ARTICLES

PRIVACY PROTECTION THROUGH PUBLICITY: LICENSING ONES LIKENESS TO EMPLOYERS VIA BIOMETRICS

*Peter D. Haas**

Table of Contents

* J.D. Candidate, December 2025, Loyola University Chicago School of Law; Associate Editor, *Loyola Law Journal of Regulatory Compliance*; M.S. in Cybersecurity, Utica University; B.A. in Intelligence Studies, American Military University; Certified Information Systems Security Professional (CISSP); Certified Fraud Examiner (CFE); US Army Veteran. I am deeply grateful to Atanu Das for his invaluable support and guidance in the development of this Article.

I. INTRODUCTION

While we, as a People, may disagree on what it is, privacy remains an essential human right.[1] That right erodes as our society evolves: traded in for the need for security and the desire for convenience.[2] With the advent of digital technology comes new ways to identify individual people and new ways that we allow

[1] *See Human Rights and Privacy*, ACLU, https://www.aclu.org/issues/human-rights/human-rights-and-privacy (last visited Mar. 14, 2025).

[2] *See* Alan L. Zegas, *Coming Soon: The Thought Police*, N.J. LAW., THE MAG., Oct. 2009, at 57, 58, 60.

others to invade our privacy, often without knowing what we have given up or fully appreciating the value attached to it.[3]

"Historically, privacy was almost implicit, because it was hard to find and gather information. But in the digital world, whether it's digital cameras or satellites or just what you click on, we need to have more explicit rules—not just for governments but for private companies."[4] Reduced privacy in the interest of security, concededly, is a valid tradeoff when the competing interests are appropriately balanced.[5] Security should only come at the expense of privacy when necessary.[6] Balancing security and privacy requires rules: rules which are emerging across the United States and across the world.[7] Regulations like the General Data Protection Regulation (GDPR) in the European Union[8] and the Biometric Information Privacy Act (BIPA) in Illinois[9] are early and promising models of individual privacy protection legislation.

People must also become more alert and capable of exercising their right to privacy. For example, had the public known the underlying cost of their "free" social network sites was the prospect of revealing their entire identity, friends, family, habits, and maybe even their secrets,[10] they may have balked at the services

---

[3] *See id.* at 58–60; Jana McGowen, *Your Boring Life, Now Available Online: Analyzing Google Street View and the Right to Privacy*, 16 TEX. WESLEYAN L. REV. 477, 478 (2010).

[4] Richard Kam, *Internet of Things Makes Big Data Even Bigger (and Riskier),* IAPP (Apr. 25, 2016), https://iapp.org/news/a/internet-of-things-makes-big-data-even-bigger-and-riskier (quoting Bill Gates on balancing surveillance and security in the digital era).

[5] *See* Katie Vloet, *Tension: Privacy vs. National Security in the Digital Age*, LAW QUADRANGLE: NOTES FROM MICH. L., Fall 2016, at 20 (discussing the importance of balancing security and privacy).

[6] *See id.* at 21.

[7] *See, e.g.*, *infra* notes 8–9 and accompanying text; Andrew Folks, *U.S. State Privacy Legislation Tracker*, IAPP (July 22, 2024), https://iapp.org/resources/article/us-state-privacy-legislation-tracker (tracking the recently proposed and enacted comprehensive privacy bills across the United States).

[8] Council Regulation 2016/679 of Apr. 27, 2016, on the Protection of Natural Persons with Regard to the Processing of Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1 [hereinafter GDPR].

[9] Biometric Information Privacy Act [BIPA], 740 ILL. COMP. STAT. 14 (2008).

[10] *See* Kalev Leetaru, *Social Media Companies Collect So Much Data Even They Can't Remember All the Ways They Surveil Us,* FORBES (Oct. 25, 2018, 12:54 PM), https://www.forbes.com/sites/kalevleetaru/2018/10/25/social-media-companies-collect-so-much-data-even-they-cant-remember-all-the-ways-they-surveil-us/ (discussing the large amount of data that companies collect from users without their knowledge).

offered.[11] Unfortunately, many people are not equipped to identify or understand the amount or manner of surveillance pursuing them.[12] Even if a person is well-equipped, they may have little practical choice in allowing the privacy intrusions, particularly surveillance in the workplace.[13]

Employers may reasonably surveil their employees within the confines of the workplace,[14] but that should be the extent of their surveillance and the limit of their claim over their employees' identity and privacy. Companies currently track their employees in a variety of ways.[15] For example, workplace wellness programs often collect employees' biometric data outside the scope of the current protections supposedly provided by the Health Insurance Portability and Accountability Act (HIPAA), unbeknownst to many participating employees.[16]

Some employers are looking to use facial recognition software as replacements for identification badges or for identifying visitors

---

[11] *See generally Transcript of Mark Zuckerberg's Senate Hearing,* WASH. POST: THE SWITCH (Apr. 10, 2018, 10:25 PM), https://www.washingtonpost.com/news/the-switch/wp/2018/04/10/transcript-of-mark-zuckerbergs-senate-hearing (transcript of congressional hearing on Facebook's non-transparent polices that users are unaware of); Debbie Dingell, *Dingell Questions Facebook CEO Mark Zuckerberg,* YOUTUBE (Apr. 11, 2018), https://www.youtube.com/watch?v=KQcIMhnI91E (Rep. Debbie Dingell questioning Zuckerberg's knowledge on Facebook's transparency at a hearing of the House Energy and Commerce Committee).

[12] *See* David Lyon, *Surveillance, Power and Everyday Life*, *in* OXFORD HANDBOOK INFO. & COMMC'N TECHS. 449, 465 (Chrisanthi Avgerou et al. eds., 2009) ("While common prudence may be expected, to assume that ordinary people have the time, expertise, or motivation to be constantly vigilant about surveillance is to sidestep questions of justice and informational fairness.").

[13] Elizabeth A. Brown, *A Healthy Mistrust: Curbing Biometric Data Misuse in the Workplace*, 23 STAN. TECH. L. REV. 252, 284 (2020) ("Even when workers are aware of the risks that health data collection presents, they may be unable or unwilling to protest for practical reasons. Most people do not have an infinite choice of employment."); *see also* discussion *infra* Section VI.A (addressing the power imbalance between employees and employers).

[14] O'Connor v. Ortega, 480 U.S. 709, 717 (1987); *see also* Vega-Rodriguez v. P.R. Tel. Co., 110 F.3d 174, 184 (1st Cir. 1997) ("Because [employees] do not have an objectively reasonable expectation of privacy in the open areas of their workplace . . . video surveillance conducted by their employer does not infract their federal constitutional rights.").

[15] *See, e.g.*, *supra* note 14 and accompanying text; Soojin Jeong, *Could Biometric Tracking Harm Workers?*, REGUL. REV. (Dec. 9, 2021), https://www.theregreview.org/2021/12/09/jeong-could-biometric-tracking-harm-workers (discussing employers' collection of biometric data through wearable devices implemented as part of wellness programs).

[16] *See* Brown, *supra* note 13, at 290–94.

entering onto their property.[17] To implement such identification programs, employers would require the means to collect, store, and use the identifiable features of anyone who may enter their property.[18] Such use of biometrics (e.g., facial geometry) should be governed by biometric laws, but biometric laws are only recently receiving attention,[19] with the Biometric Information Privacy Act (BIPA) being the most prominent American legislation in this area.[20] For many employees, employers collecting, storing, and using their biometric identifiers for the purposes of running the company's business infringes too far upon their privacy rights by way of their identity.[21]

Biometric laws concerning the employer-employee relationship

---

[17] Mike Rogoway, *Major Tech Company Using Facial Recognition to ID Workers,* OREGONIAN (Mar. 11, 2020), https://www.govtech.com/public-safety/major-tech-company-using-facial-recognition-to-id-workers.html (describing Intel's developing use of employee biometrics via facial recognition scans and "biometric templates" to monitor workers and visitors); *see also* LEE RAINIE ET AL., PEW RSCH. CTR., AI IN HIRING AND EVALUATING WORKERS: WHAT AMERICANS THINK 42 (Apr. 2023), https://www.pewresearch.org/wp-content/uploads/sites/20/2023/04/PI_2023.04.20_AI-in-Hiring_FINAL.pdf (identifying uses of facial recognition technology in the workplace, including tracking workers' clock ins and outs, screening candidates during hiring processes, and monitoring employee productivity).

[18] *See e.g.*, Rogoway, *supra* note 17 ("Intel says it will hold former workers' facial information for two years after they leave the company. It will retain most visitors' faces for 30 days, but will keep data on visitors who are denied access to a site for 30 years."); Brown, *supra* note 13, at 253–57 (discussing how employers collect and use employees' biometrics).

[19] *See, e.g.*, Charles N. Insler, *How to Ride the Litigation Rollercoaster Driven by the Biometric Information Privacy Act*, 43 S. ILL. U. L.J, 819, 819–22 (2019) (discussing how, despite BIPA's enactment in 2008, Illinois has only recently seen a surge of litigation that allege a BIPA violation as an underlying cause of action against employers); *see also* Folks, *supra* note 7 (tracking "proposed and enacted comprehensive privacy bills from across the United States" and noting that "[s]tate-level momentum for comprehensive privacy bills is at an all-time high").

[20] BIPA, 740 ILL. COMP. STAT. 14 (2008); *see also Is Biometric Information Protected by Privacy Laws?*, BL (June 20, 2024), https://pro.bloomberglaw.com/insights/privacy/biometric-data-privacy-laws/#bipa (discussing how BIPA, Illinois' biometric privacy law, was the first state privacy law of its kind and remains the most comprehensive in its creation of a private cause of action).

[21] *See* Emily Harmon, Comment, *Out of Hand: Why Federal Protection of Biometric Privacy is a Pressing Issue in U.S. Employment*, 24 WYO. L. REV 602, 609–10, 621–623 (2024) ("[T]he law must acknowledge the many reasons employees may opt-out of the collection of their biometric data."); *see also* Insler, *supra* note 19, at 819–20 ("Biometric data . . . is the most sensitive data belonging to an individual."); *see also* Figueroa v. Kronos Inc., 454 F. Supp. 3d 772, 780–81 (N.D. Ill. 2020).

are sparse.[22] The majority of existing legislation focuses on providing notice of collection and in obtaining consent, and do not offer much in terms of addressing the imbalance between an employer and employee.[23] Even proposed changes to BIPA would allow for the collection of biometric signatures "under certain circumstances relating to security purposes."[24] Under the ambiguous justification of security, companies could be permitted to collect biometrics from everyone if biometric privacy laws are amended or designed to incorporate such vague language.[25]

This Article proposes an alternative approach, one which would permit a company to collect and use the biometric signatures of its employees while providing employees adequate safeguards and assurances for their privacy beyond their employment.[26] The suggested approach advocates the premise that biometric signatures are within the definition of one's likeness, and that employees may therefore license their biometric signatures to their employers for a particular set of purposes (e.g., security).[27] Under the suggested approach, obtaining a license from an employee would require appropriate notice and informed consent

---

[22] *See Employment, Comparison Table – State Biometric Laws, Employment Context*, BL: PRACTICAL GUIDANCE, https://www.bloomberglaw.com/document/XF7V5OC8000000 (last visited Nov. 9, 2024) ("California, Illinois, New York, Oregon, and Texas have privacy or labor laws that contain specific requirements for employers who collect biometric identifiers from their employees. Colorado, Utah [effective Dec. 31, 2023], Virginia, and Washington have comprehensive privacy laws that refer to biometrics generally but are limited in their applicability in the employment context."); *see also* Lauren Caisman & Amy de La Lama, *U.S. Biometric Laws & Pending Legislation Tracker - June 2023*, JD SUPRA (Jun. 5, 2023), https://www.jdsupra.com/legalnews/u-s-biometric-laws-pending-legislation-1029655/ (providing "a high-level summary of existing laws and proposed bills introduced across the country that pertain to private sector companies' collection or use of biometric data").

[23] *See Employment, Comparison Table*, *supra* note 22.

[24] *See* H.B. 5365, 103rd Gen. Assemb., Reg. Sess. (Ill. 2024) (excepting BIPA requirements on collection of biometric information for a security purpose, defining "security purpose" as "means for the purpose of preventing or investigating retail theft, fraud, or any other misappropriation of a thing of value. 'Security purpose' includes protecting property from trespass, controlling access to property, or protecting any person from harm, including stalking, violence, or harassment, and includes assisting a law enforcement investigation.").

[25] *See id.*

[26] *See* discussion *infra* Parts V–VI (arguing that all citizens have a right to license their likeness and proposing scheme to allow employees to license their likeness to employers).

[27] *See* discussion *infra* Parts VI–VII.

on the collection, use, and disposal of their biometric signatures.[28] This Article additionally proposes certain requirements that legislation should adopt to rebalance the dynamic between employer and employee within the scope of biometric licensure consent.[29] The licensure and legislative approaches adopted in this Article provide more protections and leverage to employees, give employers an avenue to achieve its security and other purposes, and remain aligned with existing legislation.[30]

II. EVOLVING STATE OF PRIVACY IN THE UNITED STATES

Privacy, as a right, evolves closely with the evolution of technology.[31] As new innovations emerge—new methods and capabilities that can both benefit and surveil society—so too do the ways that society thinks about privacy.[32] Much of how the United States thinks of privacy today stems from its understanding of the Fourth Amendment: how technology has refined what is considered a search or intrusion by a government entity, and how that same technology may be employed to exploit one's privacy by non-government entities, service providers, and employers alike.[33]

United States' privacy law evolved to reflect that not everything we send out into the world is protected by a reasonable expectation of privacy.[34] When telephones were a growing commodity, for

---

[28] *See* discussion *infra* Part VI.

[29] *See* discussion *infra* Section VI.B.

[30] *See* discussion *infra* Part VI.

[31] Urs Gasser, *Recoding Privacy Law: Reflections on the Future Relationship Among Law, Technology, and Privacy*, 130 HARV. L. REV. F. 61, 61–64 (2016) ("The history of privacy is deeply intertwined with the history of technology.").

[32] *See id.* at 61–62 (discussing how advancements in information and communication technology and other similarly invasive practices "challenged existing notions of privacy and led to renegotiations of boundaries between the private and public spheres"); *see also* Lyon, *supra* note 12, at 455–57 ("It is not merely that more data circulate in numerous administrative and commercial systems, but that ways of organizing daily life are changing as people interact with surveillance systems.").

[33] *See supra* note 14 and accompanying text; *see also* United States v. Meregildo, 883 F. Supp. 2d 523, 525–26 (S.D.N.Y. 2012) (holding that Defendant had no reasonable expectation of privacy to a post he made on his profile; thus, law enforcement did not violate the Fourth Amendment when a cooperating "Facebook friend" gave officers access to the Defendant's Facebook profile).

[34] *See, e.g.*, *Meregildo*, 883 F. Supp. 2d. at 525–26 ("When a social media user disseminates his postings and information to the public, they are not protected by the Fourth Amendment.") (citing Katz v. United States, 389 U.S. 347, 351 (1967)); Christopher F. Carlton, *The Right to Privacy in Internet Commerce: A Call for New Federal Guidelines and the Creation of an Independent Privacy Commission*, 16 ST. JOHN'S J.L. COMM. 393, 398–400 (2002) (discussing the

example, wiretaps emerged as a way to intercept "private" conversations between individuals.[35] When confronted with the question whether wiretapping telephones was a permissible privacy intrusion under the Fourth Amendment, the Supreme Court answered in the affirmative, because "one who installs in his house a telephone instrument with connecting wires intends to project his voice to those quite outside, and that the . . . messages . . . are not within the protection of the Fourth Amendment."[36] This decision represented a departure from the protection granted to traditional sealed letters, which could only be "opened and examined" pursuant to a valid warrant.[37] However, recognizing the potential for disagreement, the Court invited Congress to protect the secrecy of telephone messages through direct legislation so long as the law would not create an "enlarged and unusual meaning of the Fourth Amendment."[38]

The idea of privacy and freedom from intrusion was further refined with the introduction of the telephone booth.[39] Telephone booths provide an area within a public place where a caller may enter, close the door, and hold a conversation without it being overheard.[40] The Supreme Court, in its reasoning, emphasized that the Fourth Amendment "protects people, not places,"[41] and held: "What a person *knowingly* exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he *seeks to preserve as private*, even in an area accessible to the public, may be constitutionally protected."[42]

By entering the phone booth and closing the door, the caller manifested a reasonable expectation of privacy from eavesdroppers.[43] Attaching a recording device to the outside of the phone booth violated that reasonable expectation of privacy as

development of privacy rights and exceptions to the "reasonable expectation of privacy" established in *Katz*).

[35] *See Wiretapping*, ELEC. PRIV. INFO. CTR., https://epic.org/issues/surveillance-oversight/wiretapping/ (last visited Sept. 17, 2024).

[36] Olmstead v. United States, 277 U.S. 438, 466 (1928).

[37] *Id*. at 460 (citing Weeks v. United States, 232 U.S. 383 (1914)).

[38] *Id*. at 465–66.

[39] *See* Katz v. United States, 389 U.S. 347, 353 (1967) (holding that surveillance of defendant petitioner inside telephone booth constituted invasion of privacy in violation of the Fourth Amendment).

[40] *See Katz*, 389 U.S. at 352.

[41] *Id.* at 351.

[42] *Id*. (emphasis added).

[43] *See id.* at 352 (A person "who occupies [a telephone booth], shuts the door behind him, and pays the toll . . . is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world.").

protected by the Fourth Amendment, even without a physical entrance into the phone booth.[44] The Supreme Court in *Katz v. United States* ultimately concluded that intrusion by electronic means onto conversations one reliably seeks to keep private, even when the intrusion is accomplished without physical trespass, may constitute a search within the meaning of the Fourth Amendment.[45]

As technology has progressed, certain innovations have become ubiquitous in our society, including cell phones, wireless devices, GPS navigation systems, and closed-circuit television (CCTV).[46] These advancements and the prevalence of technology in society challenges whether this pervasive surveillance capability is one where the public must trade privacy for convenience and security that such technology provides.[47]

Modern cell phones have become so ingrained in our daily lives that "the proverbial visitor from Mars might conclude they were an important feature of human anatomy."[48] Cell phones contain information limited only by their local capacity, and, even with that limit, may access data stored elsewhere via remote connections.[49] A person may store their entire life within the contents of a smart phone and its connected devices. Cell phones contain a person's Internet browsing history, their private interests, and their secrets, and are kept within arm's reach of a person, accompanying them everywhere the person goes, even to the bathroom.[50] These same devices track the very location of the person, second by second.[51] Cell phones' location tracking capacities are extremely precise due to the combination of the

---

[44] *Id.* at 352–53, 359.

[45] *Id.* at 353.

[46] *See* United States v. Jones, 565 U.S. 400, 428 (2012) (Alito, J., concurring) (discussing the recent emergency of devices that permit the monitoring of a person's movement, including closed-circuit television video monitoring, GPS devices, cell phones, and smart phones).

[47] *See id.* at 427 (Alito, J., concurring) ("New technology may provide increased convenience or security at the expense of privacy, and many people may find the tradeoff worthwhile. And even if the public does not welcome the diminution of privacy that new technology entails, they may eventually reconcile themselves to this development as inevitable."); *see also* Zegas, *supra* note 2, at 58.

[48] Riley v. California, 573 U.S. 373, 385 (2014).

[49] *See generally What is Remote Access and How Does it Work?*, REALVNC: BLOG (May 25, 2023), https://www.realvnc.com/en/blog/remote-access/ ("[Remote access technology] allows users to efficiently manage files and data stored on remote devices, simplifying complex tasks.").

[50] *Riley*, 573 U.S. at 395.

[51] *See* Carpenter v. United States, 585 U.S. 296, 311–12 (2018).

various types of geolocation technology they utilize.[52] The contents of cell phones, from instant messages to location data, are "the privacies of life" and are subject to the same protections that any other information would enjoy.[53] One can gain insight into the evolution of privacy law in response to emerging technology by examining how it adapted to address issues specific to cell phones.

Not only is this expansive information contained within a cell phone, but the device's location is stored and retrievable by wireless carriers.[54] Cell-site location information (CSLI), is a pervasive tool used to triangulate the location of a cell phone, with the location information produced stored for up to five years.[55] Such technology and data, when used by law enforcement in a criminal investigation, implicates the third-party doctrine.[56] The third-party doctrine holds that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[57] Under the third-party doctrine, people who voluntarily give information to a third party have no expectation of privacy for that information.[58]

The Supreme Court extended Fourth Amendment protections to cell phones (as technology associated with personal information) in *Carpenter v. United States*.[59] *Carpenter* addressed the unnerving fact that cell phone location and movement are potentially subject to a lookback by law enforcement spanning any, or all, of the stored five years of CSLI.[60] If their access to CSLI was left unchecked, then, law enforcement could easily look back at anyone's movements, benefiting substantially from the capability of stored retrospective and encyclopedic information, and moreover delve into a person's otherwise unknowable information like their "familial, political, professional, religious, and sexual

---

[52] *Id.* at 300–01; 312–13.

[53] Riley v. California, 573 U.S. 373, 403 (2014) (citing Boyd v. United States, 116 U.S. 616, 630 (1886)).

[54] Carpenter v. United States, 585 U.S. 296, 301 (2018).

[55] *Id.* at 300–01, 312.

[56] *Id.* at 314–16 (discussing whether the third-party doctrine applies to CSLI, thereby bringing the data outside of the protection of the Fourth Amendment).

[57] Smith v. Maryland, 442 U.S. 735, 743–44 (1979); *see* United States v. Miller, 425 U.S. 435, 442–44 (1976) (holding there was "no legitimate expectation of privacy . . . [when] the documents obtained . . . contain[ed] only information voluntarily conveyed to the [third-party]").

[58] *Carpenter*, 585 U.S. at 313–14.

[59] *Id.* at 315–16 (holding that even though "the Government obtained the information from a third party . . . [t]he Government's acquisition of the cell-site records was a search within the meaning of the Fourth Amendment").

[60] *Id.* at 312.

associations."[61]

Carpenter re-emphasized the observation first made in *Riley v. California* that cell phones are almost a "feature of human anatomy."[62] As a quasi-feature of human anatomy, gathering cell phone tracking data is capable of providing an unprecedented "all-encompassing record of the holder's whereabouts," made possible only by the emergence of new technology.[63] While technology has provided a "[s]ubtler and more far-reaching means of invading privacy," courts have sought to "ensure that the 'progress of science' does not erode Fourth Amendment protections."[64]

Government policies have also evolved and shifted to address privacy issues outside criminal procedure.[65] Following the Watergate incident came the Federal Privacy Act of 1974 to establish a code of "fair information practices" governing the collection, maintenance, use, and dissemination of information about individuals.[66] Congress further regulated privacy within the specific areas of fair credit reporting,[67] cable communications,[68] and video consumers.[69] These were some of the early privacy rights intended to protect consumers, recognizing the individual's right to privacy.[70]

---

[61] *Id.* at 311.

[62] *Id.* (quoting Riley v. California, 573 U.S. 373, 385 (2014)).

[63] *Id.* at 310–11, 320 ("We decline to grant the state unrestricted access to a wireless carrier's database of physical location information. In light of the deeply revealing nature of CSLI, its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection, the fact that such information is gathered by a third party does not make it any less deserving of Fourth Amendment protection.").

[64] *Id.* at 320 (quoting Olmstead v. United States, 277 U.S. 438, 473–74 (1928) (Brandeis, J., dissenting)).

[65] *See, e.g.*, U.S. DEP'T OF JUST., OFF. PRIV. & CIV. LIBERTIES, OVERVIEW OF THE PRIVACY ACT: 2020 EDITION (2020) (summarizing the Privacy Act of 1974 and its Fair Information Practice Principles, which "allow individuals to determine what records pertaining to them are collected, maintained, used, or disseminated by an agency; require agencies to procure consent before records pertaining to an individual collected for one purpose could be used for other incompatible purposes; afford individuals a right of access to records pertaining to them and to have them corrected if inaccurate; and require agencies to collect such records only for lawful and authorized purposes and safeguard them appropriately").

