] *Id.*

[136] *See also* CAL. CIV. CODE § 1798.140(h) (West 2020) (effective Jan. 1, 2023).

use and collection of their residents' biometric information.[137] Arkansas, Texas, and Washington, in addition to California, have adopted legislation modeled off of Illinois' BIPA, while several other states have pending legislation based on BIPA.[138] However, following BIPA's lead is not the only way states can regulate the privacy of their residents' biometric information.[139] Many other states monitor that information through existing statutes and/or pending legislation not modeled after BIPA.[140] Although each state gets to decide for itself how to regulate its residents' biometric information and what the details of those regulations will be, only five states, Georgia, Kansas, Michigan, Missouri, and South Dakota, lack any form of existing or pending regulations regarding biometric information as of June 2021.[141] Furthermore, just because a state models its legislation on BIPA does not mean the terms of the regulations are identical.[142] For example, while Illinois and California each allow their residents to bring a private right of action under each state's respective regulations, Texas and Washington do not and instead vest the authority to raise a claim under each state's respective acts with the attorney general.[143]

---

[137] *See* Ward & Boehm, *supra* note 74.

[138] ARK. CODE ANN. § 4-110-104 (2022); CAL. CIV. CODE § 1798.100 (West 2023); TEX. BUS. & COM. CODE § 503.001 (West 2009); WASH. REV. CODE § 19.375.020 (2022); *Id.* Some of the states with pending legislation based on BIPA as of June 2021 include New York, Pennsylvania, Florida, Connecticut, Maryland, New Jersey, Indiana, Hawaii, and Oklahoma. Ward & Boehm, *supra* note74. New York City amended its own administrative code on July 9, 2021, to include the protection of biometric identifier information. N.Y.C. ADMIN. CODE §§ 22-1201–05; *see* Sophie L. Kletzien & Mark H. Francis, *NYC Passes Biometric Data Protection Laws Aimed at Businesses, Smart Access Building Owners*, HOLLAND & KNIGHT (Aug. 19, 2021), https://www.hklaw.com/en/insights/publications/2021/08/nyc-passes-biometric-data-protection-laws-aimed-at-businesses. Additionally, Colorado and Virginia have adopted broad consumer privacy regulations similar to California's CCPA. *A Comprehensive Resource for Tracking U.S. State Privacy Legislation*, HUSCH BLACKWELL, https://www.huschblackwell.com/2022-state-privacy-law-tracker (last updated Jan. 4, 2023).

[139] *See* Ward & Boehm, *supra* note 74.

[140] *See* Ward & Boehm, *supra* note 74. These states include Delaware, New Hampshire, Nevada, Ohio, Oregon, Iowa, Tennessee, and Wyoming, as well as the District of Columbia. *Id.*

[141] *Id.*

[142] *See The Evolution of Biometric Data Privacy Laws*, BLOOMBERG L. (Jan. 25, 2023), https://pro.bloomberglaw.com/brief/biometric-data-privacy-laws-and-lawsuits/.

[143] *See* 740 ILL. COMP. STAT. ANN. 14/20 (West 2008); CAL. CIV. CODE § 1798.150 (West 2020); TEX. BUS. & COM. CODE ANN. § 503.001(d) (West 2017); WASH. REV. CODE ANN. § 19.375.030 (West 2017). In addition to having

V. EXAMPLES OF HOW MAJOR COMPANIES ARE USING BIOMETRIC DATA

A. *Apple's Use of Biometric Information*

Apple uses individuals' biometric information through its Face ID program, [144] which it describes as providing "intuitive and secure authentication enabled by the state-of-the-art TrueDepth camera system with advanced technologies to accurately map the geometry of [an individual's] face." [145] The TrueDepth camera system does this by "captur[ing] accurate face data [through] projecting and analyzing thousands of invisible dots to create a depth map of [a user's] face and also captures an infrared image of [his or her] face." [146] However, unlike Suprema's largely unencrypted Biostar 2 database, "Face ID data—including mathematical representations of [a user's] face—is encrypted and protected by the Secure Enclave."[147] This is good news for all Apple users since "the TrueDepth camera intelligently activates to support attention aware features, like dimming the display if you aren't looking at your device or lowering the volume of alerts if you're looking at your device[,]" even for those who do not enroll in the Face ID program.[148] However, consumers can manually turn this feature off.[149]