[66] *Id.*; *see also* 5 U.S.C. § 552a.

[67] 15 U.S.C. §§ 1681–1681(x) (detailing privacy rights in credit and credit reports).

[68] 47 U.S.C. § 551 (requiring cable operators to provide notice to subscribers about the collection, use, and disclosure of personally identifiable information).

[69] *See* 18 U.S.C. § 2710.

[70] Christine A. Varney, Former Comm'r, Fed. Trade Comm'n., Public Statement at The Privacy & Business National Conference (Oct. 6, 1996)

The United States continues to define and regulate individual privacy rights within the private sector.[71] States like Illinois and California have enacted statutes intended to protect their residents from the misuse of their personally identifiable information (PII)—information that is both sensitive and associated with a person's identity.[72] These states recognize that control over one's PII extends from an individual's right to privacy because of what PII may divulge about them and how that information may infringe on their right to be left alone.[73] Protection of personally identifiable information requires international considerations, in part due to how the European Union enacted the European General Data Protection Regulation (GDPR) to protect the privacy of its citizens from abuses and violations by governments and private entities alike.[74]

Illinois's Biometric Information Privacy Act (BIPA) is an extensive state statute that considers biometric identifiers (e.g., retina or iris scans, fingerprints, facial geometry scans) to be a particularly sensitive form of PII with hitherto unclear detrimental impacts if compromised.[75] The California Privacy Protection Act (CPPA) also protects biometric information, defining it as "an individual's physiological, biological or behavioral characteristics . . . that is used or is intended to be used

---

(transcript available with FTC) https://www.ftc.gov/news-events/news/speeches/consumer-privacy-information-age-view-united-states.

[71] Müge Fazlioglu, *US Federal Privacy Legislation Tracker*, IAPP (Aug. 2024), https://iapp.org/resources/article/us-federal-privacy-legislation-tracker/.

[72] *See* Personal Information Protection Act, 815 ILL. COMP. STAT 530 (2017); California Consumer Privacy Act of 2018 [CCPA], CAL. CIV. CODE § 1798.100–1798.199.100 (West 2024); *see also* BIPA, 740 ILL. COMP. STAT. 14 (2008) (extending personal information protection to biometric information).

[73] *See supra* note 72 and accompanying text. *See generally* Muhammad Tariq Ahmed Khan, *Adopting Technical Controls for Data Privacy in the Digital Age*, ISACA (Nov. 4, 2021), https://www.isaca.org/resources/isaca-journal/issues/2021/volume-6/adopting-technical-controls-for-data-privacy-in-the-digital-age ("Privacy is an individual's fundamental right to have control over the collection, usage and dissemination of individuals' personally identifiable information (PII).").

[74] *Who Does the Data Protection Law Apply To?*, EUR. COMM'N, https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/application-regulation/who-does-data-protection-law-apply_en (last visited Sept. 25, 2024) (stating that the GDPR applies to a company or entity which processes "personal data as part of the activities of one of its branches established in the EU, regardless of where the data is processed" and to any company "established outside of the EU . . . offering goods/services (paid or for free) or is monitoring the behavior of individuals in the EU.").

[75] *See* BIPA, 740 ILL. COMP. STAT. 14/5–10 (2008).

singly or in combination with each other or with other identifying data, to establish individual identity."[76] The GDPR defines biometric data similarly: "[B]iometric data means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic [fingerprint] data[.]"[77]

The collection and use of biometrics are among the latest of technological advancements that go beyond the privacy concerns of a cell phone's contents or location.[78] Biometrics are becoming—and already are in certain cases—subject to the persistent monitoring in CCTV footage, facial recognition software, and artificial intelligence (AI) algorithms capable of identifying a person without their knowledge or consent.[79]

Biometric collection technology poses a serious risk to individuals' reasonable expectations of privacy and, when collected without informed consent, remove any choice they may have in the tradeoff between privacy and convenience or security.[80] Thus, control over the collection and use of biometrics should remain with the individual and only through informed consent should any entity, particularly private employers, be permitted to exercise

---

[76] CCPA, CAL. CIV. CODE § 1798.140(c) (West 2024).

[77] GDPR, *supra* note 8, art. 4, at 14.

[78] *See Biometrics and Privacy – Issues and Challenges*, OFF. VICTORIAN INFO. COMM'R (July 2019), https://ovic.vic.gov.au/privacy/resources-for-organisations/biometrics-and-privacy-issues-and-challenges/ (explaining issues related to biometric data, such as "function creep," covert or passive collection of an individual's biometric information, secondary information that can be revealed by basic biometric data like underlying health conditions, and the potential implications all have for individuals' identities).

[79] *See Understanding Artificial Intelligence: Biometrics & AI – Explained*, COMPUT. & COMMC'NS INDUS. ASS'N, https://ccianet.org/wp-content/uploads/2023/09/Biometrics_AI_Explained.pdf (last visited Sept. 26, 2024).

[80] *See* OFF. VICTORIAN INFO. COMM'R, *supra* note 78 ("If the collection of biometric information is covert or passive, individuals may be unable to provide consent or exercise control over what biometric information is collected or how it is used. The ability to provide meaningful consent is also restricted where individuals are required to participate in a biometric system, for example where it is used as a security measure to verify employees in a workplace environment."); *see also* Press Release, Fed. Trade Comm'n, FTC Warns About Misuses of Biometric Information and Harm to Consumers (May 18, 2023) (on file with author) ("[T]he increasing use of consumers' biometric information and related technologies, including those powered by machine learning, raises significant consumer privacy and data security concerns. . . .").

that control over another's biometrics.[81]

III. TENSION BETWEEN PRIVACY AND THE APPLIED USE OF BIOMETRICS

Biometrics have become an increasingly adopted mechanism for verifying the identity of a person.[82] Modern identity validation utilizes multi-factor authentication (MFA), combining at least two of the following factors: "something you know" (e.g., usernames and passwords), "something you have" (e.g., cell phones or tokens), and "something you are" (e.g., fingerprints and iris scans).[83] Within information security principles, biometrics are commonly thought to strengthen the security over the information systems implementing MFA.[84] With the increased ability to accurately identify the authorized person enabled by biometrics, the likelihood that an unauthorized user can gain access is decreased unless the unauthorized user can convincingly emulate the authorized user's unique physical traits and behaviors.[85] By

---

[81] *See Biometrics Privacy Laws: Protecting Biometric Data Across the Globe*, PRIVACYPILLAR (Oct. 15 2024), https://privacypillar.com/biometrics-privacy-laws/ ("Privacy in biometrics involves ensuring that the collection, processing and storage of biometric data respects individual rights. It means that businesses must obtain informed consent, be transparent about how the data is used and implement proper security measures to protect against data breaches and misuse.").

[82] *See* Alessandro Mascellino, *Biometric Authentication Use in US Businesses Tripled Over 3 Years to Tackle Cyber Threats*, BIOMETRICS RSCH. GRP. (Sept. 21, 2022), https://www.biometricupdate.com/202209/biometric-authentication-use-in-us-businesses-tripled-over-3-years-to-tackle-cyber-threats ("The use of biometric authentication in U.S. businesses has almost tripled from 27 percent in 2019 to 79 percent in 2022. . . .").

[83] *See, e.g.*, *Capacity Enhancement Guide: Implementing Strong Authentication*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY 2 (Oct. 8, 2020), https://www.cisa.gov/sites/default/files/2023-09/CISA_CEG_Implementing_Strong_Authentication_FINAL%20Aug-23%20Revision.pdf.

[84] *See Multi-Factor Authentication: How It Works and Why It Matters*, ARATEK (Mar. 9, 2024), https://www.aratek.co/news/multi-factor-authentication-how-it-works-and-why-it-matters ("Biometrics play a crucial role in enhancing the security and effectiveness of MFA authentication methods. By incorporating unique physical and behavioral traits into the authentication process, biometrics provide a highly secure and user-friendly method of verifying identities."); Somnath Shukla, *#CybersecurityAwarenessMonth - Multifactor Authentication (MFA): Enhancing Digital Security*, ISC2 (Oct. 18, 2023), https://www.isc2.org/Insights/2023/10/Cybersecurity-Awareness-Month-Multifactor-Authentication (explaining that biometrics, in the context of MFA, "provide a highly secure means of authentication, as they are difficult to replicate.").

[85] *See* Daniel Brecht, *Biometrics: Today's Choice for the Future of*

allowing companies to use their biometrics for authentication, the user is trading their privacy for potentially increased security of their own information and assets.[86] As biometrics are increasingly used for security purposes, however, biometric authentication methods are becoming popular targets for hackers, scammers, and other malicious actors to gain unfettered access to protected user accounts, and maybe even the user's identity.[87]

BIPA currently provides multiple layers of protection for a person's biometric data. The statute mandates that entities seeking to utilize biometrics (1) obtain a written release from the subject of the biometric identifier; (2) provide subjects with a specific purpose for the collection of biometric information; (3) establish and implement policies to safeguard the biometric identifiers; and (4) not disclose subjects' biometric identifiers to other parties under most circumstances.[88] BIPA also forbids companies from profiting from the biometric data they collect.[89] BIPA's requirements "apply to each and every collection and capture[,]" and consent for an earlier collection does not establish informed consent for later collection.[90] The collection of these biometrics do not necessarily need to come directly from their subject to trigger BIPA protections,[91] which also "appl[y] when a

Authentication, INFOSEC (Mar. 6, 2015), https://www.infosecinstitute.com/resources/general-security/biometrics-todays-choice-future-authentication/ (discussing common privacy concerns that people have regarding the collection of biometrics and how it is difficult for hackers to access the information).

[86] *See* Meredith E. Bock, *Biometrics and Banking: Assessing the Adequacy of the Gramm-Leach-Bliley Act*, 24 N.C. BANKING INST. 309, 309, 313 (2020) (discussing how banks have incorporated biometrics into their security systems to better protect consumer information in response to massive data breaches in the industry).

[87] *See* Kim Komando, *Is it Safe to Share Biometric Data? Tech Expert Weighs In*, USA TODAY (Oct. 22, 2024), https://www.usatoday.com/story/tech/columnist/komando/2024/10/17/biometric-data-hack-safe-sharing/75617507007/); *see also* Roger Grimes, *Game-Changer: Biometric-Stealing Malware*, LINKEDIN (Feb 28, 2024), https://www.linkedin.com/pulse/game-changer-biometric-stealing-malware-roger-grimes-ikaze/?trackingId=erBdiWOzxDzy%2BIeah%2F4U4g%3D%3D (describing techniques hackers use to steal a person's biometrics and how they use the information obtained).

[88] BIPA, 740 ILL. COMP. STAT. § 14/15 (2008).

[89] *Id.* § 14/15(c).

[90] Watson v. Legacy Healthcare Fin. Servs., LLC, 196 N.E.3d 571, 580 (Ill. App. Ct. 2021).

[91] *See* Vance v. Amazon.com, Inc., 525 F. Supp. 3d 1301, 1313 (W.D. Wash. 2021) ("[T]he word 'collect' carries no inherent limitation on who or where the information is collected from.").

private entity collects, captures, purchases, trades for, or gets biometric data in some other way. [Getting] the biometric data in some other way by applying for and downloading it from a corporation and then us[ing] that data . . . suffice[s] to trigger [BIPA protections]."[92]

BIPA's consent triggers may hold little weight if some of the latest proposed changes to the statute take effect. For example, Representative Jeff Keicher introduced HB 5635, which proposes amendments that would weaken BIPA's consent provisions by adding:

> A private entity may collect, capture, or otherwise obtain a person's or a customer's biometric identifier or biometric information without satisfying the requirements of subsection (b) if: (1) the private entity collects, captures, or otherwise obtains a person's or a customer's biometric identifier or biometric information for a security purpose; (2) the private entity uses the biometric identifier or biometric information only for a security purpose; (3) the private entity retains the biometric identifier or biometric information no longer than is reasonably necessary to satisfy a security purpose; and (4) the private entity documents a process and time frame to delete any biometric information used for the purposes identified in this subsection.[93]

Such a modification would allow private companies to collect biometrics under the broad justification of a "security purpose."[94] HB 5635 would define "security purpose" to include "preventing or investigating retail theft, fraud, or any other misappropriation or theft of a thing of value" and "protecting property from trespass, controlling access to property, or protecting any person from harm, including stalking, violence, or harassment . . . includ[ing] assisting a law enforcement investigation."[95] Another proposed definition of a "security purpose" would apply to uniquely online issues:

> "Security purpose" means a purpose to ensure that (i) a person accessing an online product or service is who they person claims to

---

[92] *Id.* at 1314.

[93] H.B. 5635, 103d Gen. Assemb., Reg. Sess. (Ill. 2024).

[94] *See id.*; *Biometric Information Privacy Act (BIPA)*, ACLU ILL., https://www.aclu-il.org/en/campaigns/biometric-information-privacy-act-bipa (last visited Nov. 21, 2024).

[95] H.B. 5635.

> be or (ii) a person identified as a safety concern or as a person violating the terms of use or service of the online product or service can be kept off of or denied access to the product or service.[96]

Other efforts have been made to modernize BIPA, such as by permitting electronic signatures or expanding allowable purposes, but they often come at the expense of privacy protections.[97]

Such modifications seek to trade away privacy rights for convenience and security.[98] To a certain degree, sacrificing privacy rights for convenience and security may be acceptable, but proposals like the above would enable employers to exert overwhelming and unacceptable control over employees' identities.[99] Not only would individuals lose their right to anonymity under these proposals, but they would also lose all control over their likeness—their entire identity within society—as their employers seek to exploit those likenesses for commercial gain.[100] Biometric identifiers are more than an object of authentication for the purposes of achieving an illusory semblance of security; these biometrics are "something you are"[101] and should be subject to protection from such exploitation for vague "security purposes."[102]

Security implications of biometric use have recently garnered public attention and faced substantial scrutiny.[103] Much scrutiny

---

[96] H.B. 4102, 103d Gen. Assemb., Reg. Sess. (Ill. 2023).

[97] *See id.* (bill to expand the definition of "security purpose" and create exceptions to notice and consent provisions, time retention periods, and disclosure limitations in accordance with the proposed definition); *see also* S.B. 1607, 102d Gen. Assemb., Reg. Sess. (Ill. 2021) (bill to exempt employers when using biometrics for tracking working hours, security, and human resources); *see, e.g.*, H.B. 1764, 102d Gen. Assemb., Reg. Sess. (Ill. 2021) (bill to give Attorney General of Illinois sole enforcement power over BIPA and to limit actionable harm to actual harm); H.B. 5396, 102d Gen. Assemb., Reg. Sess. (Ill. 2022) (bill to limit employee recovery to Workers Compensation provisions); H.B. 1230, 103d Gen. Assemb., Reg. Sess. (Ill. 2023) (bill to exclude health care employers from the Act); H.B. 3112, 102d Gen. Assemb., Reg. Sess. (Ill. 2022) (bill to limit the definition of "actual harm" to mean an actual identity theft, loss, or injury and to limit recovery to only the initial violation of the Act).

[98] ACLU ILL., *supra* note 94.

[99] *See id.* (noting that BIPA was enacted to prevent employers and private entities from misusing biometric data to monitor, track, or otherwise control individuals without consent).

[100] *See* discussion *infra* Section IV.D.

[101] *See supra* note 83 and accompanying text.

[102] *See supra* notes 94–100 and accompanying text.

[103] *See infra* notes 104–09 and accompanying text (explaining the scrutiny companies like Clearview AI, Six Flags, Macy's, and Facebook have faced over collection and use of biometrics).

has focused on Clearview AI, a private company that provides search engine functionality to support identification of individuals against more than 50 billion publicly available images scraped from the Internet.[104] The images are compiled into its database, run through facial recognition algorithms to construct facial geometry for comparison, and made retrievable to Clearview AI's customers—formerly private and public entities.[105] Customers—now almost exclusively law enforcement agencies following Clearview's settlement with the ACLU[106]—can upload a picture to Clearview AI's server, which then identifies any images with similar-looking subjects and returns those images to the users after a human review.[107] Clearview AI's facial recognition algorithm touts 99% true positive accuracy across all tested demographic criteria, while also accounting for age progression and other changes in appearance.[108] Clearview AI's profile rose significantly after a data breach in February 2020 amplified

---

[104] *Clearview AI Principles*, CLEARVIEW AI, https://www.clearview.ai/principles (last visited January 28, 2024).

[105] Kashmir Hill, *The Secretive Company that Might End Privacy as We Know It*, N.Y. TIMES (Nov. 2, 2021), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html; *see* Tate Ryan-Mosley, *The NYPD Used a Controversial Facial Recognition Tool. Here's What You Need to Know.*, MIT TECH. REV. (Apr. 9. 2021), https://www.technologyreview.com/2021/04/09/1022240/clearview-ai-nypd-emails/.

[106] ACLU v. Clearview AI, Inc., No. 2020-CH-04353, 2022 Ill. Cir. LEXIS 2887, at *2–3, *5 (Cir. Ct. Cook Cty., May 11, 2022); *see also In Big Win, Settlement Ensures Clearview AI Complies with Groundbreaking Illinois Biometric Privacy Law*, ACLU (May 9, 2022, 11:45 AM), https://www.aclu.org/press-releases/big-win-settlement-ensures-clearview-ai-complies-with-groundbreaking-illinois (announcing the details of the settlement agreement).

[107] Terence Liu, *How We Store and Search 30 Billion Faces*, CLEARVIEW AI: BLOG (Apr. 18, 2023), https://www.clearview.ai/post/how-we-store-and-search-30-billion-faces.

[108] *Clearview AI Principles*, *supra* note 104; *see* Jonathan Lippman et al., *Clearview AI: Accuracy Test Report*, CLEARVIEW AI (Oct. 2019), https://s3.documentcloud.org/documents/6772775/Clearveiw-Ai-Accuracy-Test-Oct-2019.pdf (independent report on ClearviewAI's identification accuracy concluding that Clearview was 100% accurate across racial and demographics groups). *But see* Angelene Falk, *Commissioner Initiated Investigation into Clearview AI, Inc. (Privacy)*, 2021 AICMR 54, 38–40 (finding that Clearview's October 2019 accuracy test insufficient to prove that Clearview took steps to ensure the accuracy of the Matched Images it disclosed in free trials to Australian law enforcement personnel because the accuracy test was not repeated or supported by additional evidence, the independent panel in charge of the test did not have expertise or qualifications in facial recognition, and the panel did not design a new test based on Clearview's unique technology but rather reused a test conducted by the ACLU on a different facial recognition program).

existing privacy concerns and resulted in cease-and-desist orders and preliminary injunctions issued against the company, domestic civil liberties lawsuits, and the imposition of international fines on Clearview AI for the breach.[109]

Companies like Clearview AI, which compile biometric signatures and enable the unconsented collection of biometrics for law enforcement, security, and other purposes, intrude on everyone's reasonable expectation of privacy.[110] For a balance between privacy and security to be struck, it must be based upon informed consent.[111] To neglect informed consent would be to

---

[109] Mike Snider, *Clearview AI, Which Has Facial Recognition Database of 3 Billion Images, Faces Data Theft*, USA TODAY (Feb. 26, 2020, 4:34 PM), https://www.usatoday.com/story/tech/2020/02/26/clearview-ai-data-theft-stokes-privacy-concerns-facial-recognition/4883352002/ (explaining the controversial situation regarding facial software firm Clearview AI); Kaixin Fan, *Clearview AI Responds to Cease-and-Desist Letters by Claiming First Amendment Right to Publicly Available Data*, HARV. J.L. & TECH. DIGEST (Feb. 25, 2020), https://jolt.law.harvard.edu/digest/clearview-ai-responds-to-cease-and-desist-letters-by-claiming-first-amendment-right-to-publicly-available-data; *see* Letter from Sen. Edward J. Markey, U.S. Sen., Mass., to Hoan Ton-That, Founder & Chief Exec. Officer, Clearview AI (Nov. 20, 2023) (on file with author) (requesting answers to questions addressing concerns regarding Clearview AI's continued development of facial recognition technology, posing serious threat to privacy rights and civil liberties); *see also* Email from Tor Ekeland, Managing Partner, Tor Ekeland Law PLLC to Sen. Edward J. Markey, U.S. Sen., Mass. (Jan. 31, 2020) (on file with Sen. Edward J. Markey) (previous email noting alleged harms are speculative and expressing that Clearview aims to protect communities, rights, and proprietary technology); Vermont v. Clearview AI, Inc., No. 226-3-20 Cncv, 2020 Vt. Super. LEXIS 4, at *1 (Super. Ct. Chittenden Cty. 2020) (civil suit brought by Vermont Attorney General alleging that Clearview AI violated Vermont laws when it (1) engaged in unfair acts and practices by collecting billions of photographs and made them available for its customers to search using facial recognition technology without the consent of those depicted; (2) engaged in deceptive acts and practices by making material misrepresentations about its product, and fraudulently acquired brokered biometric data used to identify a consumer); ACLU v. Clearview AI, Inc., No. 2020 CH 04353, 2022 Ill. Cir. LEXIS 2887 (Cir. Ct. Cook Cty. 2022) (permanently enjoining Clearview AI from providing its facial recognition database to private entities or individuals in the US, except under specific legal conditions, and restricting access by individual government employees acting outside their official capacities); Robert Hart, *Clearview AI–Controversial Facial Recognition Firm–Fined $33 Million for 'Illegal Database,'* FORBES (Sept. 3, 2024, 7:54 AM), https://www.forbes.com/sites/roberthart/2024/09/03/clearview-ai-controversial-facial-recognition-firm-fined-33-million-for-illegal-database/.

[110] *Illinois Court Rejects Clearview's Attempt to Halt Lawsuit Against Privacy-Destroying Surveillance*, ACLU ILL. (Aug. 27, 2021), https://www.aclu-il.org/en/press-releases/illinois-court-rejects-clearviews-attempt-halt-lawsuit-against-privacy-destroying.

[111] *See* Lauren Hendrickson, *Privacy Concerns with Biometric Data Collection*, IDENTITY (Oct. 20, 2024), https://www.identity.com/privacy-concerns-with-

deprive people of their right to their autonomy, their privacy, and other fundamental rights protected by the Constitution in the name of convenience or security.[112]

The modern concept of informed consent arises from the horrific experiments conducted by Nazi physicians on human subjects, which led to the creation of the Nuremberg Code,[113] as well as the Tuskegee Untreated Syphilis Study, which resulted in the National Research Act.[114] The National Research Act created the National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research.[115] The Commission shortly thereafter released the Belmont Report outlining the significance of informed consent as a respect for personal autonomy:

> Respect for persons requires that subjects, to the degree that they are capable, be given the opportunity to choose what shall or shall not happen to them. This opportunity is provided when adequate standards for informed consent are satisfied.
>
> While the importance of informed consent is unquestioned, controversy prevails over the nature and possibility of an informed consent. Nonetheless, there is widespread agreement that the consent process can be analyzed as containing three elements: information, comprehension and voluntariness.[116]

Although these ethical principles were initially developed for medical research, they remain highly relevant to the use of artificial intelligence (AI).[117] AI's capabilities pose a growing threat

---

biometric-data-collection/.

[112] *See id.*

[113] *See* David M. Pressel, *Nuremberg and Tuskegee: Lessons for Contemporary American Medicine*, 95 J. NAT'L MED. ASS'N 1216, 1218–19 (2003) (discussing how horrific Nazi medical experiments resulted in the Nuremberg Code and its 10 principles that establish ethical and legal guidelines for medical experimentation on human subjects, including voluntary consent).

[114] *The U.S. Public Health Service Untreated Syphilis Study at Tuskegee*, CDC (Sept. 4, 2024), https://www.cdc.gov/tuskegee/about/effects-research.html ("After . . . Tuskegee, the government changed its research practices. In 1974, the National Research Act was signed into law, creating the National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research.").