Apple seems to take its users' biometric information safety more seriously than other companies by making its collection and storage

---

different approaches as to who can raise a claim, these states also differ in the amount of damages they are authorized to give, what type of notice and consent is required, and what the scope of the act is, among other things. *See The Evolution of Biometric Data Privacy Laws*, BLOOMBERG L. (Jan. 25, 2023), https://pro.bloomberglaw.com/brief/biometric-data-privacy-laws-and-lawsuits/.

[144] *See About Face ID Advanced Technology*, APPLE (Apr. 27, 2022), https://support.apple.com/en-us/HT208108. Apple's Face ID program allows users to unlock their iPhone or iPad Pro, authorize purchases from the iTunes Store and App Store, and make purchases through Apple Pay. *See id.* Developers may also choose to allow users to sign into their apps using Face ID technology. *See id.*

[145] *Id.*

[146] *Id.*

[147] *Id.* (noting further that Face ID uses the most advanced hardware and software Apple has ever created); *see* Taylor, *supra* note 45.

[148] *About Face ID Advanced Technology*, *supra* note 144.

[149] *Id.*

methods for that data known to the public.[150] For example, Apple's Secure Neural Engine creates a mathematical representation of a user's face by converting two-dimensional images and depth maps.[151] Furthermore, Apple built in precautionary measures to ensure the security and protection of a user's sensitive information in case parts of the operating system, such as the Application Processor kernel, are ever compromised.[152] Apple is able to do this through its Secure Enclave, a hardware feature "isolated from the main processor."[153] Apple similarly protects users' biometric information through forging a secure connection between the Secure Enclave and the biometric sensors.[154] It does so by dividing the responsibilities between them: the sensor captures the biometric information, then transmits it to the Secure Enclave which "processes, encrypts, and stores the corresponding Touch ID and Face ID template data."[155] When the user then wants to unlock his or her phone, the Secure Enclave compares the stored template with the current data from the biometric sensors to determine whether there is a valid match before unlocking the device.[156] Likewise, Apple's Touch ID—which allows users to unlock their devices with a fingerprint—operates via an analysis which "uses subdermal ridge flow angle mapping, a lossy process that discards 'finger minutiae data' that would be required to reconstruct the user's actual fingerprint" to help ensure the data's security.[157] Additionally, Apple does not receive the fingerprint information collected through this process, nor is it included in device backups.[158]

B. *Amazon's Use of Biometric Information*

Amazon is one of the many companies capitalizing on the increase in use and sophistication of biometric data collection through its Amazon Rekognition program which can "identify objects, people, text, scenes, and activities in images and videos, as well as detect any inappropriate

---

[150] *Id.* (describing its technology, security measures, privacy, safety, and accessibility regarding Face ID on its website).

[151] *Secure Enclave*, APPLE (May 17, 2021), https://support.apple.com/guide/security/secure-enclave-sec59b0b31ff/web.

[152] *Id.*

[153] *Id.*

[154] *Face ID Security and Touch ID Security*, Apple (Feb. 18, 2021), https://support.apple.com/guide/security/touch-id-and-face-id-security-sec067eb0c9e/1/web/1.

[155] *Secure Enclave*, *supra* note 151.

[156] *Id.*

[157] *Id.*

[158] *Id.*

content."[159] More specifically, the program "provides highly accurate facial analysis and facial search capabilities that [individuals] can use to detect, analyze, and compare faces for a wide variety of user verification, people counting, and public safety use cases."[160] The program works by using an algorithm to detect and extract the facial features of each face into a feature vector, which it stores in a backend database.[161] Then, the feature vectors created by the program are used to recall and perform face match and search procedures through the SearchFaces and SearchFacesByImage operations.[162] With the facial information now stored in the database, users can then search within a collection "for known faces in images, stored videos, and streaming videos."[163]

However, Amazon's use of biometric information extends beyond use to the general public—it provides the government with facial recognition technology, and "pushe[s] Rekognition as a tool for monitoring 'people of interest' and double[s] down on providing other surveillance technologies to governments."[164] The Washington County Sheriff's Office was the first law enforcement agency in the country to use Rekognition to help identify suspects in criminal investigations.[165]

---

[159] *Amazon Rekognition (AMS SSPS)*, AMAZON, https://docs.aws.amazon.com/managedservices/latest/userguide/rekognition.html (last visited Nov. 7, 2021).

[160] *Id.* (alteration in original).

[161] *What is Amazon Rekognition?*, AMAZON, https://docs.aws.amazon.com/rekognition/latest/dg/API_IndexFaces.html (last visited Nov. 7, 2021).

[162] *Id.*

[163] *Searching Faces in a Collection*, AMAZON, https://docs.aws.amazon.com/rekognition/latest/dg/collections.html?pg=ln&sec=ft (last visited Nov. 7, 2021).

[164] Karen Hao, *The Two-Year Fear Fight to Stop Amazon from Selling Face Recognition to the Police*, MIT TECH. REV. (June 12, 2020), https://www.technologyreview.com/2020/06/12/1003482/amazon-stopped-selling-police-face-recognition-fight/. The author notes the controversial issues surrounding Amazon's facial recognition technology and how it aids in tracking and deporting immigrants and encourages racial biases in facial recognition technology in general. The author further discusses the inaccuracies when identifying darker-skinned women found in MIT's 2018 Gender Shades study. *See also* Vance v. Amazon.com Inc., 525 F. Supp. 3d 1301, 1306 (W.D. Wash. 2021) (emphasizing how Amazon is "'the largest provider of facial recognition technology to law enforcement agencies,' including ICE, the FBI, and more than 1,300 law enforcement agencies" across the country).

[165] *See* Drew Harwell, *Oregon Became a Testing Ground for Amazon's Facial-Recognition Policing. But What if Rekognition Gets it Wrong?*, WASH. POST (Apr. 30, 2019),

However, in June of 2020, it stopped using the program amid concerns from its community and Amazon itself.[166] Furthermore, Ring, a subsidiary of Amazon, partnered "with more than 1,300 law enforcement agencies to use footage from its home security cameras in criminal investigations."[167] While user-friendliness is typically a good thing, in the context of Amazon's Rekognition program, the ease of activating an account—without major technical infrastructure—and the accessibility to "virtually anyone" at extremely affordable rates is concerning given the program's power.[168]

Amazon is also expanding its use of biometric data through its Amazon One program that allows customers to pay checkout-free with a palm print scan.[169] The scanner captures details of customer's palm such as "lines and ridges as well as subcutaneous features such as vein patterns."[170] Amazon markets this program as a quick, easy, and contact-free way to "make a payment, enter a venue, or identify yourself" by linking the customer's palm print scan with his or her payment and contact information.[171] Furthermore, Amazon can indefinitely store customer palm prints in the cloud unless users opt to delete them after all transactions are complete; otherwise, they are deleted if the feature is not used for two years.[172] That being said, Amazon reserves the right to "change, suspend, or discontinue the Service, or any part of it, at any time

---

https://www.washingtonpost.com/technology/2019/04/30/amazons-facial-recognition-technology-is-supercharging-local-police/ (further addressing concerns that police use of Rekognition could result in innocent people being arrested for crimes they did not commit due to inaccuracies in the program); *Facial Recognition Technology*, Wash. Cnty. Sheriff's Office (June 10, 2020), https://www.co.washington.or.us/sheriff/CrimePrevention/facial-recognition-technology.cfm.