[115] *See id.*

[116] NAT'L COMM'N FOR THE PROT. OF HUM. SUBJECTS OF BIOMEDICAL & BEHAV. RSCH., THE BELMONT REPORT: ETHICAL PRINCIPLES AND GUIDELINES FOR THE PROTECTION OF HUMAN SUBJECTS OF RESEARCH [6] (1979), https://www.hhs.gov/ohrp/sites/default/files/the-belmont-report-508c_FINAL.pdf.

[117] *See* Laura Stark, *Protections for Human Subjects in Research: Old Models,*

to personal autonomy by enabling the unconsented collection, analysis, and use of biometric data.[118]

Multiple lawsuits recently brought against private entities have centered on the importance of consent in biometric collection and use.[119] For example, Macy's Retail Holdings, LLC faced a class action lawsuit for its use of Clearview AI's application to surveil its Macy's retail stores in violation of (1) the Illinois Biometric Privacy Act; (2) information privacy protections contained in the California Constitution; and (3) the protection against commercial exploitation of one's name or image pursuant to New York's Civil Rights Act § 51.[120] Six Flags Entertainment Corporation similarly faced suit for alleged violations of BIPA when the company collected pass holders' fingerprints without adhering to BIPA's restrictions on how private entities "collect, retain, disclose, and destroy biometric identifiers."[121] Similarly, Facebook has had to defend against class action lawsuits, including a suit brought under BIPA for subjecting plaintiffs to facial recognition technology without their written consent through its "Tag Suggestion" feature, and another lawsuit under Cal. Civ. Code § 3344 for using names, photographs, likenesses and identities to sell advertisements without obtaining the users' consent, even if the users uploaded the photographs to the platform themselves.[122]

Now, as employers look to utilize facial recognition surveillance methods through companies like Clearview AI, employees require adequate methods to protect their rights to their identity—to be afforded true choice about whether they consent to the use of their

---

New Needs?, MIT SCHWARZMAN COLL. COMPUTING (Jan. 24, 2022), https://mit-serc.pubpub.org/pub/protections-for-human-subjects/release/1 (explaining that, in 2012, the US Department of Homeland Security published a corollary to the *Belmont Report* for research in computer science and information security called the Menlo Report, designed to impute the *Belmont Report's* principles to modern issues like biometric data collection and analysis).

[118] *See id.*

[119] *See, e.g.*, *US Biometric Privacy Litigation Takes the Forefront*, CLARIP, https://www.clarip.com/data-privacy/us-biometric-privacy-litigation-takes-the-forefront/ (last visited Dec. 19 2024) (discussing biometric privacy lawsuits recently brought in Texas, Washington, Illinois, Maryland, and New York).

[120] *See In re* Clearview AI, Inc., No. 21-CV-135, 2022 U.S. Dist. LEXIS 14882, at *10–12, *17 (N.D. Ill. Jan. 27, 2022).

[121] Rosenbach v. Six Flags Ent. Corp., 129 N.E.3d 1197, 1199–200 (Ill. 2019).

[122] *See* Patel v. Facebook, Inc., 932 F.3d 1264, 1267–68 (9th Cir. 2019); Fraley v. Facebook, Inc., 830 F. Supp. 2d 785, 790 (N.D. Cal. 2011) (alleging a violation of CAL. CIV. CODE § 3344 when Facebook used plaintiffs' names, photographs, likenesses and identities to sell advertisements for products, services, or brands without obtaining the users' consent).

biometric information.[123] What should not become the norm is for the employees to be required to acquiesce to the use of their biometrics as a condition of employment.[124] Instead, employees should be allowed to provide those biometrics in return for greater convenience or compensation, or deny collection and use thereby retaining control over their identity throughout and at the conclusion of their employment.[125]

While one of the original purposes of using biometrics has been to identify a person and protect that person's information and assets from unauthorized disclosure,[126] private entities have turned that mechanism into one they can exploit against the very people whose biometrics they collect for commercial profit or claims of enhanced security.[127] In light of this shift, privacy laws must provide individuals with greater protection against such exploitation arising out of a significant power imbalance, such as that between an employer and employee.

IV. CAUSES OF ACTION UNDER INVASION OF PRIVACY LAW

Any recommendation for refining privacy law must start with a fundamental understanding of what that body of law entails. Privacy law may already provide a framework for ways in which

---

[123] *See* Harmon, *supra* note 21, at 602, 608, 610–11, 616–19.

[124] *See id.* at 616, 619–23.

[125] *See infra* Section VI.A (outlining a recommended licensing scheme through which employees may license their likeness to their employers).

[126] *See, e.g.*, *The Evolution of Biometrics*, CAPITOL TECH. UNIV.: CAPITOLOGY BLOG (Mar. 25, 2022), https://www.captechu.edu/blog/evolution-of-biometrics (discussing the history of biometrics: "The primary benefit of biometric technology is that it is extremely difficult to fake or steal someone's physical attributes, as opposed to a PIN or social security number. . . .").

[127] *See* Sam Blum, *Biometric Monitoring is Booming in the Workplace, Raising Ethical and Legal Issues for HR*, HR BREW (Mar. 4, 2022), https://www.hr-brew.com/stories/2022/03/04/biometric-monitoring-is-booming-in-the-workplace-raising-ethical-and-legal-questions-for-hr (discussing how biometrics may be detrimental to employees through workplace monitoring and through health initiatives); Brown, *supra* note 13, at 274–76, 282–84 (identifying ways employers can use biometric data against employees); Alessandro Mascellino, *Biometric Data for Advertising Personalization Comes Under Scrutiny*, BIOMETRICUPDATE.COM (Oct. 17, 2022), https://www.biometricupdate.com/202210/biometric-data-collection-for-advertising-personalization-comes-under-scrutiny ("[A]dvertising infrastructure companies are deploying face biometrics . . . to enable brands to target specific kinds of people. Large data brokers then use the data to predict people's movements to show them ads at the perfect moment. . . . [T]he advertising industry 'functions solely to use personal data as a tool to target us as individuals just to make more sales.").

an employer may be held accountable for violating their employees' rights, specifically in the context of biometric information. There are four common law causes of action for invasion of privacy: (1) unreasonable intrusion upon the seclusion of another; (2) unreasonable public disclosure of private facts; (3) unreasonably placing another in a false light to the public; and (4) appropriation of one's name or likeness.[128] Each of these causes of action may arise from some harm upon one's biometric information as an interest, but appropriation of one's likeness holds the most potential for legal application with respect to biometric information.[129]

A. Intrusion Upon Seclusion

Most privacy interests arise from the right to be free from unwarranted publicity—"the right to be let alone."[130] Intrusion upon seclusion is the only cause of action in privacy law that does not depend on any publicity of the person whose privacy is being invaded.[131] Instead, it requires only an intentional interference with someone's solitude or seclusion of their private affairs in an offensive manner.[132]

The Restatement (Second) of Torts defines intrusion upon seclusion as: "intentional[] intru[sion], physical[] or otherwise, upon the solitude or seclusion of another or his private affairs or concerns . . . if the intrusion would be highly offensive to a reasonable person."[133] An intrusion occurs when (1) a person physically enters a place where someone has secluded themselves or their private affairs; (2) uses their senses to oversee or overhear another's private affairs; or (3) engages in a different form of

---

[128] *See* RESTATEMENT (SECOND) OF TORTS § 652A (AM. L. INST. 1977).

[129] Donald L. Buresh, *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?*, 38 SANTA CLARA HIGH TECH. L.J. 39, 87 (2021) ("[F]our distinct privacy torts . . . are available for litigants whether the privacy issue at hand deals with personal information or biometric information.").

[130] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890).

[131] *See* Auto-Owners Ins. Co. v. Websolv Computing, Inc., 580 F.3d 543, 550–51 (7th Cir. 2009) ("[O]ne can violate another's right to seclusion without publicizing anything."). *See generally* RESTATEMENT (SECOND) OF TORTS §§ 652A–E (AM. L. INST. 1977) (detailing the four common law privacy torts).

[132] *See* RESTATEMENT (SECOND) OF TORTS § 652B (AM. L. INST. 1977).

[133] *Id.*

investigation or examination into another's private concerns.[134] Intrusion upon seclusion claims require an analysis of whether the plaintiff had an objective expectation of privacy with regard to the affairs and concerns allegedly intruded upon.[135] When an alleged intrusion stems from a plaintiff's voluntary exhibition of his affairs and concerns to the public gaze, the plaintiff did not have an objective expectation of privacy with regard to those affairs and concerns, and therefore cannot prevail in an intrusion upon seclusion case.[136]

If an intrusion is established, a plaintiff must also prove that the intrusion is "highly offensive."[137] Whether an invasion of privacy is considered highly offensive is determined by the totality of the circumstances:

> In determining whether an invasion of a privacy interest would be "offensive" to an ordinary, reasonable person, a court should consider all of the circumstances including "the degree of the intrusion, the context, conduct and circumstances surrounding the intrusion as well as the intruder's motives and objectives, the setting into which he intrudes, and the expectations of those whose privacy is invaded."[138]

"Highly offensive" has been described as something that would "inspire out-and-out revulsion," such that some of the more commonly engaged activities on the Internet (e.g., browsing a website) are unlikely to reach the level of highly offensive even if companies surreptitiously track those activities.[139]

Protecting biometric information on a theory of intrusion upon seclusion would be complicated by two major challenges. The first

---

[134] *Id.* at cmt. b.

[135] 62A AM. JUR. 2d *Privacy* § 36 (2014) ("The tort of intrusion into private matters is proven only if the plaintiff had an objectively reasonable expectation of seclusion or solitude in the invaded place or matter.").

[136] *See id.*

[137] *See* RESTATEMENT (SECOND) OF TORTS § 652B (AM. L. INST. 1977).

[138] Wolfson v. Lewis, 924 F. Supp. 1413, 1421 (E.D. Pa. 1996) (quoting Hill v. Nat'l Collegiate Athletic Assoc., 865 P.2d 633, 648 (Ca. 1994)).

[139] *See, e.g.*, *In re* Nickelodeon Consumer Priv. Litig., 827 F.3d 262, 294 (3d Cir. 2016); *see also In re* Google Inc. Cookie Placement Consumer Priv. Litig., 934 F.3d 316, 325 (3d Cir. 2019) (citing *In re Nickelodeon Consumer Privacy Litigation* as the controlling circuit law on the interpretation of "highly offensive" in intrusion upon seclusion claims. 827 F.3d 262); Popa v. Harriet Carter Gifts, Inc., 426 F. Supp. 3d 108, 121–22 (W.D. Pa. 2019) (analyzing, in an intrusion upon seclusion claim, whether an intrusion was "highly offensive" according to the holding of *In re Nickelodeon Consumer Privacy Litigation*).

challenge would be successfully arguing that an intrusion occurred when a person ventures outside of their home or into the public, via the Internet or physical presence.[140] A plaintiff would need to demonstrate that they did not exhibit their biometric information to the public gaze or any intrusion upon seclusion claim would fail (i.e., they had a reasonable expectation of privacy in their facial geometry while exhibiting their face in public).[141]

Even if a plaintiff could persuade the trier of fact that an intrusion occurred, the plaintiff would still have to establish that the invasion involving biometric information was highly offensive to a reasonable person.[142] Mere collection or reference to biometric information may not be highly offensive.[143] The standard for what would satisfy this requirement currently lacks a sufficient definition other than that it "offends society's accepted, communal norms and social mores"—a definition which shifts as our global society increasingly explores privacy rights.[144]

B. Public Disclosure of Private Facts

What employers do with the biometrics of their employees after collection matters.[145] Many employers collect their employees' facial geometry and provide them to a contracted third-party business partner or through other sources with the intent to authenticate the identity of that person.[146] The more the biometric

---

[140] *See supra* notes 133–36 and accompanying text (explaining that an intrusion does not occur when the plaintiff has willingly put the information in the public eye).

[141] *See supra* notes 133–36 and accompanying text.

[142] *See supra* notes 133, 137–39 and accompanying text (explaining the "highly offensive" element of intrusion upon seclusion claims).

[143] *See* Nader v. General Motors Corp., 255 N.E.2d 765, 769 (N.Y. 1969) ("[T]he mere gathering of information about a particular individual does not give rise to a cause of action under [an intrusion upon seclusion] theory.").

[144] Cmty. Health Network v. McKenzie, 185 N.E.3d 368, 382 (Ind. 2022); *see supra* Part II (discussing how social norms regarding reasonable expectations of privacy change over time).

[145] *See* Cristina Del Rosso, *Access Granted: An Examination of Employee Biometric Privacy Laws and a Recommendation for Future Employee Data Collection*, 18 J.L. ECON. & POL'Y 24, 24–31 (2023) (identifying potential dangers of employers' biometric use, including hacking and identity theft, false identifications, and degradation of civil liberties).

[146] *E.g.,* Cothron v. White Castle Sys. 216 N.E.3d 918, 920–21 (Ill. 2023) (White Castle sued for contracting a third-party vendor to implement fingerprint authentication for employee access to pay stubs and computers); Neals v. PAR Tech. Corp., 419 F. Supp. 3d 1088, 1090 (N.D. Ill. 2019) (BIPA lawsuit against PAR Technology, a third-party vendor that developed a system enabling the plaintiff's employer to track her time using fingerprint scans).

information is shared, the greater the risk becomes that the data is subject to a breach, potentially resulting in broad disclosure of the biometric information.[147] Without legal protection, the biometric information collected by an employer may easily be spread far outside the reach of the original data subject.[148]

A claim under public disclosure of private facts protects plaintiffs facing similar issues, attaching liability to an offender for invasion of another's privacy when the offender "gives publicity to a matter concerning the private life of another . . . if the matter publicized is of a kind that (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public."[149] Although courts across the country have adopted slightly different versions of the cause of action, they generally agree that a plaintiff must prove the disclosure to the public of private facts that are both highly offensive and of no legitimate concern to the public to prevail.[150]

Indiana is one of the states that recently adopted this disclosure

---

[147] *See* Michael Meyer, *5 Common Data-Sharing Challenges and How to Overcome Them*, ALATION: BLOG (Jan. 4, 2024), https://www.alation.com/blog/data-sharing-challenges/ ("As data accessibility increases, so does the risk of unauthorized access, hacking, and insider breaches.").

[148] *See generally* Hendrickson, *supra* note 111 (explaining the increasing risk that biometric data will be compromised when collected by any entity and stating that the 2015 hacking of the US Office of Personnel Management resulted in exposure of 5.6 million federal employees' fingerprints).

[149] RESTATEMENT (SECOND) OF TORTS § 652D (AM. L. INST. 1977).

[150] *See* Wolf v. Regardie, 553 A.2d 1213, 1220 (D.C. Cir. 1989) (stating the elements of the tort as: "(1) publicity, (2) absent any waiver or privilege, (3) given to private facts, (4) in which the public has no legitimate concern, (5) and which would be highly offensive to a reasonable person of ordinary sensibilities"); Dep't of Labor v. McConnell, 828 S.E.2d 352, 359 (2019) ("There are at least three necessary elements for recovery under [the public disclosure of private facts] theory: (a) the disclosure of private facts must be a public disclosure; (b) the facts disclosed to the public must be private, secluded or secret facts and not public ones; [and] (c) the matter made public must be offensive and objectionable to a reasonable man of ordinary sensibilities under the circumstances."); Cmty. Health Network v. McKenzie, 185 N.E.3d 368, 380–82 (Ind. 2022) (explicitly adopting the public disclosure of private facts tort as articulated in the *Restatement (Second) of Torts*); Shulman v. Grp. W Prods., Inc., 18 Cal. 4th 200, 214 (1998) (listing the following as elements of the public disclosure tort: "(1) public disclosure (2) of a private fact (3) which would be offensive and objectionable to the reasonable person and (4) which is not of legitimate public concern"); Hunstein v. Preferred Collection & Mgmt. Servs., 48 F.4th 1236, 1246 (11th Cir. 2022) (stating that the elements of public disclosure are (1) publicity; (2) of a matter in the private life of another; (3) that is highly offensive to a reasonable person; and (4) that the disclosed information is not of legitimate public concern).

tort amidst the technological advances of the day.[151] The digitization of our personal lives has added to the "increase in speed and ease with which [sensitive, personal information can now] be [accessed and] broadcast to the public."[152] Thus, "with the ubiquity of digital data, it is easier than ever for unwanted third parties to obtain—and share—sensitive information."[153] Such concerns about the growing dangers of privacy invasion in the digital age have led to the recognition of public disclosure of private facts as a tort within jurisdictions that have previously refrained from adopting the tort.[154]

What constitutes a private fact—the first element of a public disclosure of private facts claim—differs across jurisdictions.[155] Information like one's name, address, phone number, and social security number, however, are never considered private facts.[156] Instead, private facts are generally considered information one may withhold from others, which may also be of an embarrassing nature.[157] What makes the fact private is that the person took steps to prevent discovery of that fact.[158] This remains true even if the person disclosed the information to some degree to family or friends.[159]

A public disclosure, the tort's second element, requires that "the information must be communicated in a way that either reaches

---

[151] *See McKenzie*, 185 N.E.3d at 380–81.

[152] *See* Robbins v. Trs. of Ind. Univ., 45 N.E.3d 1, 13 (Ind. Ct. App. 2015) (Crone, J., concurring in part and concurring in result in part).

[153] *See* F.B.C. v. MDwise, Inc., 122 N.E.3d 834, 838–39 (Ind. Ct. App. 2019) (Bailey, J., dissenting).

[154] *See* Allstate Ins. Co. v. Dana Corp., 759 N.E.2d 1049, 1057 (Ind. 2001); *McKenzie*, 185 N.E.3d at 381; MDwise, Inc., 122 N.E.3d at 836–37 (not recognizing public disclosure of private information as a tort); J.H. v. St. Vincent Hosp. & Health Care Ctr., Inc., 19 N.E.3d 811, 815 (Ind. Ct. App. 2014) (recognizing the public disclosure of private information to the public at large is required); Munsell v. Hambright, 776 N.E.2d 1272, 1282–83 (Ind. Ct. App. 2002) (recognizing the uncertainty of whether specific sub-torts are recognized in Indiana courts); Vargas v. Shepherd, 903 N.E.2d 1026, 1031 (Ind. Ct. App. 2009) (recognizing public disclosure of private information as a tort); Westminster Presbyterian Church of Muncie v. Cheng, 992 N.E.2d 859, 868 (Ind. Ct. App. 2013).

[155] Whitney Kirsten McBride, Comment, *Lock the Door: Does Private Mean Secret?*, 42 MCGEORGE L. REV. 901, 908–09 (2011) ("A jurisdictional split of authority exists in determining whether a fact is 'private' for the purposes of public disclosure of private facts.").

[156] *See* RESTATEMENT (SECOND) OF TORTS § 652D cmt. b (AM. L. INST. 1977).

[157] 62 AM. JUR. *Privacy* § 85 (2014).

[158] *See id.*

[159] *See id.*

or is sure to reach the public in general or a large enough number of persons such that the matter is sure to become public knowledge."[160] There is no specific number requirement to meet the "large enough number," but the facts must support such a claim that the requisite number has been reached.[161]

The third element, that the private fact be "highly offensive," is assessed similarly to potentially offensive facts under an intrusion upon seclusion claim. Like with intrusion upon seclusion, the highly offensive standard reflects the mores of society and is the subject of debate and change throughout time as society continues to examine privacy, both at a national and global level.[162] With respect to the fourth element, whether the facts are of public concern or otherwise newsworthy, the analysis ultimately hinges on whether "a reasonable member of the public . . . would say that he had no concern with the information disclosed."[163] Where there is no concern for the information disclosed, the "is not of legitimate concern to the public" requirement is satisfied.[164]

Classifying biometric information as a matter of public concern remains a key obstacle in applying the tort of public disclosure of private information to biometric data.[165] Whether a piece of published information, including biometric information, is of "public concern" requires a legal inquiry in which courts must

---

[160] *McKenzie*, 185 N.E.3d at 382; *see* RESTATEMENT (SECOND) OF TORTS § 652D cmt. a (AM. L. INST. 1977).

[161] *See McKenzie*, 185 N.E.3d at 382 (citing RESTATEMENT [SECOND] OF TORTS § 652D cmt. a [AM. L. INST. 1977]).

[162] *See* RESTATEMENT (SECOND) OF TORTS §652D cmt. a, cmt. c ("The protection afforded to the plaintiff's interest in his privacy must be relative to the customs of the time and place, to the occupation of the plaintiff and to the habits of his neighbors and fellow citizens.").

[163] *See McKenzie*, 185 N.E.3d at 382; RESTATEMENT (SECOND) OF TORTS § 652D cmt. h (AM. L. INST. 1977).

[164] *See supra* note 149 and accompanying text.

[165] *See* Connie Davis Powell, *"You Already Have Zero Privacy. Get over it!" Would Warren and Brandeis Argue for Privacy for Social Networking?*, 31 PACE L. REV. 146, 170 (2011) ("[I]t is hard to establish that the facts are private when a user has voluntarily posted them on a social networking site and many terms and conditions give the social networking site control to use the information."); Mariana Renke, Note, *TikTok and Instagram Know What You Did Last Summer and the Federal Government Will Not Be the One to Put a Stop to It*, 2023 U. ILL. J.L. TECH. & POL'Y 451, 469–70 ("Public disclosure of private facts . . . falls short because in deciding [biometric collection] cases involving this tort the courts unanimously hold that there is no reasonable expectation of privacy in public places classifying the internet . . . as [a] public place[]."); *see* RESTATEMENT (SECOND) OF TORTS §652D cmt. b ("[T]here is no liability for giving further publicity to what the plaintiff himself leaves open to the public eye.").

weigh the "conflicting interests of individual privacy and press freedom."[166]

The prominent biometric identifier that may most likely be considered "of public concern" is a fingerprint. Fingerprints are firmly incorporated into our criminal justice system.[167] Because of their usefulness in criminal investigations,[168] fingerprints may be argued to be of public concern. However, the public concern argument relies more on the application of the fingerprints in the criminal context than on the fingerprints themselves.[169] Therefore, establishing biometric information as information "of public concern" may not be feasible in the context of privacy torts, in which biometrics likely lack the criminal identification component that renders them of public concern.

C. False Light

False light is a different type of privacy tort similar in nature to defamation. As conceptualized by the Restatement:

> One who gives publicity to a matter concerning another that places the other before the public in a false light is subject to liability to the other for invasion of his privacy, if (a) the false light in which the other was placed would be highly offensive to a reasonable person, and (b) the actor had knowledge of or acted in reckless disregard as to the falsity of the publicized matter and the false light in which the other would be placed.[170]

Similarly, liability for defamation may attach to a defendant when the defendant makes (1) a false and defamatory statement (2) to a third party without privilege (3) with fault amounting to

---

[166] *See* Shulman v. Group W Prods., Inc., 18 Cal. 4th 200, 215–16 (1998).

[167] *See generally* M. Edwin O'Neill, *Fingerprints in Criminal Investigation*, 30 AM. INST. CRIM. L. & CRIMINOLOGY 929, 931 (1939-1940) (explaining the application of fingerprints in criminal investigation).

[168] Roger Antonio Tejada, *Keep Your Hands Off My Fingerprints: How State Constitutionalism Can Stop On-Site Fingerprinting Dragnets*, 41 MINN. J.L. & INEQ. 287, 297 (2023) ("Fingerprinting technology was incorporated into the United States criminal justice system shortly after its creation in the late 1800s and has since become a cornerstone in the administration of justice.").