[166] *Id*.

[167] Hao, *supra* note 164.

[168] *See* Harwell, *supra* note 165. During the time the Washington County Sheriff's Department used Amazon's Rekognition program, it only paid a mere $7 a month for the service and an initial charge of $700 for its first large photo upload.

[169] *How It Works: Meet Amazon One*, AMAZON, https://one.amazon.com/how-it-works (last visited Nov. 6, 2021); *see* Zach Whittaker, *Amazon Will Pay You $10 in Credit for Your Palm Print Biometrics*, TECHCRUNCH (Aug. 2, 2021, 11:49 AM), https://techcrunch.com/2021/08/02/amazon-credit-palm-biometrics/.

[170] *Id.*

[171] *Id.*

[172] *Amazon One Terms of Use*, AMAZON, https://one.amazon.com/terms-of-use (last updated on May 18, 2021); Whittaker, *supra* note 169.

without notice."[173] These are the terms of Amazon One which the user consents to if he or she continues to use the service after the new terms are put in effect.[174]

C. *Clearview*

Clearview is an artificial intelligence (AI) tech startup known in the biometric privacy arena largely surrounding the many lawsuits against it for violating various privacy laws both in the United States and abroad. This privately owned American company "created an app that enables law enforcement agencies to match photographs to its database of over 3 billion photos scraped from millions of public websites including Facebook, YouTube, Twitter, Instagram, and Venmo."[175] However, just because Clearview is scraping data from these companies does not mean the companies approve of Clearview's actions.[176] In fact, Facebook, LinkedIn, Twitter, and YouTube, among other companies, have all demanded that Clearview "stop its invasive practices and delete the scraped images," although Clearview has yet to meet their demand.[177] Additionally, the facial recognition software Clearview is attempting to

[173] *Amazon One Terms of Use*, *supra* note 172.

[174] *Id*.

[175] Ronald Bailey, *Facial Recognition and the Danger of Automated Authoritarianism*, REASON (Jan. 21, 2020, 3:10 PM), https://reason.com/2020/01/21/facial-recognition-and-the-danger-of-automated-authoritarianism/ (illustrating as a frame of reference for the vast amount of photos Clearview has, the FBI only has 640 million images in its database); *see also Company Overview*, CLEARVIEW AI, https://www.clearview.ai/overview (last visited Feb. 7, 2022). At the time of the quoted article's publication in January 2020, Clearview only had 3 billion images; however, in an interview in October 2021, the company's co-founder and CEO, Hoan Ton-That, revealed that the number of images Clearview collected from across the web had more than tripled to include over 10 billion images. *See* Will Knight, *Clearview AI Has New Tools to Identify You in Photos*, WIRED (Oct. 4, 2021, 7:00 AM), https://www.wired.com/story/clearview-ai-new-tools-identify-you-photos/.

[176] *See* J.D. Tuccille, *Lawsuit Challenges Clearview's Use of Scraped Social Media Images for Facial Recognition*, REASON (Mar. 15, 2021, 8:45 AM), https://reason.com/2021/03/15/lawsuit-challenges-clearview-use-of-scraped-social-media-images-for-facial-recognition/; *see also* Thornley v. Clearview AI, Inc., 984 F.3d 1241, 1242–43 (7th Cir. 2021) (noting how "Clearview uses a proprietary algorithm to 'scrape' pictures from social media sites such as Facebook, Twitter, Instagram, LinkedIn, and Venmo" with all publicly available materials).