[169] *See generally* Andre A. Moenssens & Stephen B. Meagher, *Fingerprints and the Law, in* NAT'L INST. OF JUSTICE, THE FINGERPRINT SOURCEBOOK (Alan McRoberts ed., 2011)

[170] *Compare* RESTATEMENT (SECOND) OF TORTS § 652E (AM. L. INST. 1977), *with* Counterman v. Colorado, 600 U.S. 66, 73 (2023) (defining defamation as "false statements of fact harming another's reputation") (citing Gertz v. Robert Welch, Inc., 418 U.S. 323, 340, 342 (1974)).

at least negligence on the defendant's part (4) that caused special harm or is actionable without special harm.[171] Where a defamation claim may succeed or fail, so too does a false light claim.[172] While defamation and false light torts are similar, they can be distinguished by the interests they are intended to protect:

> The gravamen of a defamation action is injury to the reputation. An injury to reputation affects a proprietary interest and is not a personal injury. On the other hand, the right of privacy [embodied in false light claims] is designed to protect feelings and sensibilities, rather than safeguarding pecuniary or proprietary interests.[173]

Currently, biometric information and false light claims have only a faint potential for overlap: false positives and false negatives that facial recognition algorithms may generate.[174] Within the context of biometric identifiers, a false positive occurs when a person being compared against a registered biometric identifier matches that identifier when, in fact, the identifier belongs to someone else.[175] A false negative occurs when a person being compared against a biometric identifier does not match the identifier, when that person provided the identifier and should have resulted in a match.[176] False light concerns around false positives involve being misidentified as someone else—being misidentified as a criminal or someone with an unsavory reputation that may attach to the person being identified.[177] The concerns surrounding false negatives apply when someone is not identified when they should have been identified, like when an algorithm fails to associate a job seeker with their information and hinders their ability to seek employment.[178] It would be the people who are subject to those false reports, and the harms they may

---

[171] RESTATEMENT (SECOND) OF TORTS § 558 (AM. L. INST. 1977).

[172] Mitchell v. Twin Galaxies, LLC, 70 Cal. App. 5th 207, 224 (2021) (citing Eisenberg v. Alameda Newspapers, Inc., 74 Cal. App. 4th 1359, 1385 (1999)).

[173] John L. Breeden Jr. & Douglas M. Zayicek, *False Light Invasion of Privacy: A New Tort in Town?*, 9 S.C. LAW. 39, 41 (1997) (internal citation omitted).

[174] *Face Recognition Technology Evaluation: Demographic Effects in Face Recognition*, NAT'L INST. OF STANDARDS & TECH. (Aug. 18, 2023), https://pages.nist.gov/frvt/html/frvt_demographics.html.

[175] Greg Fiumara, *A Tale of Two Errors: Measuring Biometric Algorithms*, NAT'L INST. OF STANDARDS & TECH. (May 18, 2022), https://www.nist.gov/blogs/taking-measure/tale-two-errors-measuring-biometric-algorithms.

[176] *Id*.

[177] *Id.*

[178] *Id.*

create, who may have a semblance of a claim under a false light claim.[179] Those false light claims, however, would likely fail because the tort requires that the matter be publicized for liability to attach.[180]

D. Appropriation of One's Likeness and the Related Right to Publicity

Appropriation of one's likeness is the last of the privacy torts and provides protections similar to those intended to protect a person's right to publicity.[181] According to the Restatement, a person may be subject to liability to another under appropriation of one's likeness if they "appropriate[] to their own use or benefit the name or likeness of another"[182] Similarly, the right to publicity prevents a person or corporation from appropriating the commercial value of a person's identity by using, without consent, the person's name, likeness, or other indicia of identity for purposes of trade.[183] The distinguishing feature between the appropriation of one's likeness tort and the right of publicity is in the nature of the harm the causes of action are intended to address.[184] While the appropriation of one's likeness tort "is not limited to commercial appropriation,"[185] the right of publicity "protects against commercial loss caused by appropriation of an individual's identity for commercial exploitation."[186]

The origins of law concerning one's likeness involved those of celebrities and public figures.[187] The law emerged to place a limitation on the likenesses of publicly known persons from the unjustified interference of their "right to enjoy the fruits of his own industry."[188] The right to publicity is founded on the idea that "one

---

[179] *See supra* text accompanying notes 170–73.

[180] *See supra* text accompanying note 171.

[181] *See* Olivia Wall, Note, *A Privacy Torts Solution to Postmortem Deepfakes*, 100 Wash. U. L. Rev. 885, 898 (2023) ("Resembling the elements of the right of publicity, the elements of the appropriation tort are using another's name or likeness for one's own use or benefit. The key difference is that 'use' in an appropriation claim focuses on mental or emotional harm, rather than commercial harm.").

[182] RESTATEMENT (SECOND) OF TORTS § 652C (AM. L. INST. 1977).

[183] RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 46 (AM. L. INST. 1995).

[184] 62A AM. JUR. 2d *Privacy* § 62 (2014).

[185] RESTATEMENT (SECOND) OF TORTS § 652C cmt. b.

[186] *Id.*

[187] *See* Samantha Barbas, *From Privacy to Publicity: The Tort of Appropriation in the Age of Mass Consumption*, 61 BUFFALO L. REV. 1119, 1123 (2013).

[188] Palmer v. Schonhorn Enters., Inc., 232 A.2d 458, 462 (N.J. Super. Ct. Ch.

should [not] be permitted to commercialize or exploit or capitalize upon another's name, reputation or accomplishments merely because the owner's accomplishments have been highly publicized."[189] The right to publicity does not concern the simple publication of biographical or other identity data, but the application of that data for a commercial project or use.[190]

Actions concerning appropriation of one's likeness, specifically the right to publicity, provide the most promising protection for employee's privacy rights surrounding their biometric information. To succeed on such a claim, however, a plaintiff would have to establish that biometric information is considered within the definition of one's likeness. Although what constitutes "one's likeness" may slightly vary between jurisdictions, the common law right of publicity "is not limited to an appropriation of name or likeness; the key issue is the appropriation of the plaintiff's *identity*."[191] State statutes are similarly intended to "preserv[e] the individual's right of control over the commercial aspects of one's identity."[192] A "[b]iometric identifier" is "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry."[193] As "unique personal feature[s] that can be used to *identify*" [] unique individual[s],"[194] biometric identifiers should fit comfortably within the protections offered pursuant to anti-appropriation statutes.

With respect to the commercial purpose required to state a claim under statutory rights to publicity,[195] an employer may exploit the biometrics of their employees to its own benefit by selling, leveraging, or otherwise putting the biometrics to some commercial purpose. Clearview AI has already demonstrated that anyone's biometric data has commercial value, as evidenced by its sale and use of biometric signatures *en masse*.[196] In appropriating

---

Div. 1967).

[189] *Id.*

[190] Melendez v. Sirius XM Radio, Inc., 50 F.4th 294, 307–08 (2d Cir. 2022) (internal quotations omitted); s*ee also* CAL. CIV. CODE § 3344 (1995).

[191] 62A AM. JUR. 2d *Privacy* § 63 (2014) (emphasis added).

[192] *Id.*

[193] BIPA, 740 ILL. COMP. STAT. § 14/10 (2008).

[194] Carpenter v. McDonald's Corp., 580 F. Supp. 3d 512, 515 (N.D. Ill. 2022) (emphasis added).

[195] *See* AM. JUR. 2d *Privacy* § 63, *supra* note 191.

[196] Hill, *supra* note 105; Dave Gershgorn, *This Is the Ad Clearview AI Used to Sell Your Face to Police*, MEDIUM (March 11, 2020), https://onezero.medium.com/this-is-the-ad-clearview-ai-used-to-sell-your-face-to-police-8997c2a6f0a8.

an employee's likenesses, an employer may be denying the employee the right to control their likeness, including the choice to keep that information private and potentially the ability to benefit from utilizing their likeness themselves.[197]

V. LICENSING ONE'S BIOMETRIC IDENTIFIERS AS "LIKENESS" PURSUANT TO RIGHT TO PUBLICITY LAWS

As previously discussed, an individual may license or assign the use of his or her name or likeness.[198] This area of law most commonly sees use by public figures and celebrities—people who are commonly within the public eye.[199] Nevertheless, most scholars and courts agree that the right to publicity remains available to everyone else, whether they be in the public eye or out of it.[200]

Likeness licenses greatly vary, including regarding what aspects of nature and likeness are protected, how the licensee's name or likeness may be used, exclusivity, and the length of time the license is valid.[201] Thus, licenses must set parameters that

---

[197] *See infra* notes 199–200, 217–19 (discussing the existence of a right of publicity for non-celebrity plaintiffs).

[198] 1 Anne Gilson LaLonde & Jeremy Gilson, *Gilson on Trademarks* § 2B.05 (2024).

[199] *See* Jennifer L. Carpenter, *Internet Publication: The Case for an Expanded Right of Publicity for Non-Celebrities*, 6 VA. J.L. & TECH. 3 (2001) (explaining why celebrities are the usual plaintiffs in appropriation of one's likeness cases); *see also* Pellegrino v. Epic Games, Inc., 451 F. Supp. 3d 373, 377–78 (E.D. Pa. 2020) (asserting that misappropriation of a professional figures trademark violated his right to publicity); Kirby v. Sega of Am., Inc., 50 Cal. Rptr. 3d 607, 608–09, 611 (Cal. Ct. App. 2006) (alleging misappropriation of her likeness and identity, a celebrity sued video game distributors for using them in developing, marketing, and creating a character); Winter v. DC Comics, 69 P.3d 473, 475–76 (Cal. 2003) (explaining that "celebrities have a statutory right of publicity by which they can prohibit others from using their likeness.").

[200] *See* Sessa v. Ancestry.com Operations Inc., 561 F. Supp. 3d 1008, 1020–23 (D. Nev. 2021) (concluding that non-celebrity plaintiffs sustained injury sufficient for standing to sue under the Nevada Right of Publicity Act for company's use of their names and likeness); *see also* Wilson v. Ancestry.com LLC, 653 F. Supp. 3d 441, 447, 453–54 (S.D. Ohio 2023) (denying defendant's motion to dismiss because the right of publicity is a part of the common-law right of privacy available to those in and out of the public eye); Knapke v. PeopleConnect Inc., 553 F. Supp. 3d 865, 872, 877 (W.D. Wash. 2021) (explaining that a claim under the Right of Publicity law requires the person's persona to be used for commercial purposes); Perkins v. LinkedIn Corp., 53 F. Supp. 3d 1222, 1225, 1236, 1254 (N.D. Cal. 2014) (arguing that reminder emails in connection to non-celebrity plaintiff's names and likeness were incidental and therefore not a violation of California's common law right of publicity); J. Thomas McCarthy, *The Rights of Publicity and Privacy* § 4.16 (2d ed. 2000).

[201] Gilson LaLonde & Gilson, *supra* note 198, at § 2B.05.

clearly explain the outer limits of how the biometrics may be used, under which circumstances, and for how long the license is valid.[202] Remedies for likeness licensure violations vary among state statutes and common law doctrines, but generally include injunctive relief, monetary relief, punitive damages, and/or attorney's fees and costs.[203] This Part will argue that biometric identifiers are components of one's likeness that can be subject to improper use and should therefore be subject to licensing agreements.

A. Everyone Has a Right to Control Their Likeness in the Form of Certain Biometrics

Under the common understanding, one's likeness attaches to their resemblance, their personality, and their identity.[204] Biometric identifiers meet these definitions when they capture an individual's physiological, biological or behavioral characteristics that can be used, singly or in combination with each other or with other identifying data, to establish individual identity.[205] While reduced to a purer physiological state than characteristics like personality, biometric identifiers still capture the essential qualities as those traditionally protected by name, image, likeness (NIL) laws.[206] Thus, NIL and publicity laws must also incorporate

---

[202] *See id.*

[203] *See* Gilson LaLonde & Gilson, *supra* note 198, at § 2B.08.

[204] *See* Gignilliat v. Gignilliat, 684 S.E.2d 756, 759–60 (S.C. 2009) (explaining that the right of publicity protects a person's name, likeness, or identity for commercial purposes and is also referred to as wrongful appropriation); *see also* Onassis v. Christian Dior-New York, Inc., 472 N.Y.S.2d 254, 261–63 (N.Y. Sup. Ct. 1984) (describing how a picture conveys not only actuality but also the essence and resemblance of an individual, and that someone's resemblance in a picture can constitute misappropriation of another's identity when the resemblance is exploited to promote deception or confusion). *But see* Burck v. Mars, Inc., 571 F. Supp. 2d 446, 453–54 (S.D.N.Y. 2008) (limiting the application of the right to publicity to living persons and declining to protect "fictitious characters adopted or created by celebrities.").

[205] *See* GDPR, *supra* note 8, art. 4, at 14 ("'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person. . . .").

[206] *See id.*; Matthew G. Perlow, *Protecting Your Name, Image, and Likeness for Long-Term Wealth Preservation*, HUSCH BLACKWELL (June 8, 2023), https://www.huschblackwell.com/newsandinsights/its-more-than-just-a-name-how-to-protect-your-name-image-and-likeness ("The right of publicity is essentially the right to control the commercial use of an individual's name, image, likeness, or other identifiable characteristics. . . .").

and address biometric identifiers.[207]

Every person may be identified according to their facial geometry and thus, is identifiable through facial recognition software.[208] What makes this software so powerful is the accuracy with which it can be used to identify each person.[209] A positive identification can only be accomplished because of the unique combination of features each person's face possesses—how every person possesses some combination that differentiates them from all others.[210]

Although true biometric systems did not emerge at all until the latter half of the twentieth century as a result of the emergence of computer systems, and biometric identifiers did not have everyday applications until the early 2000s,[211] one biometric identifier was protected as a celebrity's "likeness" in the 20th century: Bette Midler's voice.[212] After Ford Motor Co. hired a "soundalike" to imitate Bette Midler in a television advertisement, Midler sued the company for misappropriating her name, image, or likeness under California privacy law.[213] Although Ford Motor Co. did not

---

[207] *See supra* Section IV.D.

[208] See *What is Facial Recognition?*, AMAZON WEB SERVS., https://aws.amazon.com/what-is/facial-recognition/ (last visited Jan. 19, 2024).

[209] *See* William Crumpler, *How Accurate are Facial Recognition Systems – and Why Does It Matter?*, CTR. FOR STRATEGIC & INT'L STUD.: BLOG (Apr. 14, 2020), https://www.csis.org/blogs/strategic-technologies-blog/how-accurate-are-facial-recognition-systems-and-why-does-it ("[F]acial recognition systems can have near-perfect accuracy . . . comparable to the best results of iris scanners.").

[210] *See* Iman Haq & Dillon Murphy, *Facial Recognition in Humans Versus Artificial Intelligence: When Are We Wrong?*, PSYCH. IN ACTION: BLOG, https://www.psychologyinaction.org/facial-recognition-in-humans-versus-artificial-intelligence-when-are-we-wrong/ (last visited Jan. 19, 2025) (explaining that AI recognition software translates a person's facial geometry into a "faceprint" and that identification and verification succeed because each individual has a unique faceprint that can be used to identify the individual).

[211] Stephen Mayhew, *History of Biometrics*, BIOMETRICS RSCH. GRP., INC. (Feb. 1, 2018), https://www.biometricupdate.com/201802/history-of-biometrics-2.

[212] Midler v. Ford Motor Co., 849 F.2d 460, 461, 463–64 (9th Cir. 1988) ("A voice is as distinctive and personal as a face. The human voice is one of the most palpable ways identity is manifested."). For additional analysis on courts' treatment of traits like biometrics in appropriation of one's likeness and right to publicity suits, see White v. Samsung Elecs. Am., Inc., 971 F.2d 1395, 1399 (9th Cir. 1992) (holding that a robot with mechanical features did not constitute a reproduction of Vanna White's likeness but refusing to hold that caricatures or impressions of a person's facial structure [now classified as biometric information] could never become a "likeness"); Carson v. Here's Johnny Portable Toilets, Inc., 698 F.2d 831, 835 (6th Cir. 1983) (acknowledging that a catchphrase is not one's "name or likeness" but is still protected by the right of publicity when used to exploit a person's identity).

[213] *Midler*, *supra* note 212, at 461.

use Midler's name or picture in the commercial, the Ninth Circuit held that Ford Motor Co. misappropriated Midler's identity when it hired a soundalike to closely imitate her "distinctive voice" to sell a product.[214] Although the case predates the modern concept of biometric identifiers,[215] a voice print is considered a biometric identifier today.[216]

Biometric data has a commercial value which differs depending on the context. At the lowest thresholds, one's biometric data is one of millions of records within a database that is sold and queried by a series of customers—one bit of information to support a profitable business service.[217] At some of the highest thresholds, biometrics are pivotal to a person's business product, such as the faces and voices of actors and celebrities.[218] This spectrum of commercial value applies to anyone whose biometric identifiers may be collected and exploited, including any employee whose employer posts their pictures on a website. Each person possesses biometrics which are commercially exploitable, and their likenesses are entitled to the same protections as those of celebrities and public figures.[219]

B. Commercial Misappropriation of Biometric Identifiers

When considering the traditional application of the definition of one's "likeness,"[220] biometric identifiers provide for unique ways in which to misappropriate one's likeness. Biometric identifiers enable malicious actors to emulate one's likeness far beyond finding a soundalike to mimic a celebrity's voice or using a lookalike to pose as a celebrity.[221] They create a portable set of

---

[214] *Id.* at 463–64.

[215] Mayhew, *supra* note 211.

[216] BIPA, 740 ILL. COMP. STAT. 14/10 (2008).

[217] *See* Jon Brodkin, *Clearview AI Aims to Put Almost Every Human in Facial Recognition Database*, ARS TECHNICA (Feb. 17, 2022, 7:00 AM), https://arstechnica.com/tech-policy/2022/02/clearview-ai-aims-to-put-almost-every-human-in-facial-recognition-database/; *see also* Tracy Bielenberg, *Biometric Marketing*, KSM MEDIA, https://ksmmedia.com/intel/biometric-marketing/ (last visited Jan. 19, 2025) (identifying different commercial uses for biometrics, like using facial expressions to determine what features of promotional ads garner the best reactions, and monitoring brainwaves during flights to track how passengers are feeling).

[218] *See supra* notes 211–15 and accompanying text; *see also supra* notes 187–90 and accompanying text.

[219] *See supra* notes 211–15 and accompanying text; *see also supra* notes 187–90 and accompanying text.

[220] *See supra* notes 204–07.

[221] *See generally* Laura Álvarez, *Deepfakes: The New Challenge of Biometric*

information that may be used to generate another's likeness in a convincing emulation, i.e., a set of information that can be used to create a digital rendering of any person's entire identity.[222] Both the collected information and any derivative products generated from that information are subject to misappropriation for, among other things, commercial purposes.[223]

Biometric identifiers are becoming a common component within business processes and transactions. Biometrics have become a method for authenticating a person to log into their bank accounts, to make purchases, or for businesses to generate some form of targeted advertisements.[224] Each of these serve a commercial purpose because they are designed to either complete a transaction or to otherwise engage in a marketplace of some form.[225] Targeted advertisements are a clear example of misappropriating biometric information for a commercial purpose, since targeted advertisements are used to generate income for the

Authentications, RECORDIA (Feb. 2024), https://recordia.net/en/deepfakes-the-new-challenge-of-biometric-authentications/. ("[D]eepfakes can exploit [biometric] characteristics by convincingly replicating them. For example, an attacker could use a deepfake to fool a facial recognition system into believing that a fake image or video is an authentic representation.").

[222] While deepfakes are not the type of misappropriation employers are likely to commit using employees' biometric data, deepfake technology poses a serious threat to any person whose biometric data is accessible to malicious actors. For more information, see Forrest v. Meta Platforms, Inc., No. 22-cv-03699-PCP, 2024 U.S. Dist. LEXIS 107340, at *3–4 (N.D. Cal. June 17, 2024) (lawsuit detailing how the use of deepfake videos depicting a well-known Australian businessman and philanthropist endorsing fraudulent cryptocurrency schemes caused the plaintiff reputational harm and financial losses); *What the Heck is a Deepfake?* UNIV. VA. INFO. SEC., https://security.virginia.edu/deepfakes (last visited Oct. 2, 2024) (discussing potential consequences of emerging deepfake technology for individuals and society); Ricardo Amper, *New Technologies are Helping to Identify Sophisticated AI Deepfakes. Here's How*., WORLD ECON. F. (Jan 4, 2024), https://www.weforum.org/agenda/2024/01/in-an-increasingly-fake-world-biometrics-technology-can-help-you-prove-your-identity (acknowledging the increasing threat of deepfake technology and discussing the intersection of deepfakes and biometric authentication methods).

[223] *See supra* notes 217–19 and accompanying text.

[224] *5 Reasons to Use Biometrics to Attract More Business*, AWARE BIOMETRICS, (Feb. 15, 2024), https://www.aware.com/blog-5-reasons-to-use-biometrics-to-attract-more-business. *See generally* Press Release, Fed. Trade Comm'n, FTC Warns About Misuses of Biometric Information and Harm to Consumers (May 18, 2023) (on file with author).

[225] *See generally* Therese Stowell, *How Biometrics Are Transforming the Customer Experience*, HARV. BUS. REV. (Mar. 29, 2023), https://hbr.org/2023/03/how-biometrics-are-transforming-the-customer-experience (explaining how the use of biometrics can improve customer experience in business transactions).

company selling a product or for the company effectuating the advertisements.[226] While there are conceptual differences between businesses using biometrics to increase customers' efficiency in account accessibility, and using biometrics to track consumers and directly target them with advertisements,[227] both uses still further commercial purposes by facilitating business transactions.[228]

Finally, the simple process of collecting and using biometrics as part of a standard business practice is a commercial purpose.[229] When a security company collects an individual's biometric data and uses that data in a commercially available authorization/identification process, the third-party security company is profiting from the collection and use of biometrics.[230] Any company who collects biometric data and provides it to another in return for anything of value (services, money, or goods) is using those biometrics for a commercial purpose.[231]

Commercial use of biometric information is an inappropriate use of information if the subject of the biometrics does not provide consent.[232] Without consent, the company has no grounds to use the person's identity for their own purposes. The business also misappropriates the person's likeness if they do not compensate the person or provide some form of consideration in return for the biometric information.[233] Without consideration, any agreement

---

[226] *See* Tracy Bielenberg, *Biometric Marketing*, KSM, https://ksmmedia.com/intel/biometric-marketing/ (last visited Oct. 18, 2024) (explaining how "biometric marketing" is advancing with modern technologies and being used by companies to enhance advertising techniques).

[227] *Compare* Catharina Eklof, *The Future of Payments: Biometrics Within the Financial Eco-system,* BIOMETRIC UPDATE (Nov. 9, 2022, 12:56 PM), https://www.biometricupdate.com/202211/the-future-of-payments-biometrics-within-the-financial-eco-system (suggesting that using biometrics for two-factor authentication is convenient for consumers), *with* Bielenberg, *supra* note 226 (describing the use of biometric information to track consumer emotional responses such as heart rates, facial expressions, and eye movements).

[228] *See* Right of Publicity Act, 765 ILL. COMP. STAT. 1075/5 (1999) (defining "commercial purpose" to include the use of an individual's identity for advertising or promoting products, which can generate income for the company selling the product or effectuating the advertisements).

[229] *Compare* 765 ILL. COMP. STAT. 1075/5 (1999), *with* BIPA, 740 ILL. COMP. STAT. 14/15(c) (2008).

[230] *Compare* 765 ILL. COMP. STAT. 1075/5 (1999), *with* BIPA, 740 ILL. COMP. STAT. 14/15(c) (2008).

[231] BIPA, 740 ILL. COMP. STAT. 14/15(c). *See generally* Stacy-Ann Elvy, *Commodifying Consumer Data in the Era of the Internet of Things*, 59 B.C. L. REV. 423, 512 (2018) (addressing concerns with "direct sales of consumer data" and the Illinois BIPA).

[232] *See infra* Section VI.B.ii.

[233] *See* RESTATEMENT (SECOND) OF CONTRACTS § 71 (AM. L. INST. 1981)

reached would be invalid and would unjustly enrich the business appropriating the biometric information.[234] Simply put, a business who collects and uses a person's biometric information without properly obtaining their consent and appropriately compensating them misappropriates that person's likeness.

VI. PROPOSED STATUTORY REQUIREMENTS FOR BIOMETRIC LICENSING AGREEMENTS BETWEEN EMPLOYERS AND EMPLOYEES

As each person may license their own likeness, each employee may license their likeness via the collection and use of their biometric information with their employer.[235] The process of obtaining that license should encompass certain criteria to protect the privacy rights of the employee, while still providing the employer some flexibility to use their employee's likeness for commercial purposes.

A. Consent Challenges and Approaches

The issue of true consent must be considered before any potential licensing scheme granting employers the use of employees' biometrics can be developed. Regulations have regularly recognized the potential damage that may result from the exposure of sensitive information, including biometrics.[236] To guard against the potential damage such exposure could cause, these regulations require consent by the subject of the data—the person to whom the sensitive information describes or relates—before the data can be collected or disclosed.[237]

Employers commonly obtain consent from their employees to collect and store personally identifiable information using

(explaining the meaning of consideration in contract formation).

[234] RESTATEMENT (THIRD) OF RESTITUTION & UNJUST ENRICHMENT §§ 36, 38–39 (AM. L. INST. 2011).

[235] *See supra* Section V.B.

[236] *See generally* DHHS Administrative Data Standards and Related Requirements, 45 C.F.R. §160.103 (2024) (commonly known as the Health Insurance Portability and Accountability Act (HIPAA)); FTC Children's Online Privacy Protection Rule, 16 C.F.R. §§ 312.8, 312.10 (2024); Financial Services Modernization Act (Gramm-Leach-Bliley) of 1999, 15 U.S.C. § 6801; Family Educational Rights and Privacy Act (FERPA) of 1974, 20 U.S.C. §1232g(b)(1); BIPA, 740 ILL. COMP. STAT. 14/15(a) (2008); CCPA, CAL. CIV. CODE § 1798.82(g)–(h) (West 2024); GDPR, *supra* note 8.

[237] 45 C.F.R. § 164.508(a)(1) (2024); 16 C.F.R. § 312.5(a) (2024); 15 U.S.C. § 6802; 20 U.S.C. § 1232g(b)(1)–(2), (d); BIPA, 740 ILL. COMP. STAT. 14/15(b) (2008); CCPA, CAL. CIV. CODE § 1798.82(g)–(j) (2024); GDPR, *supra* note 8, at 1, 6.

standardized forms during onboarding to facilitate the employee's background screening, their pay and tax elections, and any information necessary for benefits to the employee.[238] Obtaining consent to collect biometric information of the employee could follow a similar model in which consent is obtained via a standardized form. However, the hypothetical form and subsequent release would have to reflect that the employee gave true consent—that employment was not conditioned upon consent and that the employee had a true choice whether to allow their employer to use their biometric information.

Not all consent is viewed equally. Consent can be understood as "a continuum that includes some level of coercion and some level of choice."[239] The European Union recognizes an imbalanced relationship in an employer-employee situation because the employer wields more power than the employee.[240] Since consent must be freely given, the significant power imbalance between employers and employees may result in situations where the employer cannot rely on the employee's consent to use their data unless the consent is in the interest of the employee.[241]

i. Consent Under Europe's GDPR

The European Union's General Data Protection Regulation (GDPR) sets a high standard for what constitutes consent regarding biometric data.[242] It stipulates that the person granting consent must provide an indication of the data subject's wishes or

---

[238] *See, e.g.*, *What Employers Need to Know About Employee Data Privacy*, VENSUREHR: BLOG (July 27, 2024), https://www.vensure.com/resources/blog/employee-data-privacy-what-employers-need-to-know/ ("Employers should disclose how they collect, process, and share employee data. You can have employees sign a consent form outlining this process either with their employment contract or within your employee handbook.").

[239] Maayan Niezna & Guy Davidov, *Consent in Contracts of Employment*, 86 MOD. L. REV. 1134, 1136 (2023).

[240] *See Working Party Guidelines on Consent Under Regulation 2016/679*, at 6–7 (Nov. 28, 2017), https://ec.europa.eu/newsroom/article29/redirection/document/51030 (discussing the power imbalance between employers and employees, and the corresponding consent issues under the GDPR); *see also* GDPR, *supra* note 8, art. 88 (emphasizing the need for protection of the specific interests of employees is emphasized and creating the possibility for derogations in Member State law is created).

[241] *See Working Party Guidelines on Consent Under Regulation 2016/679*, *supra* note 240.

[242] *See id.* at 32–33, 43.

intention that is (1) freely given; (2) specific; (3) informed; and (4) unambiguous.[243] Freely given consent is that of real choice and control by the person granting the consent; consent is not freely given and is thus invalid where a person feels compelled to grant consent or endure negative consequence.[244] The "freely given" requirement is particularly salient when there is an imbalance between the parties.[245]

In addition to freely given, consent under the GDPR must be specific and informed.[246] The consent provided must be a specific opt-in for that intended purpose and separate each intended purpose by requiring separate consent for each purpose.[247] Each of those purposes must reach a determination to fulfill a specific, explicit, and legitimate purpose.[248] Informed consent requires that the person understand to what they are agreeing.[249] A reasonable degree of transparency is required for the person to make informed decisions based on an understanding of accessible information.[250] Providing information to satisfy informed consent is often accomplished in the form of notices or statements that are made in clear and plain language which is easily understood by the average person.[251] This information cannot be hidden nor obscured in a way that would make it difficult to locate or understand (e.g., placing information relevant to consent within general terms and

---

[243] GDPR, *supra* note 8, at Recital 32.

[244] *Opinion of the Working Party on the Protection of Individuals with Regard to the Processing of Personal Data on the Definition of Consent*, at 12–13 (July 13, 2011), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf.

[245] *See id.*, GDPR, *supra* note 8, at Recital 42 ("Consent should not be regarded as freely given if the data *subject* has no genuine or free choice or is unable to refuse or withdraw consent without detriment.").

[246] GDPR, *supra* note 8, art. 5.

[247] *See id.* art. 6, 1.

[248] *See id.*; *Opinion of the Working Party on the Protection of Individuals*, *supra* note 244, at 15–17 ("For these reasons, a purpose that is vague or general, such as for instance 'improving users' experience', 'marketing purposes', 'IT-security purposes' or 'future research' will - without more detail - usually not meet the criteria of being 'specific.'").

[249] *See* GDPR, *supra* note 8, art. 7; *Opinion of the Working Party on the Protection of Individuals*, supra note 244, at 9 ("To be valid, consent must be informed. This implies that all the necessary information must be given at the moment the consent is requested, and that this should address the substantive aspects of the processing that the consent is intended to legitimise.").

[250] *See* GDPR, *supra* note 8, art. 12, at 1 (requiring that information relating to the processing of data be communicated to the subject "in a concise, transparent, intelligible and easily accessible form, using clear and plain language.").

[251] *See id.*

conditions).[252] This provided information must also consider the audience to which it is being presented.[253]

Finally, under the GDPR, unambiguous indication of the person's wishes must clearly demonstrate that the person is consenting to a particular purpose.[254] This must be in the form of a statement or a clear affirmative action.[255] A clear affirmative act requires the person to take a deliberate action to consent to the particular purpose.[256] When consent is to be provided electronically, a request for consent should not be unnecessarily disruptive to the use of the service requiring consent.[257] Additionally, any forms regarding consent may not have any boxes pre-ticked or have opt-out mechanisms that require intervention by the person granting consent to prevent agreement.[258] Regardless of mechanism or medium, it must be clear that the person granting consent is clearly doing so.[259]

ii. Consent Under Illinois' BIPA

Like the GDPR, BIPA requires consent to be specific, informed, and unambiguous.[260] BIPA further requires that, for consent to be valid, private companies must (1) inform the person that a biometric identifier will be collected or stored in writing; (2) provide, in writing, the specific purpose and length of time the data will be collected, stored, and used; and (3) obtain a written release executed by the subject.[261] Unlike the GDPR, though, BIPA mandates all disclosures and releases to be in writing.[262] BIPA

---

[252] *Id.*

[253] *See id.* ("The controller shall take appropriate measures to provide any information . . . relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child.").

[254] *Id.* at Recital 32.

[255] *See* GDPR, *supra* note 8, at Recital 32.

[256] *See id.*

[257] *Id.*

[258] *See id.*; *see also Working Document of the Working Party Providing Guidance on Obtaining Consent for Cookies* 3–5 (Oct. 2, 2013), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp208_en.pdf (discussing the importance of consent as informed, specific, timely, and assented to affirmatively in the context of consumer cookie usage).

[259] *See supra* notes 254–38 and accompanying text.

[260] *Compare* GDPR, *supra* note 8, at Recital 32, *with* BIPA, 740 ILL. COMP. STAT. 14/15(b) (2008).

[261] BIPA, 740 ILL. COMP. STAT. 14/15(b) (2008).

[262] *Compare* GDPR, *supra* note 8, at Recital 32 ("Consent should be given by a

falls short of the GDPR, however, by failing to require that the consent "be freely given."[263]

iii. Consent in Proposed Statutory Framework

Though these regulations differ, they may instruct on the degree of consent that should be required with respect to the use of facial recognition technology. BIPA, when supplemented with the "freely given" requirement, would set a high standard for consent,[264] a standard that should be required in relationships where there is a substantial imbalance of power, like that of an employer and employee.[265] The GDPR, lacking the stringent written memorialization requirements,[266] generally provides an intermediate standard of consent that should be required where power imbalance is a lesser concern, like when a person's presence on a commercial property may be incidental to a purpose other than direct employment, like visitors or contractors.[267]

Obtaining freely given, informed consent from an employee may be dubious. For consent to be freely given, it must be given "with an opportunity for the individual to refuse consent without detriment, as well as being offered a suitable alternative."[268] Any employee faces pressures when negotiating with their current or prospective employer; pressures which may induce that employee to agree to something they may otherwise reject but for the perception that they will lose their job if they do not agree.[269] If an

---

clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement . . . such as by a written statement . . . or an oral statement."), *with* BIPA, 740 ILL. COMP. STAT. 14/15(b) (2008) (requiring any private entity seeking to collect a person's biometric information to first (1) informs the subject in writing that biometric information is being stored and collected; (2) informs the subject in writing of the specific purpose and length of term for which the information is being collected, stored, and used; and (3) receives a written release executed by the subject).

[263] *Compare* BIPA, 740 ILL. COMP. STAT. §14/15 (2008) (requiring only "consent" for collection, storage, use, and disclosure of biometric information), *with* GDPR, *supra* note 8, art. 4, at 11 (requiring that consent be freely given).

[264] *See supra* notes 260–63 and accompanying text.

[265] *See supra* notes 242–45 and accompanying text.

[266] *See supra* note 262 and accompanying text.

[267] *See supra* notes 242–45 and accompanying text; *see supra* notes

[268] Niamh Millais, *ICO Issues Updated Guidance on Using Biometric Data in Monitoring Workers*, SHOOSMITHS (Apr. 3, 2024), https://www.shoosmiths.com/insights/articles/ico-issues-updated-guidance-on-using-biometric-data-in-monitoring-workers.

[269] *See generally* Remberto Castro-Castañeda et al., *Job Insecurity and Company Behavior: Influence of Fear of Job Loss on Individual and Work Environment Factors*, INT'L J. ENV'T RSCH. & PUB. HEALTH (Feb. 17, 2023),

employee perceives providing consent over their biometric data as a prerequisite to maintaining or gaining employment, showing that consent was freely given would prove challenging.[270] An employer may proactively obtain true consent by providing employees with alternative options to biometric data and making it clear that an employee is free to select whichever option they prefer without consequence.[271]

Consent may be questionable even if it is voluntarily given if the consent is based on inadequate information. Should the employee not receive information on how the biometric information may be used, the employee would lack any manner of understanding how far, and to what purposes, their identity may be used.[272] Consent granted in such a situation would fail to be specific or informed as to the purpose or use of the biometrics, and would thus prevent an individual from genuinely exerting control over their biometric information.[273] Consent would also be invalidated if the use of the employee's biometric data exceeded the specific uses the employee consented to.[274] Moreover, particularly because an employee-employer relationship is ongoing, valid consent must include the ability to withdraw consent easily, at any time.[275] Ideally, an

---

https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9959084/ (discussing the repercussions that job insecurity has on employees physical and mental health and how it is strongly linked to individual factors and the work environment).

[270] Tim Hickman, *Processing Biometric Data in the Workplace*, 25 PRIV. & DATA PROT. 3, 3 (2024) ("[I]in a workplace context, it can be very difficult to show that consent has been 'freely given,' due to the imbalance that often exists between an employer and an employee.").

[271] *Id.*

[272] *See supra* notes 246–53 and accompanying text.

[273] *See* Sarah Shelley, *Understanding the Ethics of Data Collection and Responsible Data Usage*, U. CUMBS.: BLOG (June 20, 2024), https://www.ucumberlands.edu/blog/understanding-the-ethics-of-data-collection (discussing that transparency to human subjects is crucial to data collection ethics and the relation between transparency and a subject's ability to exert control over their data and privacy).

[274] *See* GDPR, *supra* note 8, art. 5, at 1 ("Personal data shall be . . . collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes."); *see also* Aryamala Prasad, *Unintended Consequences of GDPR: A Two-Year Lookback*, GW REGUL. STUD. CTR. (Sept. 3, 2020), https://regulatorystudies.columbian.gwu.edu/unintended-consequences-gdpr (stating that organizations "may be in violation of the purpose limitation principle . . . [restricting] businesses from processing data more than required for the initial purpose."); *Consent*, INTERSOFT CONSULTING, https://gdpr-info.eu/issues/consent/ (last visited Mar. 28, 2025).

[275] *See* GDPR, *supra* note 8, at Recital 42 ("Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment."); Ann Bevitt, *Watching You – Watching*

agreement founded in consent would benefit both employees and employers by allowing employees to exercise their rights over their identity and allowing the employer to legally and ethically collect employees' biometric data.[276]

The best available mechanism for accomplishing this arrangement would come in the form of a written licensure agreement between the employer and employee regarding the collection, use, and eventual disposal of the employee's likeness in the form of their biometric information.[277] To provide for truly informed consent, the terms of that licensure agreement should include a notice to the employee stating which biometric information will be collected, how it will be collected, when it will be collected, how it will be used, and how the employer will dispose of the biometrics. Additionally, the license should establish a specific purpose that is unambiguous and therefore capable of receiving specific consent.[278] Finally, the licensure should establish ramifications if the terms of the license are violated (e.g., the employer sells the biometric information despite a term prohibiting that sale).[279] Within this context, the employee may freely give their consent to their employer.

B. Required Elements for Proposed Employer/Employee Biometric Statutory Licensing Framework

To appropriately balance the competing interests in licensing

---

Me — The ICO's New Guidance on Employee Monitoring, 23 PRIV. & DATA PROT. 10, 12 (2023) ("[E]mployees are likely to feel that they have no choice but to give consent if asked, and that employees must have the option to withdraw their consent without detriment. Accordingly, consent is only appropriate in circumstances where employees have a genuine choice and control over the monitoring.").

[276] *See supra* text accompanying notes 26–30, 235–36; *see* Cristina Del Rosso, *supra* note 145, at 26–29 (discussing the advantages biometric collection offers to employers and explaining why employee consent and control over information is vital)

[277] *See* discussion *supra* Section IV.D (analyzing the benefits of licensing agreements to licensees and licensors).

[278] *See* GDPR, *supra* note 8, art. 4, at 11 (defining consent as "freely given, specific, informed and unambiguous indication of the data subject's wishes. . . ."); *Opinion of the Working Party on the Protection of Individuals*, *supra* note 244, at 17–19 ("Consent must be given in relation to the different aspects of the processing, clearly identified. It includes notably which data are processed and for which purposes. This understanding should be based on the reasonable expectations of the parties. 'Specific consent' is therefore intrinsically linked to the fact that consent must be informed.").

[279] *See infra* notes 443–47 and accompanying text (discussing the importance of adequate enforcement in licensing schemes).

agreements between employers and employees, and to ensure that employees are given adequate privacy protections and can provide informed consent, each of the following elements should be incorporated into any statutory scheme regulating employee biometric licensure:

i. Establish which biometric information is to be collected;
ii. Establish the purpose(s) for which the collected biometrics may be used;
iii. Establish specificity regarding the collection of the biometric information (who, when, and how);
iv. Establish specificity regarding the storage of biometric information;
v. Establish the timeframe for retaining the biometric information;
vi. Establish all criteria by which the licensure terminates;
vii. Establish specificity regarding disposal;
viii. Establish any penalties for failure to comply with the license's terms; and
ix. Establish any consideration the employee receives pursuant to this licensure.[280]

Each suggested required element is pivotal to correcting the power imbalance between employers and employees, as is necessary for any licensing agreement to be fair and valid. This Section will thus analyze the importance of each element.

i. Establish Which Biometric Information Is to Be Collected

There are many different forms and types of biometric information.[281] Only a subset of this information fits within a reasonable interpretation of one's likeness.[282] The biometric information which may be relevant to an employer is facial geometry, iris scans, retina scans, and fingerprints.[283] The license

[280] *See infra* Section VI.B.i–ix (explaining each of the nine suggested requirements and justifying their importance).

[281] *See* BIPA, 740 ILL. COMP. STAT. 14/10 (2008) (defining biometric identifiers and biometric information).

[282] *See* Zahra Takhshid, *Data as Likeness*, 112 GEO. L.J. 1161, 1181–85 (2024) (analyzing how the common law definition of likeness has expanded over time and arguing that the definition should be expanded to cover biometric information not currently protected by the tort).

[283] *See* Emily K. Arida, Student Scholarship, *Biometrics in Employment Guidance "BEG": Best Practices for Employers Begging to Use Biometrics in the*

should explain which of these biometric identifiers, or which combination of these biometric identifiers, will be collected from the employee.[284] The license should moreover define these biometric identifiers to remove any ambiguity of what is being collected and to ensure that all parties agree on what constitutes each biometric identifier.[285] Finally, the license should limit the collection so that only the specified biometric identifiers may be collected or the terms under which these collections may expand.

ii. Establish the Purpose(s) for Which the Collected Biometrics May Be Used

Biometrics should only be collected and used for clearly articulated purposes.[286] Acceptable purposes may include use for employee authentication purposes or as test data for specific software or products the employer develops, but acceptable uses are more properly considered any purpose so long as that purpose is clearly communicated in the license.[287] The license should also clearly communicate that only the articulated purposes are permissible under the license.[288] Under this element, the license should also provide limits on what uses are clearly prohibited.[289] Should the employee want to prohibit the sale, sharing, or any other distribution of their biometric information, that, too, should be clearly explained.

iii. Establish Specificity Regarding the Collection of Biometric Information (Who, When, and How)

Specificity around the collection is important to understanding

---

Workplace, 60 WASHBURN L.J. 313, 316–17 (2021).

[284] *See id.* at 317.

[285] Kevin J. Cassato, Note, *Unfair, Uninformed, and Undoable-Replacing Unenforceable Adhesion Contracts for Consumer Biometric Data with Uniform Standards*, 2023 U. ILL. J. L. TECH. & POL'Y 83, 87 (2023).

[286] *See* Cynthia M. Ho, *Patent Breaking or Balancing?: Separating Strands of Fact from Fiction Under TRIPS*, 34 N.C. J. INTELL. L. & COM. REGUL. 371, 434–35 (2009).

[287] *See* Jacey Norris, Case Note and Comment, *Art or Artifice: The Second Circuit's Misapplication of the Fair Use Factors in* Cariou v. Prince *in Light of* Kienitz v. Sconnie Nation, 25 DEPAUL J. ART TECH. & INTELL. PROP. L. 429, 456 (2015).

[288] *See* Ho, *supra* note 286, at 394.

[289] *See* Lauren Katzenellenbogen et al., *Alternative Software Protection in View of* In re Bilski, 7 NW. J. TECH. & INTELL. PROP. 332, 336 (2009).

the initial disposition of that biometric information.[290] The employee should understand whether the employer will be conducting the collection or whether it will be a third party.[291] If a third party is collecting the biometrics, then the employee should understand who that third party is and whether they are subject to the same terms as the employer.[292] As a general guide, the life of biometric data should be limited to the time of employment between employer and employee.[293] As such, collection should take place only after the person begins employment. The license should also provide the mechanisms for collecting the biometric information.[294] For example, if the employee is to submit a picture for the employer to be subject to facial recognition software, that should be specified. Both the employer and employee should understand the specifics of the collection prior to it taking place.

iv. Establish Specificity Regarding the Storage of the Biometric Information

Providing subjects with specificity about how their biometric information will be stored after collection is as important as the collection itself.[295] The same concerns surrounding the collection of

---

[290] *See* N. Cameron Russell et al., *Privacy in Gaming*, 29 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 61, 85 (2018).

[291] *See* Andrew Schuman, Note, *Who's Checking? A Proposal to Protect Employee Health Screening Data*, 39 HOFSTRA LAB. & EMP. L.J. 177, 183–84 (2021).

[292] *See* Sarah Hunt-Blackwell, Comment, *You Have the Right to Remain Private: Safeguarding Biometric Identifiers in Civil and Criminal Contexts*, 24 TUL. J. TECH. & INTELL. PROP. 205, 207–08 (2022).

[293] *See* BIPA, ILL. COMP. STAT. 14/15 (2008) ("A private entity in possession of biometric identifiers or biometric information must . . . permanently destroy[] biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first."); TEX. BUS. & COM. CODE ANN. § 503.001(c-2) (West 2024) (establishing a presumption that the purpose of an employer's use and storage of biometric information ends when the employment relationship is terminated); *see also* Arida, *supra* note 283, at 313 (stating that employers should delete employees' biometric information when the information is no longer needed or when the employment relationship ends).

[294] *Cf.* Adrian K. Felix et al., *Consumer Data Collection and Privacy: Best Practices and Risk Mitigation Strategies for Franchise Systems*, 42 FRANCHISE L.J. 445, 449 (2023) (emphasizing the importance of data subjects' informed consent on collection methods used by companies collecting personal data); Kirsten Flicker, Note, *The Prison of Convenience: The Need for National Regulation of Biometric Technology in Sports Venues*, 30 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 985, 1012–13 (2020).

[295] *See How Do We Keep Biometric Data Secure?*, INFO. COMMR'S OFF.,

biometric information—whether the employer or third party possesses the biometric information and the treatment of that biometric information—also apply here but warrant additional terms in the license.[296] Both the employer and employee should understand where the biometric information is and how to reach it.

v. Establish the Timeframe for Retaining the Biometric Information

Biometric information collected from employees by employers is relevant to an employer only as long as the employee remains within the employer's employ, and perhaps shortly afterward.[297] Therefore, the employer has no cause to possess the biometric information of former employees and the employer should therefore take reasonable means to ensure that they do retain employees' biometric information past employment termination.[298] A reasonable timeframe—no more than fourteen calendar days—should be provided to allow employers to delete biometric information of former employees to account for the complexities of a business's records and the due diligence required by the process.[299] Retaining the biometric information outside the limits of this timeframe risks misappropriation of the employee's likeness and exposes the employee to unnecessary risk associated with data and information security breaches and disclosures.[300]

---

https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/how-do-we-keep-biometric-data-secure/ (last visited Oct. 19, 2024).

[296] *See* Kelsey Atherton, *The Enduring Risks Posed by Biometric Identification Systems*, BROOKINGS (Feb. 9, 2022), https://www.brookings.edu/articles/the-enduring-risks-posed-by-biometric-identification-systems/ (discussing consequences of an entity's failure to protect biometric information using adequate storage methods and confidentiality procedures); *Facing the Risks: Biometric Data*, MALK PARTNERS (Jan. 30, 2024), https://malk.com/facing-the-risks-biometric-data/ (suggesting that companies inform individuals of how and why their biometric information is collected and stored due, in part, to the potential for misuse and unauthorized access of the individuals' biometric information).