[177] Tuccille, *supra* note 176176.

develop would allow users wearing augmented reality glasses to identify people in public in real-time, which could lead to new privacy concerns.[178]

VI. WHAT BUSINESSES SHOULD DO

With respect to the CCPA and CPRA, businesses should first and foremost check and see if their company falls within the scope of what the Acts define as a "business" to determine whether or not they will be bound by them.[179] Additionally, businesses should check if California residents—or Illinois residents under the BIPA[180]—use their company's goods or services because the Acts only protect California residents.[181] Next, businesses should determine if the information they collect on consumers falls within the scope of protected information.[182] If an entity is the correct business type, deals with consumers with the correct state residency, and collects the type of information protected under the Act, then that entity meets the baseline requirements to be bound by the CCPA or CPRA and should begin monitoring its actions and adjusting them to meet the protocols set forth in the Acts.[183] Businesses should establish clear notice to consumers, prior to or at the time of collecting their information, and identify the categories of information it plans on collecting along with the purpose for collecting said information.[184]

---

[178] *See* Bailey, *supra* note 175.

[179] *See* CAL. CIV. CODE § 1798.140(c) (West 2020) (noting how the CCPA is effective from January 1, 2020 to December 31, 2022); CAL. CIV. CODE § 1798.140(d) (West 2020) (effective Jan. 1, 2023). Again, although referred to as two separate acts, the CPRA is an amendment—whose provisions will begin taking effect January 1, 2023—to the CCPA, whose regulations are currently active until December 31, 2022. *See CCPA vs. CPRA: What's the Difference?*, *supra* note 118.

[180] Christina Lamoureux & Kristin L. Bryan, *Another Federal Court Allows BIPA Claims to Proceed, Finding State of Mind Allegations Not Necessary for Plaintiff's Claim*, NAT'L L. REV. (Oct. 13, 2021), https://www.natlawreview.com/article/another-federal-court-allows-bipa-claims-to-proceed-finding-state-mind-allegations.

[181] *See* CAL. CIV. CODE § 1798.140(i) (West 2020) (defining consumer as a "natural person who is a California resident").

[182] *See id.* at § 1798.140(b) (West 2020); *id.* at § 1798.140(c) (West 2020) (effective Jan. 1, 2023); *see also* 740 ILL. COMP. STAT. ANN. 14/10 (defining what personal information is considered "biometric information" or a "biometric identifier" under the BIPA).

[183] *See* CAL. CIV. CODE §§ 1798.100(a)–(b) (West 2020) (effective Jan. 1, 2023).

[184] *See* CAL. CIV. CODE § 1798.100(b) (West 2020). The CPRA also added that businesses must share if the collected information will be shared or sold and the amount of time the business plans on retaining each category of

Furthermore, now that the CPRA has come into effect, third parties, service providers, or contractors that a business shares a consumer's personal information with must enter into an agreement with the business specifying that the personal information was disclosed or sold for a limited purpose and obligating the third party, service provider, or contractor to adhere to the terms of the CPRA and provide the same level of privacy the Act requires.[185]

The CCPA and CPRA also give consumers more control over their personal information and businesses must be ready to respond to those requests appropriately.[186] For instance, consumers may choose to exercise their right under the Acts and request a business delete the personal information it collected on them, so businesses must be equipped with a certain process to be able to comply with those types of requests.[187] Businesses should also be prepared to locate and retrieve specific pieces of a consumer's personal information the business collected since the CCPA and CPRA grant the consumer the right to request that.[188] Furthermore, to stay in compliance with the CCPA and CPRA, businesses that collect or share consumers' personal information with third parties must give consumers the opportunity to opt-out of having their information sold or shared by the business and provide notice of such practices.[189] Businesses must also "maintain reasonable security

---

personal information. *See* CAL. CIV. CODE §§ 1798.100(a)–(b) (West 2020) (effective Jan. 1, 2023).

[185] *See* CAL. CIV. CODE § 1798.100(d) (West 2020) (effective Jan. 1, 2023).

[186] *California Consumer Privacy Act (CCPA)*, State of California Department of Justice (last updated Jan. 20, 2023), https://oag.ca.gov/privacy/ccpa.