[297] *See* Carla Llaneza, Comment, *An Analysis on Biometric Privacy Data Regulation: A Pivot Towards Legislation Which Supports the Individual Consumer's Privacy Rights in Spite of Corporate Protections*, 32 ST. THOMAS L. REV. 177, 183 (2020).

[298] *See supra* notes 475–82 and accompanying text.

[299] *See supra* notes 480–82 and accompanying text

[300] *See* Mark P. McKenna, *The Right of Publicity and Autonomous Self-Definition*, 67 U. PITT. L. REV. 225, 287–88 (2005).

vi. Establish All Criteria by Which the Licensure Terminates

Each of the ways in which the license may automatically terminate should also be explained, including those outside the timeframe of employment.[301] The license should establish under what circumstances the employee's consent to the employer's use of their biometric information may be revoked.[302] Alternatively, if the employee cannot revoke consent during employment, the license should stipulate as much. What that revocation, if any, looks like should also be explained (e.g., whether the employee can rely on oral revocations or must submit those revocations in writing or through a specific process).

vii. Establish Specificity Regarding Disposal

Both the employer and employee should understand the disposal process and the actors involved in that process up to, and including, the confirmation that the biometric information ceases to exist.[303] Disposal methods should be sufficient to meet the then-current standards for information security practices to either destroy the information (e.g., breaking or crushing a hard drive) or render it unintelligible (e.g., encrypt and wipe the data in an irretrievable way).[304]

viii. Establish Any Penalties for Failure to Comply with the License's Terms

A license holds little binding power without some consequence for failing to adhere to its terms.[305] It is the inclusion of punitive terms that truly balances the relationship between employer and

---

[301] *See* Peter B. Maggs, *License Contracts, Free Software and Creative Commons in the United States*, 62 AM. J. COMPAR. L. 407, 409 (2014).

[302] *See* Marcia M. Boumil et al., *Prescription Data Mining, Medical Privacy and the First Amendment: The U.S. Supreme Court in* Sorrell v. IMS Health Inc., 21 ANNALS HEALTH L. 447, 456 (2012).

[303] *See* Joshua Valentino, Note, *Setting the Framework for Biometric Privacy Legislation After the "Big Bang" of Biometrics in the Workplace*, 38 HOFSTRA LAB. & EMP. L.J. 167, 177 (2020).

[304] *See Proper Disposal of Electronic Devices*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY: BLOG (Feb. 1, 2021), https://www.cisa.gov/news-events/news/proper-disposal-electronic-devices.

[305] *See* Collins v. Brown, 268 F. Supp. 198, 201 (D.D.C. 1967) ("The purpose of punishment, be it a criminal sentence, a civil penalty, or punitive damages, is not to inflict suffering or to impose a loss on the offender. Its object is to act as a deterrent: first to discourage the offender himself from repeating his transgression; and, second, to deter others from doing likewise.").

employee. Disposal penalties should establish an amount to be paid for each day the biometric information is retained beyond the termination period. Penalties should not, however, only apply to improper disposal of biometric information, but should provide for a failure to follow any of the statutory elements (e.g., a violation of the type of biometrics the employer may collect and use pursuant to the license at issue). The penalties should establish reasonable, but unignorable, outcomes for failing to adhere to the terms of the license. The license would need to be careful not to unreasonably overextend these penalties; doing so may invalidate them should the employee ever need to enforce these terms.[306]

ix. Establish Any Consideration the Employee Receives Pursuant to this Licensure

Finally, the license must identify consideration to be given to the employee. A license permitting an employer to collect and use an employee's biometric information requires consideration to be given to the employee in return for their reduced privacy and to compensate the employee for the appropriation of their likeness.[307] Should the circumstances warrant it, or if both parties agree, additional consideration may be provided in return for further use of the employee's biometric information. Such situations may involve additional compensation for broader use of an employee's biometrics (i.e. outside of workplace identity authentication systems) or when the employer uses the biometric information in a particularly intrusive manner.[308]

Looking at consideration, an employee must be afforded a true

---

[306] *See* State Farm Mut. Auto Ins. Co. v. Campbell, 538 U.S. 408, 416 (2003) ("While States possess discretion over the imposition of punitive damages, it is well established that there are procedural and substantive constitutional limitations on these awards. . . . The Due Process Clause of the Fourteenth Amendment prohibits the imposition of grossly excessive or arbitrary punishments. . . ."); *see also* Breuder v. Bd. Trs. Cmty. Coll. Dist. No. 502, 888 F.3d 266, 269 (7th Cir. 2018) ("Courts in Illinois regularly refuse to enforce particular clauses—say, those creating penalties or imposing unreasonable restraints on competition after the end of employment—while enforcing the remainder of the contracts."); United States v. Alshabkhoun, 277 F.3d 930, 934 (7th Cir. 2002) (stating that a stipulated penalty is not enforceable if it is unreasonable or is against public policy); Jefferson Standard Life Ins. Co. v. Adams, 129 F.2d 431, 435 (6th Cir. 1942) (holding that, in Kentucky, surrender charges are void as they are against public policy and unreasonable).

[307] *See* Evan Darryl Walton, *Avoiding Pitfalls: Employer Contractual and Compensation Lessons for Modifying the Employment Relationship*, 8 WAKE FOREST L. REV. ONLINE 27, 31 (2018).

[308] *See id.* at 29.

opportunity to decline to provide their biometrics.[309] An existing employee may be provided an appropriate severance or a voluntary transfer into a role or situation that does not require the collection of biometrics if they wish to decline. If an employee is being onboarded for a role, refusal to license their biometrics may result in the prospective employee being denied the position. Such a situation would necessitate early notice to job candidates that the role in question will require the use of biometrics (e.g., include a notice in the job posting), thereby allowing applicants to decline licensure by refraining from applying for roles requiring biometric collection and use. Similarly, provided notice is given to applicants, while an employer should not solicit from a candidate their willingness to provide their biometrics, the employer should have a right to terminate the employment or hiring process of a new employee who is not willing to license their biometric information.

These nine elements should be present in any license in which an employee is permitting their employer to appropriate their likeness via their biometric information. Incorporating all nine elements balances the dynamic between the employer and employee by affording the employee limitations and clarity on the use of their likeness. These limitations prevent, or mitigate, an intrusion into the employee's privacy rights.

VII. ASSESSING RECOMMENDATIONS AGAINST EXISTING PRIVACY LAWS

While the proposed statutory licensure framework extends beyond current law, consideration must be given to how the proposed statutory licensure framework intersects or conflicts with current law. Currently, the Illinois Biometric Privacy Act (BIPA), the California Privacy Protection Act (CPPA), and the European Union General Data Protection Regulation (GDPR) are the laws concerning privacy that most significantly impact the United States.[310] Each aligns and potentially conflicts with some

---

[309] *See* Amy Olsen, Comment, *Family Leave Legislation: Ensuring Both Job Security and Family Values*, 35 SANTA CLARA L. REV. 983, 1006–07 (1995); Abraham Tabaie, Note, *Protecting Privacy Expectations and Personal Documents in SEC Investigations*, 81 S. CAL. L. REV. 781, 816 (2008); Marcy E. Peek, *Information Privacy and Corporate Power: Towards a Re-Imagination of Information Privacy Law*, 37 SETON HALL L. REV. 127, 164 (2006).

[310] *See* Billee Elliott McAuliffe et al., *Privacy Regimes for Protecting Biometric Information*, LEWISRICE (Sept. 2019), https://www.lewisrice.com/publications/privacy-regimes-for-protecting-

pieces of these recommendations. By examining how each interact with this Article's proposals, conflicts of law may be more adequately examined and addressed.

A. Illinois Biometric Information Privacy Act (BIPA)

The Biometric Information Privacy Act (BIPA) is the sole avenue for residents of Illinois seeking to protect their biometric information.[311] One unique issue BIPA addresses is that, unlike other personal information, biometrics cannot be changed, and biometrics thus require substantial protections.[312] Lawmakers have made several attempts, and continue to attempt, to weaken BIPA's protections by requiring those protections to yield to security purposes and rights of action.[313] The recommendations suggested in this Article closely align with the strong provisions of BIPA as unamended.[314] The only conflict which may exist between these recommendations and BIPA are those regarding the ban on profiting from biometric data.[315] The remaining six of the seven components of BIPA are aligned with these recommendations, as outlined below.

i. Biometric Identifiers Defined

BIPA provides several definitions that have been incorporated throughout these recommendations. BIPA defines a "biometric identifier" as only one of the following: (1) a retina or iris scan; (2)

---

biometric-information/ (identifying the GDPR, BIPA, and the CCPA as major biometric privacy laws); *Consumer Data Privacy Laws*, BL, https://pro.bloomberglaw.com/insights/privacy/consumer-data-privacy-laws/#the-need-for-privacy-laws (last visited Feb. 1, 2025) (explaining how the GDPR and other privacy laws impact consumer data protection); *Is Biometric Information Protected by Privacy Laws*, BL (June 20, 2024), https://pro.bloomberglaw.com/insights/privacy/biometric-data-privacy-laws/#what (explaining how BIPA protects biometric data for consumers); *see also* BIPA, 740 ILL. COMP. STAT. 14/1–14/99 (2008); GDPR, *supra* note 8, at 1; CCPA, CAL. CIV. CODE §§ 1798.100–1798.199.100 (2024).

311 *See Biometric Information Privacy Act*, supra note 94 ("BIPA is the one recourse Illinoisans have to control their own fingerprints, facial scans, and other crucial information about their bodies").

312 *Id.*

313 *Id.*; *see supra* notes 93–102 and accompanying text.

314 *Compare supra* Part VI, *with* BIPA, 740 ILL. COMP. STAT. 14/15 (2008).

315 *Compare* BIPA, 740 ILL. COMP. STAT. 14/15(c) (2008) (BIPA does not allow companies to "sell, lease, trade, or otherwise profit" from biometric identifiers or information), *with supra* Section VI.B.ix (allowing employers to use employees' biometric information for additional purposes if employees agree and are given additional consideration).

a fingerprint; (3) a voiceprint; (4) a scan of hand geometry; or (5) a scan of face geometry.[316] Other features of the human body (e.g., height, weight, hair color, eye color, tattoos) do not meet BIPA's definition of biometric identifier.[317] BIPA defines "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."[318] BIPA additionally defines "confidential and sensitive information" as "personal information that can be used to uniquely identify an individual or an individual's account or property."[319]

No conflicts exist between the definitions used in this Article's recommendations and the definitions used within BIPA.[320] Indeed, these recommendations address one of the BIPA biometric identifiers—scan of face geometry[321]—as their primary focus.[322]

ii. Requirement to Inform the Person How Data Will Be Collected, What Data Will Be Collected, the Purpose of the Collection, and Obtaining Written Consent

BIPA prohibits the collection or receipt of biometric identifier or biometric information unless the entity first: (1) informs the subject of the biometrics in writing that biometric collection will take place; (2) informs the subject in writing of the specific purpose of the collection and length or term the identifier is stored and used; and (3) obtains a written release from the subject to collect, store, and use the biometrics.[323] These steps must be taken prior to collections taking place.[324]

This Article's recommendations call for employers to obtain a license from the employee-subject of the biometric collection, storage, and use once employment begins.[325] The terms of the recommended licensure agreement would include written notice, in clear and simple language, of which biometric information will be collected, how it will be used, and when the license will

316 BIPA, 740 ILL. COMP. STAT. 14/10 (2008).
317 *Id.*
318 *Id.*
319 *Id.*
320 *Compare id.*, *with supra* Section VI.B.i.
321 BIPA, 740 ILL. COMP. STAT. 14/10 (2008).
322 *See supra* text accompanying notes 281–84 (identifying facial scans as biometric identifiers of concern in the employment context).
323 BIPA, 740 ILL. COMP. STAT. 14/15 (2008).
324 *Id.*
325 *See supra* text accompanying notes 277–80.

terminate.[326] Once signed by the employee, the employer then has documented consent of the license.[327] There may be some argument for the temporary collection of the employee's facial geometry upon entering the employer's premises prior to effectuating this license, but that collection would be de minimis under the rationale for any visitor's biometrics may be temporarily collected with adequate notice via signage. By requiring the process surrounding this license upon hire, the employer provides the employee with written notice.

iii. Requirement to Inform the Person of the Specific Purpose and Length of Storage of Biometrics Collected and Used

When notifying the subject that the biometric collection will take place, BIPA requires that the subject receive information as to the purpose and length for which the biometric identifiers will be collected, stored, and used.[328] That information must be provided in writing.[329]

The recommendations in this Article advise that this obligation be met simultaneously with informing the employee upon hire about the data to be collected and obtaining the license.[330] The recommended written information provided to the employee includes the purpose of storage and collection (e.g., identification and authentication of identity for valid employees) and length of storage (e.g., until termination of employment).[331] This information, like the information provided to inform the employee about the collection generally, should be provided to the employee via license prior to collecting an employee's biometric identifier.[332]

iv. Requirement to Obtain the Person's Written Consent

As per BIPA, the collection and use of biometric identifiers may not begin until after the subject has provided a written release—their consent—to permit the specified collection and use of the person's biometric identifier.[333] That written release must be executed by the subject of the biometrics or their legally

---

[326] *See supra* text Section VI.B.
[327] *See* text accompanying notes 277–80.
[328] BIPA, 740 ILL. COMP. STAT. 14/15(b) (2008).
[329] *Id.*
[330] *See supra* Section VI.B.
[331] *See supra* Section VI.B.
[332] *See supra* Section VI.B.
[333] BIPA, 740 ILL. COMP. STAT. 14/15(b) (2008).

authorized representative.[334]

This Article's recommendations require a signed licensure agreement prior to the collection of an employee's biometric identifiers and requires the disclosure of the collection, retention, and use of their biometric identifiers for a particular purpose and length.[335] Moreover, the license must detail what the employee is consenting to by explicitly identifying and granting the permissible uses for those biometric identifiers while also identifying impermissible uses.[336] The license should narrowly establish the parameters of the consent and state that anything outside of those parameters does not receive consent.[337]

v. Ban on Profit Provision Prohibiting Any Private Entity from Profiting from Biometric Data

BIPA prohibits a "private entity in possession of biometric identifiers to sell, lease, trade, or otherwise profit from a person's or a customer's biometric identifier or biometric information."[338] To "otherwise profit" is an expansive term which may include commercial transactions which may make use of the biometrics, even without any "actual injury or adverse effect, beyond violation of his or her rights."[339] Indeed, Illinois' highest state court held in 2019 that a person is "aggrieved" under BIPA when an entity fails to comply with one of BIPA's requirements, even absent a separate actual injury, as that violation constitutes "an invasion, impairment, or denial" of that person's statutory rights.[340]

The recommendations set forth in this Article conflict with BIPA's ban on profits, as obtaining consent through the statutory scheme recommended by this Article, permits employer's to profit from employee biometrics and would leave the employee aggrieved only if the employer were to violate the terms of the license.[341] Thus, a business could profit from an employee's biometrics as long as the employer does so within the license's parameters.[342] When the employee licenses their likeness via their biometrics and the

---

[334] *Id.*

[335] *See supra* text accompanying notes 277–80.

[336] *See supra* Sections VI.B.

[337] *See supra* text accompanying notes 272–74.

[338] BIPA, 740 ILL. COMP. STAT. 14/15(c) (2008).

[339] Rosenbach v. Six Flags Ent. Corp., 129 N.E.3d 1197, 1207 (Ill. 2019); *see* BIPA, 740 ILL. COMP. STAT. 14/15(c)–(d) (2008).

[340] *Rosenbach*, 129 N.E.3d at 1205–06.

[341] *See id; see supra* Sections VI.B.ix; *see infra* text accompanying notes 274–85.

[342] *See supra* Sections VI.B.ix; *see infra* text accompanying notes 274–85.

employer abides by that license, the employee would have no claim.[343]

However, the issue remains that BIPA explicitly prohibits the profit from the employee's biometrics.[344] The conflict is only relevant, though, where BIPA applies—where an Illinois resident's biometrics are involved.[345] Residents of other states may not be protected by similar laws,[346] and, therefore, would not be subject to this potential conflict. Where that conflict remains, a waiver to BIPA's requirements may be necessary for the ban on profit. Use of a waiver may be permissible so long as an adequate measure—the license—is used in lieu of BIPA's profit prohibition.

vi. Ban on Disclosure of Biometric Data Without Consent

BIPA mandates that disclosure of biometric identifiers occurs only with consent from the subject of the biometrics unless that disclosure is (1) required to complete a financial transaction authorized by the subject; (2) required by law; or (3) required pursuant to a valid warrant or subpoena.[347] Under this Article's recommendations, biometric identification disclosures should identify the specific purpose(s) for which the employee's biometric data may be used.[348] Notably, in the employer-employee relationship context, a valid argument may exist that the rendering of services in return for a paycheck, may "complete[] a financial transaction" pursuant to BIPA requirements.[349] If so, then any disclosure that occurs to complete that transaction could be done without specific disclosure consent.[350]

---

[343] *See infra* Section VIII.A.

[344] BIPA, 740 ILL. COMP. STAT. 14/15 (2008).

[345] *See* Syed S. Ahmad et al., *Nine-figure Verdicts: What Is BIPA and Why You Should Care*, REUTERS (Apr. 24, 2023), https://www.reuters.com/legal/legalindustry/six-figure-verdicts-what-is-bipa-why-you-should-care-2023-04-24/ ("Illinois is the only state that currently permits a private right of action for BIPA violations, but plaintiffs are filing suits in other jurisdictions and seeking to apply Illinois law. Thus far, courts have denied these efforts.").

[346] Carra Pope, Note and Comment, *Biometric Data Collection in an Unprotected World: Exploring the Need for Federal Legislation Protecting Biometric Data*, 26 J.L. & POL'Y 769, 789–95 (2018) (discussing the absence of state-level biometric privacy laws).

[347] BIPA, 740 ILL. COMP. STAT. 14/15(d) (2008).

[348] *See supra* Section VI.B.ii.

[349] *See supra* Section V.B; *see also* BIPA, 740 ILL. COMP. STAT. 14/15(d) (2008) (containing the financial transaction exception to disclosure terms).

[350] *See* BIPA, 740 ILL. COMP. STAT. 14/15(d).

vii. Storage Requirements for Confidential and Sensitive Information

BIPA requires entities to store biometric identifiers with a reasonable standard of care and in a manner consistent with the entity's protections for its own confidential and sensitive information.[351] Thus, the employer must treat the employee's biometric identifiers as if they were the company's own protected information.[352] The recommendations set forth in this Article further ensure that companies store biometric identifiers appropriately by attaching pecuniary consequences for retaining the biometric identifiers beyond their authorized timeframe and by enhancing consequences should an employee's biometric data be subject to a breach.[353] The recommendations, then, make it so that the employer is best served by protecting the biometrics to the same level as its own confidential and sensitive information and to ensure a timely disposal.

B. California Consumer Privacy Act (CCPA) & California Privacy Rights Act (CPRA)

The California Privacy Rights Act (CPRA) expands the rights granted under the California Consumer Privacy Act (CCPA) by updating obligations of businesses and affording better opt-out provisions for consumers in California.[354] The CPRA took effect in 2023 and provided additional protections for consumers' privacy.[355] While BIPA addresses the specific topics of biometric information,[356] the CCPA, as amended by the CPRA, is broad and

---

[351] BIPA, 740 ILL. COMP. STAT. 14/15(e) (2008).

[352] BIPA, 740 ILL. COMP. STAT. 14/15(e)(2) ("[A private entity shall] . . . protect from disclosure all biometric identifiers and biometric information in a manner that is the same as or more protective than the manner in which the private entity stores, transmits, and protects other confidential and sensitive information").

[353] *See* discussion *infra* Section VIII.B.

[354] CCPA, CAL. CIV. CODE § 1798.100–1798.199.100 (2024); CA Prop 24, 2020 Cal. Legis. Serv., Prop. 24 (PROPOSITION 24) (the California Privacy Rights Act, presented as Proposition 24, was approved by California voters on the 2020 election ballot); *see California Consumer Privacy Act*, CAL. DEP'T OF JUST.: OFF. OF THE ATT'Y GEN., https://oag.ca.gov/privacy/ccpa (March 13, 2024).

[355] *California Consumer Privacy Act, supra* note 354. The CPRA amended, but did not replace, the CCPA. The CCPA, as amended, is referred to as the "CCPA" or the "CCPA, as amended," by government entities. This Article adopts the California Attorney General's naming convention and refers to the CCPA, as amended by the CPRA, as the CCPA.

[356] BIPA, 740 ILL. COMP. STATE. 14/5 (identifying the purpose of the Act as

applies privacy laws in a more general manner.[357] The CCPA universally focuses on any data which may be deemed sensitive personal information, which would include biometric identifiers.[358]

i. Personal Information and Sensitive Personal Information Defined

The CCPA separates information into two tiers: personal information and sensitive personal information.[359] Under the CCPA, as amended by the CPRA, biometric information is defined as "an individual's physiological, biological or behavioral characteristics . . . that is used or is intended to be used singly or in combination with each other or with other identifying data, to establish individual identity."[360] Personal information is "information that identifies, relates to . . . or could reasonably be linked . . . with a particular consumer or household."[361] This may include certain records, characteristics, and one's biometrics generally.[362] Sensitive personal information, on the other hand, is a specific subset of personal information designated as requiring additional protections, including genetic data, biometric information when used to identify a person, and precise

protection for citizens' biometric information and explaining the legislative purpose).

[357] *See* Luis Miguel M. del Rosario, Note, *On the Propertization of Data and the Harmonization Initiative*, 90 FORDHAM L. REV. 1699, 1720 (2022) ("CCPA creates property interests in a wider swath of data than BIPA by covering all '[p]ersonal [i]nformation,' which is defined as 'information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.'") (citing CAL. CIV. CODE § 1798.140(o)(1) (West 2021)).

[358] *See California Amends CCPA to Cover Neural Data and Clarify Scope of Personal Information*, HUNTON: BLOG (Oct. 2, 2024), https://www.hunton.com/privacy-and-information-security-law/california-amends-ccpa-to-cover-neural-data-and-clarify-scope-of-personal-information ("Other types of sensitive information under the CCPA include genetic, biometric and health data."); CCPA, CAL. CIV. CODE § 1798.121 (West 2024) (outlining the expanded protections afforded to consumers by the approval of Proposition 24, colloquially known as the CPRA, related to their sensitive personal information shared with businesses).

[359] CIV. § 1798.140(v) (defining personal information for purposes of the statute); CIV. § 1798.140(ae) (defining sensitive personal information for purposes of the statute).

[360] CCPA, CAL. CIV. CODE § 1798.140(c) (West 2024).

[361] CIV. § 1798.140(v).

[362] CIV. § 1798.140(v) (outlining the different types of information that qualify as personal information which includes specific types of records, characteristics, and biometric information which includes fingerprints).

geolocation.[363] Neither personal information nor sensitive personal information include publicly available information.[364]

No conflicts exist between this Article's recommendations and the definitions used within CPPA.[365] Much like the CCPA's definition of biometric information establishing as worthy of protection an individual's physiological, biological or behavioral characteristics when used to identify an individual,[366] these recommendations demand protection for biometric information when they capture an individual's physiological, biological, or behavioral characteristics that can be used, singly or in combination with each other or with other identifying data, to establish individual identity. [367]

ii. Right to Know Categories and Specific Pieces of Personal Information

Upon request by the subject of biometrics, the CPPA requires a business that collects personal information, including biometrics, to disclose each of the following:

> (1) The categories of personal information it has collected about that consumer.
> (2) The categories of sources from which the personal information is collected.
> (3) The business or commercial purpose for collecting, selling, or sharing personal information.
> (4) The categories of third parties to whom the business discloses personal information.
> (5) The specific pieces of personal information it has collected about that consumer.[368]

An employee under this Article's proposed licensing scheme would automatically receive the same information that the CPPA permits by request only.[369] These same five parameters are the

---

[363] CIV. § 1798.140(ae).
[364] CIV. § 1798.140(v)(2), (ae)(3).
[365] *Compare supra* Section VI.B.i., *with supra* notes 359–67 and accompanying text.
[366] *See supra* note 360 and accompanying text.
[367] *See supra* notes 281–85 and accompanying text.
[368] CIV. § 1798.110(a).
[369] *See* discussion *supra* Section VI.B (discussing the disclosure requirements that would be required under the proposed licensing framework in the context of the nine proposed elements).

terms that would be established by the license upon hire under this Article's proposed statutory scheme.[370] The key difference is that the license proposed in this Article grants certain uses while also identifying that information,[371] while these requests under the CPPA act as a recurring check on those uses while providing a method to remedy any unacceptable uses.[372]

iii. Right to Limit the Use and Disclosure of Sensitive Personal Information

In California, a person may direct businesses to only use their sensitive personal information for limited purposes.[373] These directions are in line with how a license proposed within the recommended scheme would operate, as the license would direct the employer on how to use an employee's sensitive personal information, in the form of their facial geometry, and identify the limited purposes for which the employer may use those biometrics.[374] The license limits the use to the specified, agreed upon parameters.[375]

iv. Right to Opt-out of Automated Decisionmaking Technology

On November 8, 2024, the California Privacy Protection Agency Board voted to commence formal rulemaking on Automated Decisionmaking Technology (ADMT).[376] The proposed regulation would grant a person the right to opt-out of a business's use of

---

[370] *Compare supra* note 369 and accompanying text, *with* discussion *supra* Section VI.B (outlining the nine elements of disclosure that would be required in a license agreed to upon hire, which closely mirror the five parameters of the CCPA disclosures required upon request enumerated in text accompanying note 369).

[371] *See supra* Section VI.B.

[372] *See California Consumer Privacy Act (CCPA)*, *supra* note 354 ("If you are a California resident, you may ask businesses to disclose what personal information they have about you and what they do with that information, to delete your personal information, to direct businesses not to sell or share your personal information, to correct inaccurate information that they have about you, and to limit businesses' use and disclosure of your sensitive personal information.").

[373] CCPA, CAL. CIV. CODE § 1798.121 (West 2024).

[374] *See supra* Part VI.

[375] *See supra* Part VI.

[376] *Proposed Regulations on CCPA Updates, Cybersecurity Audits, Risk Assessments, Automated Decisionmaking Technology (ADMT), and Insurance Companies*, CAL. PRIV. PROT. AGENCY (last visited Feb. 2, 2025), https://cppa.ca.gov/regulations/ccpa_updates.html.

automated decision-making technology (ADMT).[377] The Agency has not yet provided a definition for what ADMT would include.[378] One proposed definition defined ADMT as "any system, software, or process — including one derived from machine-learning, statistics, other data-processing or artificial intelligence — that processes personal information and uses computation as whole or part of a system to make or execute a decision or facilitate human decision making. ADMT includes profiling."[379]

Facial recognition software would be covered under the proposed definition of ADMT, meaning an employee would have a right to opt out of its use.[380] This California provision may conflict with any licenses granted pursuant to this Article's recommendations by providing the employee an avenue through which to alter the terms of the license after it has been agreed upon.[381] Should a conflict emerge, waivers may be required for licenses, like those recommended in this Article, to remain intact.[382] Otherwise, terminations or modifications of the license recommendation in states like California must be considered.

v. Right to Request Deletion

While exemptions exist,[383] a person has the right to have their personal information deleted by a business under the CCPA.[384] One statutory exemption from the right to delete provides that

---

[377] *Id.* The public comment period on the proposed regulation closed on February 19, 2025.

[378] Cobun Zweifel-Keegan, *CPPA's Draft Automated Decision-Making Rules Unpacked*, IAPP (Nov. 27, 2023), https://iapp.org/news/a/cppas-draft-automated-decision-making-rules-unpacked.

[379] *Id.*

[380] *Fact Sheet: Draft Automated Decisionmaking Technology (ADMT) Regulations*, CAL. PRIV. PROT. AGENCY 1, https://cppa.ca.gov/meetings/materials/adt_regulations.pdf (last visited Feb. 2, 2025) ("Examples of ADMT include . . . [f]acial-recognition technology. . . .").

[381] If the ADMT provision is passed, California residents could potentially invoke the new protections to opt out of biometric identifier collection via facial recognition technology even if the invocation would be averse to a licensure agreement giving the employer permission to use ADMT in the form of facial recognition software.

[382] *See* Jeff D. McAlpin, *Programming Digital Privacy into Public Policy: A New Rule of Law Through Legislative Action*, 70 LA BAR J. 430, 432 (2023) (suggesting that a waiver could be granted by a federal privacy protection law to harmonize the provisions of the federal privacy law with the CCPA).

[383] CCPA, CAL. CIV. CODE §1798.145 (West 2024).

[384] CIV. §1798.105.

> [p]ersonal information that is collected by a business about a natural person in the course of the natural person acting as . . . an employee of . . . that business to the extent that the natural person's personal information is collected and used by the business solely within the context of the natural person's role or former role . . . [at] that business.[385]

Another exemption states:

> The obligations imposed on businesses . . . shall not apply to personal information reflecting a written or verbal communication or a transaction between the business and the consumer, where the consumer is a natural person who acted or is acting as an employee . . . and whose communications or transaction with the business occur solely within the context of the business conducting due diligence regarding, or providing or receiving a product or service . . . .[386]

Opinions may differ as to whether the licensed use of an employee's biometrics would fit solely within the context of that employee's role with the employer. The argument that the biometrics fit solely within the employee's role with the employer would have merit should the use of biometric information be limited to the identification and authentication of a person (i.e., to ensure the person using certain assets are authorized within their role to use those assets).[387] Such a situation would prevent the complete deletion of the employee's biometric information upon termination of employment.[388] However, CCPA § 1798.145(m) and (n), discussed above, became inoperative on January 1, 2023.[389]

---

385 CIV. §1798.145(m)(1)(a).

386 CIV. § 1798.145(n)(1).

387 *See* Lydia F. de la Torre & Laure Kitces, *Compliance with the California Consumer Privacy Act in the Workplace: What Employers Need to Know*, 29 ANTITRUST & UNFAIR COMP. L.J. 96, 111 (2019) ("The obligation to comply with a deletion request is subject to various exceptions, including the right of the employer to keep data if necessary to meet a legal obligation or for the employer's internal use if otherwise lawful and compatible with the context in which the information was provided by the worker. The majority of employee or applicant data will likely fall under one of these two exceptions."); *see also supra* Sections VI.B.ii, ix.

388 *See* Torre & Kitces, *supra* note 387, at 107–08 (explaining that proper practice under the CCPA is for employers to evaluate their records retention policies, determine how long they may legally store employees' personal information, and that employers should delete personal information as soon as it is no longer needed generally).

389 CCPA, CAL. CIV. CODE § 1798.145(m)(4), (n)(3) (West 2024).

With these provisions inoperative, the employee maintains the option to incorporate specific deletion criteria within the license with their employer.

C. European Union General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) is the pivotal regulation intended to protect the privacy rights of persons within the European Union (EU).[390] The GDPR has had a global effect due to the nature of how information is shared.[391] The GDPR established seven principles to which organizations doing business with the EU must adhere should they seek to receive data about EU consumers.[392] Countries outside the EU may be permitted to do business with EU countries only if they are able to meet the EU's adequacy requirements for data protection and are approved by the European Commission.[393] The United States has had some difficulty in meeting these adequacy requirements,[394] with ongoing concern for the validity of the European Commission's most recent decision to grant the United States adequacy with GDPR requirements.[395] Any new enactment or understanding of privacy laws within the United States should keep in mind the GDPR's data protection requirements and the need to maintain compliance

---

[390] GDPR, *supra* note 8, art. 1; *see also* Rebecca Harris, Note, *Forging a Path Towards Meaningful Digital Privacy: Data Monetization and the CCPA*, 54 LOY. L.A. L. REV. 197, 214 (2020) (describing the GDPR as a "comprehensive privacy law" that affords European citizens the right to demand companies to delete their data).

[391] *See* Harris, *supra* note 390, at 214 ("[T]he GDPR's scope is not limited to European businesses and applies to any "controller or processor" of personal data that offers goods or services to data subjects in the European Union, regardless of where the processing takes place.").

[392] GDPR, *supra* note 8, art. 5, at 1 (Identifying seven "[p]rinciples relating to personal data," summarized as: (1) lawfulness, fairness, and transparency; (2) purpose limitation; (3) data minimisation; (4) accuracy; (5) storage limitation; (6) integrity and confidentiality; and (7) accountability).

[393] *See* GDPR, *supra* note 8, art. 45, at 1; *Adequacy Decisions: How the EU Determines if a Non-EU Country has an Adequate Level of Data Protection,* EUR. COMM'N, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (last visited Feb. 15, 2025).

[394] Case C-311/18, Data Prot. Comm'r v. Facebook Ir. Ltd., ECLI:EU:C:2020:559, ¶ ¶ 160, 198–201 (July 16, 2020) (invalidating a previous decision that established that the US offered adequate data protection).

[395] Mikolaj Barczentewicz, *Schrems III: Gauging the Validity of the GDPR Adequacy Decision for the United States*, INT'L CTR. FOR L. & ECONS., 1–3 (Sept. 25, 2023), https://laweconcenter.org/wp-content/uploads/2023/09/ICLE-Schrems-III_2023.09.21.pdf.

with those requirements.

i. Lawfulness, Fairness, and Transparency

The GDPR presents its personal data principles relative to the data subject—the person to which the data associates or describes.[396] The first principle states: "Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject."[397] Lawfully processing personal data requires compliance with all applicable laws that control that personal data and generally must not do anything unlawful with that personal data.[398] Processing the data fairly and in a transparent manner requires that the data subject be able to understand what will be done with that data and requires that the data processor be able to explain and justify any adverse or unexpected impacts without deceiving or misleading the data subject.[399]

The recommendation in this Article for employers to provide employees with a notice of biometric identifier collection accompanied by a consent form parallel this principle.[400] Under these recommendations, the form provides the employee with the purpose for the use of biometrics and presents that purpose in clear and simple language rendering the purpose understandable.[401] Permitting the employee an opportunity to ask questions or to seek counsel prior to providing consent further demonstrates adherence with this principle, as it promotes fairness and transparency, in addition to compliance with the

---

396 GDPR, *supra* note 8, art. 5, at 1.

397 GDPR, *supra* note 8, art. 5, at 1.

398 *See Principle (a): Lawfulness, Fairness and Transparency*, INFO. COMM'R'S OFF., https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/lawfulness-fairness-and-transparency/ (Jan. 10, 2025); *see also* Joshua M. Wilson, Comment, *Cross-Border Data Transfers: A Balancing Act Through Federal Law*, 6 BUS., ENTREPREN. & TAX L. REV. 150, 160–61 (2022) (discussing the EU providing an international framework for data privacy and how lawfully processing personal data requires compliance with all applicable laws that control that personal data).

399 *See Principle (a): Lawfulness, Fairness and Transparency*, *supra* note 398; *see also* Elena Gil González & Paul de Hert, *Understanding the Legal Provisions that Allow Processing and Profiling of Personal Data—An Analysis of GDPR Provisions and Principles*, 19 ERA F. 597, 605–06 (2019) (discussing reasonable expectations of the data subject and transparent data collection and processing); GDPR, *supra* note 8, art. 5, at 1.

400 *See* discussion *supra* Section VI.

401 *See* discussion *supra* Section VI.

law.[402]

ii. Purpose Limitation

The GDPR's second principle limits the purposes for which personal data may be processed.[403] The principle dictates that "[p]ersonal data shall be . . . collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes."[404] Accordingly, the purpose for which the data is used must be identified.[405] The processing is limited to that identified purpose, and any new purpose that is not compatible with that originally identified purpose is prohibited without consent for that new purpose.[406]

Under this Article's guidelines, the recommended license granted to the employer sets the purpose limitation of the biometric identifiers and thus comports with the GDPR's second principle.[407] The license provides the employer with explicit information about whether the biometric identifiers may be used for identification, security, authentication, or for some other specified purpose.[408]

iii. Data Minimization

The third GDPR principle focuses on collecting personal data only if it is needed for the identified purpose.[409] "Personal data shall be . . . relevant and limited to what is necessary in relation to the purposes for which [the data is] processed."[410] The collection of personal data should not exceed what is necessary to accomplish those purposes; personal data should not be collected "on the off-chance that it might be useful in the future."[411] Indeed, the

---

[402] *See* discussion *supra* Section VI.

[403] GDPR, *supra* note 8, art. 5, at 1.

[404] *Id.*

[405] *Id.*; *see Principle (b): Purpose Limitation*, INFO. COMM'R'S OFF., https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/purpose-limitation/ (last visited Nov. 23, 2024); Isabel Hahn, *Purpose Limitation in the Time of Data Power: Is There a Way Forward?*, 7 EUR. DATA PROT. L REV. 31, 37–39 (2021).

[406] GDPR, *supra* note 8, art. 5, at 1; *Principle (b): Purpose Limitation*, *supra* note 405; Hahn, *supra* note 405, at 37–38.

[407] *See* discussion *supra* Section VI.B.

[408] *See* discussion *supra* Part VI.

[409] GDPR, *supra* note 8, art. 5, at 1.

[410] *Id.*

[411] *Principle (c): Data Minimisation*, INFO. COMMR'S OFF., https://ico.org.uk/for-

collected personal data should also be deleted once the identified purpose for which it was collected has ceased and no necessity remains.[412]

Similarly, the recommendations in this Article instruct that an employer licensure should explain what will be collected from the employee to prevent any ambiguity.[413] By requiring that the license limit the collection so that only the specified biometric identifiers required for carrying out the permitted purposes may be collected, this Article's recommendations align with the GDPR's data minimization principle.[414]

iv. Accuracy

The fourth principle under the GDPR addresses accuracy, which is inherently embedded in the processes behind biometric collection and use.[415] "Personal data shall be . . . accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay."[416] The personal data must be kept updated and mistakes must be clearly corrected when the data subject raises their right to rectify their personal data.[417]

The reliability on biometrics necessitates the methods and processes to collect and compare biometric identifiers to be accurate.[418] NIST has addressed the accuracy of those methods

---

organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/data-minimisation/ (last visited Nov. 23, 2024); *see id.*

412 *Principle (e): Storage Limitation*, INFO. COMMR'S OFF., https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/storage-limitation/ (last visited Nov. 23, 2024).

413 *See* discussion *supra* Section VI.B.

414 *See* discussion *supra* Section VI.B.

415 GDPR, *supra* note 8, art. 5, at 1.

416 *Id*.

417 *See Principle (d): Accuracy*, INFO. COMM'R'S OFF., https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/accuracy/ (last visited Nov. 23, 2024); GDPR, *supra* note 8, art. 16; *see also* Dara Hallinan & Frederik Zuiderveen Borgesius, *Opinions Can be Incorrect (in Our Opinion)! On Data Protection Law's Accuracy Principle*, 10 INT'L DATA PRIV. L. 1, 1–4 (2020) (discussing the duties on data controllers to update incorrect data).

418 *See supra* notes 174–80 and accompanying text (discussing the consequences of inaccurate biometric identification); *see also* Brian Bennett, *The Impact of Biometrics in Cybersecurity*, DAVENPORT GRP. (Aug. 15, 2024), https://davenportgroup.com/insights/the-impact-of-biometrics-in-cybersecurity/

and processes, and has provided recommendations on how to mitigate the declining errors in biometric identifiers that may lead to misidentification.[419]

The recommended license scheme in this Article does not address the specific accuracy requirements within the GDPR data processing principles, but employers may still adhere to accuracy principles and implement accuracy protocols nonetheless.[420] Establishing processes which record the percent match, the method of matching, and similar metrics—which employers will likely do to ensure the biometrics they are collecting are accurate enough for their specified purposes—would make any processes the employer incorporates to collect and use biometrics in line with this principle.[421] Should any of those metrics fall below a pre-determined threshold, a re-collection may be required to maintain the integrity of this principle in the recommended license scheme.

v. Storage Limitations

The fifth principle fortifies purpose limitations with storage limitations.[422] "Personal data shall be . . . kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed." [423] This principle further addresses the retention and deletion of personal data, requiring that the biometrics collected pursuant to the data minimization principle be kept for no longer than actually needed.[424] Careful consideration is required under this principle for how personal data is stored, where personal data is stored, and for how long personal data is stored.[425]

("One of the most compelling advantages of biometric security is its high level of accuracy and reliability.").

[419] *See Face Recognition Technology Evaluation*, *supra* note 174; GROTHER ET AL., NAT'L INST. OF STANDARDS & TECH., REPORT NO. 8280, FACE RECOGNITION VENDOR TEST (FRVT) PART 3: DEMOGRAPHIC EFFECTS 70–72, (2019).

[420] *See supra* notes 174–180 and accompanying text (discussing the potential consequences inaccurate biometric identification technology could have on employers and applicants).

[421] *See supra* notes 126–27; 174–80 and accompanying text.

[422] GDPR, *supra* note 8, art. 5, at 1.

[423] *Id.*

[424] *Id.*; *see Principle (e): Storage Limitation*, *supra* note 412; *see also Principle (c): Data Minimisation*, *supra* note 411; *see also* Alexander Tsesis, *The Right to Erasure: Privacy, Data Brokers, and the Indefinite Retention of Data*, 49 WAKE FOREST L. REV. 433, 463–66 (2014).

[425] *See Principle (e): Storage Limitation*, *supra* note 537; GDPR, *supra* note 8, art. 5, at 1; *see also* Tsesis, *supra* note 424, at 463–66.

Like with the purpose limitation and data minimization principles, the license addresses storage limitations primarily through the termination provisions.[426] The recommendations described in this Article honor the storage limitation principle by requiring that an employer delete an employee's biometric information when employment terminates, or shortly thereafter.[427] Although the recommended license focuses more on when the biometric identifiers are collected and stored, the recommendations provide that both the employer and employee be aware of how the collected information will be stored.[428]

vi. Integrity and Confidentiality (Security)

The sixth GDPR principle focuses on the information security of the personal data, aimed at safeguarding the information entrusted by the data subject.[429] "Personal data shall be . . . processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."[430] This principle requires that an entity receiving personal data employs appropriate security measures to protect the personal data.[431] For most organizations, this means having a data protection policy and a data protection program focused on safeguarding sensitive information, including personal information.[432] When creating a data protection policy, organizations should consider factors like "risk analysis, organizational policies, and physical and technical measures."[433]

---

[426] *See* discussion *supra* Section VI.B.; *see also Principle (b): Purpose Limitation*, *supra* note 405; *Principle (c): Data Minimisation*, *supra* note 411; *Principle (e): Storage Limitation*, *supra* note 412.

[427] *See* discussion *supra* Section VI.B.v.

[428] *See* discussion *supra* Section VI.B.

[429] GDPR, *supra* note 8, art. 5, at 2.

[430] *Id.*

[431] *Id.*; *see Principle (f): Integrity and Confidentiality (Security)*, INFO. COMM'R'S OFF., https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/integrity-and-confidentiality-security/ (last visited Nov. 26, 2024); *see also A Guide to Data Security*, INFO. COMM'R'S OFF., https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/security/ (last visited Nov. 26, 2024).

[432] *See A Guide to Data Security*, *supra* note 431; *see also* Lina Jasmontaite et al., *Data Protection by Design and by Default: Framing Guiding Principles into Legal Obligations in the GDPR*, 4 EURO. DATA PROT. L REV. 168, 169, 172, 175–76 (2018).

[433] *A Guide to Data Security*, *supra* note 431.

This principle is accomplished indirectly in this Article's recommendations via the proposed damage parameters.[434] By allowing for additional damages when an employer experiences a data breach, the employer must thoughtfully consider and address how they protect an employee's biometric information to prevent liability for serious damages pursuant to potential breaches.[435] Per this Article's recommendations, experiencing a breach provides the employee the ability to recover up to twice their damages, but to reach that maximum amount would depend on whether the employer was safeguarding the employee's biometric identifiers.[436] The extent to which the employer adequately safeguarded the employee's biometric identifiers determines whether the circumstances warrant minimum or maximum damages.[437]

vii. Accountability

The seventh, and final, GDPR principle drives accountability to bring effect to the other six principles. "The controller shall be responsible for, and be able to demonstrate compliance with, [the previously listed principles]."[438] This principle requires that those entrusted with personal data take responsibility with how they treat that personal data and comply with the other principles through accountability and governance processes.[439] The information holder must have "appropriate measures and records in place" to be able to demonstrate compliance.[440]

This principle is met through the license and the proposed damages of these recommendations. The license provides documentation of what the employer will do to comply with the other principles while providing the employee an opportunity to review and assess that compliance to a reasonable degree.[441] The

---

[434] *See infra* Section VIII.B.

[435] *See* discussion *infra* Section VIII.B.

[436] *See* discussion *supra* Section VIII.B.

[437] *See* discussion *supra* Section VIII.B.

[438] GDPR, *supra* note 8, art. 5, at 1.

[439] *See id.*; *Accountability Principle*, INFO. COMM'R'S OFF., https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/accountability-principle/ (last visited Nov. 26, 2024); *Guide to Accountability and Governance*, INFO. COMM'R'S OFF., https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/guide-to-accountability-and-governance/ (last visited Nov. 26, 2024); *see also* González & de Hert, *supra* note 399.

[440] *Accountability Principle*, *supra* note 439.

[441] *See* discussion *supra* Section VI.B.

proposed damages are one mechanism for the employer to take responsibility for failure to comply with these principles while also encouraging employers to adopt, enhance, or invigorate their policies and programs which intersect with biometric information.[442] The license thus makes the employer accountable to the employee, notwithstanding other applicable laws that may govern the employer's biometric collection efforts.

VIII. THEORY FOR CALCULATING DAMAGES

A law without adequate enforcement is ultimately ineffective.[443] Enforcement, and the consequences that stem from that enforcement, require that there be adequate means for a person to protect their privacy rights.[444] What constitutes adequate enforcement depends on who and what society aims to deter and what society seeks to preserve.[445] At a minimum, protecting each person's identity from unfettered exploitation by their employer requires that the consequences sufficiently deter the employer from using their employee's identities without proper licensure.

The consequences cannot be so great, however, that they would chill innovation to the point that employers would be unwilling to pursue new and creative uses of society's resources.[446] To set the

---

[442] *See* discussion *infra* Part VIII.

[443] *See* Jon S. Vernick et al., *Regulation of Firearm Dealers in the United States: An Analysis of State Law and Opportunities for Improvement,* 34 J.L. MED. & ETHICS 765, 769 (2006) ("Simply having a law on the books, without adequate enforcement, is ineffective.").

[444] *See* Jason Heitz, Note, *Federal Legislation Does Not Sufficiently Protect American Data Privacy*, 49 N. KY. L. REV. 287, 291 (2022) (stating that the current statutes that the Federal Trade Commission uses to enforce data privacy on the Internet leaves private individuals with using statutes that are too narrow for individual use).

[445] *See e.g.*, Mary Fan, *Rebellious State Crimmigation Enforcement and the Foreign Affairs Power*, 89 WASH. U. L. REV. 1269, 1275–76 (2012) (explaining that, when applying and enforcing the law, authorities exercise judgment in deciding which cases are worth the fiscal and community costs of enforcement); Peninsula Counseling Ctr. v. Rahm, 719 P.2d 926, 936 (Wash. 1986) (Pearson, J., dissenting) ("As the ultimate arbiters of our state's constitution, we have the duty to protect the privacy rights of our state's citizens."); McGrath v. Nassau Health Care Corp., 209 F.R.D. 55, 59–60 (E.D.N.Y. 2002) (in reviewing a motion for production of a DNA sample to corroborate a sexual encounter between two employees in a sexual harassment lawsuit, the court weighed an individual's privacy rights and the State's interest in providing a reasonable means or forum for its citizens to resolve disputes, regulating litigation in the courts, and in protecting its citizens from discrimination in the workplace).