[187] *See* CAL. CIV. CODE § 1798.105(a) (West 2020); *see also* CAL. CIV. CODE § 1798.105(c)(3) (West 2020) (effective Jan. 1, 2023) (requiring service providers and contractors to comply with a consumer's request for the deletion of his or her information as well unless the consumer directly made the request to the service provider or contractor for the personal information it collected on the consumer in its "role as a service provider or contractor to the business"). Businesses have a default of forty-five days from the date of receipt to comply with a verifiable consumer request, so it is important they store and can access and deliver the requested information within that timeframe. *See* CAL. CIV. CODE § 1798.130(a)(2) (West 2020).

[188] *See* CAL. CIV. CODE § 1798.110(c)(5) (West 2020)(effective Jan. 1, 2023).

[189] *See* CAL. CIV. CODE §§ 1798.120(a)–(b) (West 2020) (effective Jan. 1, 2023) (expanding the notice requirement and choice to opt-out for businesses sharing consumers' personal information and not just for businesses selling it).

procedures and practices appropriate to the nature of the information" which is not specifically defined in the CCPA but is likely a high standard given the permanent and unchangeable nature of consumers' biometric information.[190]

VII. CONCLUSION

While the use of individuals' biometric data is not a new development, its increasing sophistication and widespread use necessitates restrictions on its collection in order to protect the general public.[191] Illinois led the path for these protective measures by being the first state to enact protocols specifically regarding biometric information with its innovative Illinois Biometric Privacy Act.[192] Following Illinois' lead, California enacted an even broader set of regulations under the California Consumer Privacy Act, which Californians voted to further develop and amend with the California Rights Privacy Act, which took effect January 1, 2023.[193] These guidelines hold businesses to a higher standard of care surrounding individuals' biometric information and require an increased level of transparency regarding when a business collects information, how it collects it, the purpose of its collection, and how it will store and eventually dispose of that information.[194]

While beneficial to the general public, who now have more control over their biometric information than before, businesses must take extra steps in order to avoid liability under the respective Acts.[195] All businesses collecting personal information or considering collecting personal information should take note of the changing landscape regarding biometric information.[196] This is also true for entities that do not operate

---

However, businesses cannot share the personal information of minors they know to be under sixteen years old without affirmative consent and of minors under thirteen years old without the consent of their parent or guardian. CAL. CIV. CODE § 1798.120(c) (West 2020).

[190] *See* CAL. CIV. CODE § 1798.81.5(c) (West 2022); *The California Consumer Privacy Act and 'Reasonable Security': A Game Changer*, MCDERMOTT WILL & EMERY (Jan. 9, 2020), https://www.mwe.com/insights/the-california-consumer-privacy-act-and-reasonable-security-a-game-changer/.

[191] *See* 740 ILL. COMP. STAT. ANN. 14/5 §§ 5(f)–(g).

[192] *See* Ward & Boehm, *supra* note 74.

[193] *See* Alysa Hutnik & Alexander Schneider, *CPRA Update: How to Prepare for Privacy Compliance as an Employer*, KELLEY, DRYE, & WARREN LLP (June 21, 2021), https://www.adlawaccess.com/2021/06/articles/cpra-update-how-to-prepare-for-privacy-compliance-as-an-employer/.

[194] *Id.*

[195] *Id.*

[196] *Id.*

in Illinois or California since they may be bound by the CCPA, CPRA, or BIPA by interacting with those states' residents or as a precautionary measure in case their state enacts similar protocols building off other Illinois or California's current laws.[197] Ultimately, the increased use of biometric data has led states to impose restrictions on businesses collecting their residents' biometric information, giving more power to the people and creating more limitations and regulations those businesses must be aware of and abide by.

[197] *See* CAL. CIV. CODE § 1798.140(g) (West 2020); Lamoureux & Bryan, *supra* note 180; *see also* Ward & Boehm, *supra* note 74 (noting how several states have adopted or are in the process of enacting their own privacy regulations based on Illinois' BIPA).