[446] *See* Jonathon W. Penney, *Understanding Chilling Effects*, 106 MINN. L. REV. 1451, 1454–55 (2022) ("The conventional understanding in law is that a chilling

consequences to the point that any one infraction could completely undo a business is too steep to be tenable; a balance must be struck. That balance must consider both the employer and the employee, and the law must be designed to assure employees that their rights are protected without being so harsh that employers will not be willing to participate in commercial activity if they must adhere to the law's provisions.[447]

With the acknowledgment that every person has a right to publicity, so, too, must come the acknowledgment that any individual person's likeness may not have the same value as another individual's likeness, and the value of a typical person's likeness is not equal to that of a public figure.[448] In this way, the damages awarded based on violations of employee biometric privacy laws would need to deviate slightly from decisions in cases where celebrities and public figures seek damages for the misappropriation of their likeness.[449] A common approach for non-public figures, employees in this case, would provide a practicable solution without placing an excessive administrative burden on the courts.

Borrowing from intellectual property law, a standard calculation could be created to form the basis for damages when misappropriating an average person's likeness via biometrics.[450] For the misappropriation of one's likeness via biometrics, damages may be comparably calculated through statutory damages, which set ranges for each infringement.[451] Under this proposal,

---

effect is when a person, deterred by fear of some legal punishment or privacy harm, engages in self-censorship.").

[447] *See* Emma Graham, Note, *Burdened by BIPA: Balancing Consumer Protection and the Economic Concerns of Businesses*, U. ILL. L. REV. 929, 957 (2022) (acknowledging the importance of balancing the "need for biometric privacy protection with the protection of businesses").

[448] *See* Deana Pollard Sacks, *Snyder v. Phelps: A Prediction Based on Oral Arguments and the Supreme Court's Established Speech-Tory Jurisprudence*, CARDOZO L. REV. DE NOVO 418, 422 (2010) ("The public figure/private individual distinction was first recognized in defamation cases. In both *New York Times Co. v. Sullivan* and *Gertz v. Robert Welch, Inc.*, the Court made clear that public figures are entitled to less tort law protection than persons who lead private lives because public figures 'voluntarily inject' themselves into the public spotlight and thereby 'assume the risk' of sharp attacks on their character.").

[449] *See supra* notes 187–90 and accompanying text (discussing that appropriation of one's identity and right to publicity are primarily used by celebrities and public figures due to the issues private plaintiffs have in proving damages).

[450] *See* discussion *infra* Section VIII.A.

[451] *See* discussion *infra* Section VIII.A; *see also* 17 U.S.C. § 504(c)(3)(A) (2024).

additional damages could also be warranted if an employer violates an employee's license, thereby misappropriating the employee's likeness, willfully or recklessly.[452] Moreover, any statute implemented, even one which imposes fines on an employer for the same infractions, would need to retain the employee's right of action under privacy torts and their license agreement to provide employees the option to collect on any misappropriation of their likeness.[453] Providing the employee with the right to pursue an action against their employer is paramount to balancing the power dynamic between the employer and the employee.[454]

A. Statutory Damages: Borrowing from Intellectual Property Law

The number of cases surrounding the right to publicity for a non-public figure are inadequate to form a sufficient basis for analysis because they are frequently dismissed on procedural grounds and rarely reach the damages stage of litigation.[455] To make the matter even more complex, determining the actual value of each person's likeness may be impossible without relying on the factors associated with celebrities, public figures, and athletes (e.g., success in their field of choice, popularity, recognizability, and social following).[456] The average person is likely to lack certain

---

[452] *See* discussion *infra* Section VIII.B.; *see also* 17 U.S.C. § 504(c)(3)(A).

[453] *See infra* Section VIII.C; *see, e.g.,* 17 U.S.C. § 504 (a)–(c); Rosenbach v. Six Flags Entm't Corp., 129 N.E.3d 1197, 1206 (Ill. 2019) (asserting that a violation under 740 ILCS 14/15 [BIPA] is "in itself, sufficient to support the individual's or customers statutory cause of action.").

[454] *See* Jenny R. Yang & Jane Liu, *Strengthening Accountability for Discrimination*, ECON. POL'Y INST. (Jan. 19, 2021), https://www.epi.org/unequalpower/publications/strengthening-accountability-for-discrimination-confronting-fundamental-power-imbalances-in-the-employment-relationship/ (arguing that US courts must interpret certain laws with a deeper understanding of the imbalances in the employment relationship to provide employees with a meaningful private right of action should an employer violate an employee's statutory rights).

[455] *See* Ratermann v. Pierre Fabre USA, Inc., 651 F.Supp.3d 657, 671 (S.D.N.Y. 2023); Hepp v. Facebook, 14 F.4th 204, 214 (3d Cir. 2021); Marshall v. ESPN Inc., 111 F.Supp.3d 815, 825 (M.D. Tenn. 2015); Milo & Gabby, L.L.C. v. Amazon.com, Inc., 12 F.Supp.3d 1341, 1349 (W.D. Wash. 2014); Dutch Jackson IATG, L.L.C. v. Basketball Mktg. Co., 846 F.Supp.2d 1044, 1052 (E.D. Mo. 2012).

[456] Adam R. Cocco & Anita M. Moorman, *Untapped Potential: An Examination of Name, Image, and Likeness Earnings Estimates for Community College Athletes*, 15 J. ISSUES INTERCOLLEGIATE ATHLETICS 256, 260–61 (2022) (examining name-in-likeness value of college athletes as social media influencers); Nathan Sharp et al., *Name, Image, and Likeness: Assessing One's "Brand Identity,"*

factors—such as popularity and recognizability—that are typically used in damage assessments under right to publicity laws.[457] As a result, a general approach to calculating damages, rather than one based on detailed, case-specific analysis, may be more suitable for non-public figures like employees.[458] By drawing from intellectual property law, a standardized method could be developed to calculate damages when an average person's likeness is misappropriated through biometrics.

There are three categories of damages available to successful copyright infringement plaintiffs: (1) actual damages; (2) infringer's profits; and (3) statutory damages.[459] Actual damages, sometimes called "compensatory damages," are the losses the infringed person actually suffered as a result of the infringer and are attributable to the infringing activity.[460] Actual damages may be in the form of lost sales, licensing revenues, or other provable financial loss stemming from the infringement.[461] Conversely, awards of the infringer's profits consist of "any profits of the infringer that are attributable to the infringement and are not taken into account in computing the actual damages."[462] The infringer's profits are typically only awardable if the infringer's profits exceed the infringed person's actual damages.[463] Statutory damages are specific, monetary damages set by law in place of actual damage awards.[464] In a copyright infringement action, a plaintiff may "elect their remedy" and pursue either actual damages or statutory damages, but not both.[465]

LIBERTY U. (May 20, 2024), https://digitalcommons.liberty.edu/cgi/viewcontent.cgi?article=2448&context=research_symp (a study examining college athletes on the Athlete Brand Identity Scale [ABIdS], which consists of four different dimensions: athletic integrity, athletic success, fan engagement, and character traits).

457 *See supra* notes 187–90, 448 and accompanying text; *see also* Bonilla v. Ancestry.com Operations Inc., 574 F.Supp.3d 582, 597 (N.D. Ill. 2021); Upper Deck Co. v. Flores, 569 F.Supp.3d 1050, 1068 (S.D. Cal. 2021).

458 *See supra* notes 455–57 and accompanying text.

459 17 U.S.C. § 504(a) (2024).

460 17 U.S.C. § 504(b).

461 Hard Candy, LLC v. Anastasia Beverly Hills, Inc., 921 F.3d 1343, 1353 (11th Cir. 2019); Bell v. Taylor, 827 F.3d 699, 709 (7th Cir. 2016); Dash v. Mayweather, 731 F.3d 303, 312 (4th Cir. 2013).

462 17 U.S.C. § 504(b).

463 *See* ECIMOS, LLC v. Carrier Corp., 971 F.3d 616, 631–32 (6th Cir. 2020); Aqua Shield v. Inter Pool Cover Team, 774 F.3d 766, 770 (Fed. Cir. 2014); 4 Pillar Dynasty LLC v. N.Y. & Co., 933 F.3d 202, 212 (2d Cir. 2019).

464 17 U.S.C. § 504(c).

465 *See* Smith v. Thomas, 911 F.3d 378, 381–82 (6th Cir. 2018); Coach, Inc. v. Hubert Keller, Inc., 911 F. Supp. 2d 1303, 1308–09 (S.D. Ga. 2012); Mango v.

Among these three damage categories, only statutory damages appropriately apply to misappropriation of one's likeness via biometrics for non-public figures. Proving actual damages in standard cases of copyright infringement is already an onerous task.[466] Attempting to trace a non-public figure's biometric information to assess the truest amount of profits and opportunities lost because of the misappropriated use of those biometrics would be an impossible task.[467] Similarly, proving how much an employer profited from a single employee's biometrics would be impractical at best.[468] Furthermore, it would be inappropriate to contemplate the profits by the employer without also including the actual damages portion of the calculation because the employer-infringer's profits would be awarded only when the profits exceed the employee's actual damages under the intellectual property law framework.[469] Because neither actual damages nor infringer's profits are feasible for employee biometric licensure violation awards, only the third option for recovery provided by copyright infringement law remains: statutory damages.[470]

Statutory damages for copyright infringement establish a monetary range to be awarded based on the severity of the infringement.[471] Each infringement may result in an award between $750 and $30,000, but each infringement includes the entire work and "all the parts of a compilation or derivative work constitute one work."[472] Thus, if an infringer were to distribute the infringed work many times over, but those distributions all derived from the same single work, then the infringer would have committed only one infringement and be liable for a single award

---

BuzzFeed, Inc., 356 F. Supp. 3d 368, 374–75 (S.D.N.Y. 2019).

466 *See Hard Candy*, 921 F.3d at 1354; Chi-Boy Music v. Charlie Club, Inc., 930 F.2d 1224, 1229–30 (7th Cir. 1991); Frank Music Corp. v. Metro-Goldwyn-Mayer, Inc., 886 F.2d 1545, 1554 (9th Cir. 1989); Cable/Home Commc'n Corp. v. Network Prods., 902 F.2d 829, 850–51 (11th Cir. 1990).

467 *See supra* notes 187–90, 466, 448 and accompanying text.

468 *See Cable/Home Commc'm Corp.*, 902 F.2d at 850–51 ("Generally, statutory damages are awarded when no actual damages are proven, or actual damages and profits are difficult or impossible to calculate.") (citation omitted).

469 *See supra* notes 459–63 and accompanying text.

470 *See supra* note 459 and accompanying text. *See generally* David V. Radack, *Remedies for Copyright Infringement*, JOM: MINERALS, METALS & MATERIALS SOC'Y (1998), https://www.tms.org/pubs/journals/jom/matters/matters-9805.html (discussing how the plaintiff in a copyright infringement action can elect to recover different damages).

471 17 U.S.C. § 504(c).

472 17 U.S.C. § 504(c)(1).

typically ranging between $750 and $30,000.[473] If, however, the infringement was found to be committed willfully or recklessly, then a court may increase the statutory damages up to an additional $150,000.[474]

Although typical infringements include "all the parts of a compilation or derivative work" as one work,[475] the collection and compilation of one's biometrics is not so simple that it should be considered a single work. Each collection, easily occurring multiple times per day, is a separate capture of a person's face and a separate recalculation of their identity (i.e., their facial geometry is recalculated and compared for each time the employer uses their facial recognition software to identity an employee).[476] Attaching damages to the plethora of captures of an employee's face that may occur as the employee walks throughout their workplace may strike some as too excessive to be workable within the copyright infringement model.[477] However, treating an entire collection of one's facial geometry and every subsequent collection, recollection, comparison, and use of that facial geometry—especially within the context of a terminated license—may be insufficient to protect

---

[473] *Id.*; *see* Yvette Joy Liebesman, *Intellectual Property Edition Article: Redefining the Intended Copyright Infringer*, 50 AKRON L. REV. 765, 809–10 (2016) ("[S]tatutory damages are based on the 'work' and not the 'copy,' [so] the same liability is incurred whether one makes 2, 20, 200 or 20,000 unauthorized copies.").

[474] 17 U.S.C. § 504(c)(2); *see* L.A. Printex Indus., Inc. v. Doe, 543 Fed. App'x 110, 111 (2d Cir. 2013) ("When a plaintiff can demonstrate, either directly or through circumstantial evidence, that the defendant had knowledge that his actions constituted infringement, or recklessly disregarded such possibility, enhanced statutory damages for willful copyright infringement under 17 U.S.C. § 504(c)(2) may be awarded.").

[475] *See supra* notes 472–73 and accompanying text.

[476] *See* James Andrew Lewis & William Crumpler, *How Does Facial Recognition Work?*, CTR. STRATEGIC & INT'L STUD. (June 10, 2021), https://www.csis.org/analysis/how-does-facial-recognition-work; Armen Ghambaryan, *Deploying Facial Recognition Technology at the Enterprise Level*, SCYLLA, https://www.scylla.ai/deploying-facial-recognition-technology-at-the-enterprise-level/ (last visited Oct. 31, 2024); Press Release, Nat'l Acads., Advances in Facial Recognition Tech. Have Outpaced Ls., Reguls. (Jan. 17, 2024) (on file with author) ("Systems utilize trained artificial intelligence models to extract facial features and create a biometric template from an image, and compare the features in the template to the features of another image or set of images to produce a similarity score.").

[477] *See* Amanda Levendowski, *Resisting Face Surveillance with Copyright Law*, 100 N.C. L. REV. 1015, 1043–45, 1048–50 (discussing difficulties plaintiffs may have in facial recognition copyright litigation, including issues in establishing standing and the potential for defendants to successfully argue that facial profiles fall under fair use).

employees' rights. A better balance may be struck by modifying the copyright law damages framework once again to depend upon the amount of time the employee's data is kept past the license's termination date rather than the number of "works" infringed upon.

Once a person's employment terminates, this Article contends that the license for the person's likeness via their biometrics should also terminate.[478] Any retention or use of those biometrics beyond that point would then be a misappropriation of that person's likeness and subject to damages.[479] Certain allowances may be granted to account for business processes and a thorough disposition of those biometrics, but these allowances must not exceed fourteen days before the retention of those biometrics is considered unreasonable, willful, or reckless.[480] In an era where electronic information is easily accessible, queryable, and organized for efficient comparison, there are no obstacles which would reasonably prevent an employer from being able to quickly determine where specific biometric identifiers reside and promptly destroy them.[481] Additionally, a fourteen-day grace period would provide employers with a reasonable amount of time to properly

---

[478] *See* discussion *supra* Section VI.C.v.

[479] *See* discussion *supra* Sections VI.C.v, viii.

[480] *See supra* Section VI.C.viii. *See generally Storage Limitation Principle – How Long Should You Keep Personal Data?*, DATA PRIV. MANAGER: BLOG (Mar. 20, 2021), https://dataprivacymanager.net/how-long-should-you-keep-personal-data-data-retention/ (discussing the data principle of storage limitation in the context of the GDPR's requirement that data not be stored longer than needed); Catie Edmondson, *An Airline Scans Your Face. You Take Off. But Few Rules Govern Where Your Data Goes.,* N.Y. TIMES: INT'L ED. (Aug. 7, 2018), https://www.nytimes.com/2018/08/06/us/politics/facial-recognition-airports-privacy.html (identifying fourteen days as the maximum time period Customs and Border Protection will retain facial scans of American citizens); 1 DAVID J. OBERLY, BIOMETRIC DATA PRIV. COMPLIANCE & BEST PRACTICES § 11.03 (2024 ed.) ("As a matter of best practices, companies should implement a data retention and destruction schedule that provides for biometric data to be destroyed as soon as practicable . . . in the context of employers, when the employment relationship with a worker has ceased . . . destroying biometric data at the earliest feasible juncture can significantly limit potential liability exposure. . . .").

[481] *See generally Personally Identifying Information (PII): How is it Destroyed?*, FULL CIRCLE ELECS. (Jan. 19, 2023), https://fullcircleelectronics.com/resources/pii-how-do-you-destroy-it/ (explaining different ways corporations can destroy PII, including through digital destruction and sanitization); *What Are the Different Types of Data Destruction and Which One Should You Use?*, DATA SPAN: BLOG (July 20, 2023), https://dataspan.com/blog/what-are-the-different-types-of-data-destruction-and-which-one-should-you-use/ (identifying and explaining different methods of data destruction).

conclude any terms of the license. Any delay beyond this point would thus be unreasonable and provide the employer inappropriate access to and use of the person's biometric identifiers, which may then be subject to uses that the employer no longer has permission to apply against those biometric identifiers.[482]

Each day the employee's biometrics are kept beyond those fourteen days should be considered a separate infringement. Each day that passes is an additional unreasonable retention of the collection, and therefore uses and applications of that person's likeness.[483] These proposed time-based damages would serve as the base of statutory damages. Much like damage multipliers available in copyright infringement cases,[484] the base statutory damages could be supplemented with additional damages if certain conditions are met.

B. Adjusting for Willful or Reckless Misappropriation and Actual Breaches

There are two additional, but separate, factors which should enhance the potential damages that an employer is subject to. The first aggravating factor would be if the employer acted willfully or recklessly in its misappropriation of the biometric information of its former employee.[485] The second would occur if the employer was subject to a data breach that may have compromised the biometric identifiers.[486] If either factor is implicated in any case, additional damages could be warranted.

A willful or reckless infringement enhances the damages in copyright cases, and is established by a preponderance of the evidence.[487] "Subjective willfulness alone—i.e., proof that the defendant acted despite a risk of infringement that was 'either known or so obvious that it should have been known to the accused

---

[482] *See* discussion *supra* Section VI.B.

[483] *See* 17 U.S.C. § 101 ("A 'derivative work' is a work based upon one or more preexisting works."); 1 MELVILLE B. NIMMER, NIMMER ON COPYRIGHT § 3.01 (2024 ed.) ("[A]ny work based in whole, or in substantial part, upon a pre-existing (or 'underlying') work, if it satisfies the requirements of originality . . . and is not itself an infringing work, will be separately copyrightable.").

[484] *See supra* notes 471–74 and accompanying text.

[485] *See infra* notes 487–92 and accompanying text.

[486] *See infra* notes 496–50.

[487] *E.g.*, Capitani v. World of Miniature Bears, Inc., 55 F. Supp. 3d. 781, 786, 799 (M.D. Tenn. 2021) (discussing the standard of proof as a preponderance of evidence and discussing willful infringement).

infringer,'—can support an award of enhanced damages."[488] Objective reasonableness, on the other hand, may be a factor when determining if a defendant acted willfully, but objective reasonableness alone is not enough to defeat an assertion of willfulness.[489]

When determining whether an employer infringed an employee's likeness, objective reasonableness may act as a mitigating factor for employers on findings of willfulness. However, the objective reasonableness would be called into question if the employer retained the information even after the proposed fourteen-day grace period from the employee's termination, as would be required by the statute for liability to attach anyway.[490] Immediately upon an employee's termination, the employer is aware, or should be aware, of the termination of the license granting them access to the former employee's biometric identifiers. To retain the biometric identifiers beyond that termination misappropriates the person's likeness with the employer's knowledge.[491] While it could be objectively reasonable to keep the biometrics for up to fourteen days, failing to dispose of the biometrics after fourteen days should be an adequate basis for a court to find a willful or reckless misappropriation. Should a court find an employer willful or reckless in its misappropriation, the statute should further borrow from copyright infringement law and allow the court to award an additional $150,000 for the plaintiff.[492]

However, a conservative mind may not approve of the suggested

---

[488] WesternGeco, LLC, v. ION Geophysical Corp., 837 F.3d 1358, 1362 (Fed. Cir. 2016) (quoting Halo Elecs., Inc. v. Pulse Elecs., Inc., 579 U.S. 93, 97 (2016) (citation omitted)).

[489] *See* WBIP, LLC v. Kohler Co., 829 F.3d 1317, 1340 (Fed. Cir. 2016) (discussing that defenses mitigating willfulness must be objectively reasonable); Stryker Corp. v. Zimmer, Inc., 782 F.3d 649, 661–62 (Fed. Cir. 2015) (discussing objective reasonableness as a defense to objective recklessness); Exmark Mfg. Co. v. Briggs & Stratton Power Prods. Grp., LLC, 879 F.3d 1332, 1337, 1353 (Fed. Cir. 2018) ("[T]he district court [does not] determine[] as a threshold matter whether the accused infringer's defenses are objectively reasonable. Rather, the entire willfulness determination is to be decided by the jury.").

[490] *See* Lee v. Mike's Novelties, Inc., 543 F. App'x 1010, 1016–17 (Fed. Cir. 2013) (discussing how a defense must be reasonable, making the risk of infringement not high enough to satisfy the objective prove of willfulness); *supra* notes 478–82 and accompanying text.

[491] *See supra* notes 478–82 and accompanying text.

[492] 17 U.S.C. § 504(c)(2) (allowing the court to use its discretion to increase the award of statutory damages to a sum of not more than $150,000 where the copyright owner proves willful infringement).

automatic allowance of both traditional statutory damages and willfulness or recklessness enhancers whenever an employer keeps an employee's biometric information beyond the grace period.[493] Critics in general may also require additional violations or acts by the employer to justify a finding of willfulness or recklessness beyond simple misappropriation.[494] One solution to any such argument could be to set a second timing threshold (e.g., 30 days from employment termination) when willfulness or recklessness automatically attaches once that threshold is passed. Such a second-timing-approach may, however, be less flexible than the fourteen-day grace period alone since the former calls for an automatic enhancement at the second timing threshold, whereas courts would retain some discretion in determining any willfulness or recklessness of the misappropriation under the latter.[495]

Data breaches are nearly an inevitable truth rather than a mere possibility for any company maintaining electronic information.[496] The impacts of those breaches are significant, far-reaching, and may cause ripple effects for both businesses and victims alike.[497]

---

[493] *See generally* Ben Depoorter, *Copyright Enforcement in the Digital Age: When the Remedy is the Wrong,* 66 UCLA L. REV. 400, 415–16 (2019) (discussing the perception that statutory damages can lead to excessive court awards in copyright law, particularly when willful infringement is alleged).

[494] *See generally id.*

[495] *See supra* notes 487–92 and accompanying text (explaining the application of the suggested willfulness or recklessness factor).

[496] David Barton, *When Will Your Data Breach Happen? Not a Question of if but When*, SEC. INFO WATCH (Mar. 10, 2015), https://www.securityinfowatch.com/cybersecurity/information-security/article/12052877/preparing-for-your-companys-inevitable-data-breach (discussing how no company is safe from a data breach this day in age); Tyler Anders & Victoria Oguntoye, *Not "If" But "When"–The Ever Increasing Threat of a Data Breach in 2021*, K&L GATES (July 15, 2021), https://www.jdsupra.com/legalnews/not-if-but-when-the-ever-increasing-8569092/ ("If the statistics are correct, the question for most companies is not *if* they will be a victim of cybercrime, but *when*."); *see also The Growing Threat of Data Breaches,* DELOITTE CAN., https://www2.deloitte.com/ca/en/pages/risk/articles/growing-threat-of-data-breaches.html (last visited Oct. 10, 2024) (analyzing statistical trends in cybercrimes and data breaches from 2015 to 2020 and suggesting that companies prepare for potential data breaches).

[497] *See* Keman Huang et al., *The Devastating Business Impacts of a Cyber Breach*, HARV. BUS. REV. (May 4, 2023), https://hbr.org/2023/05/the-devastating-business-impacts-of-a-cyber-breach (discussing what impacts can occur when businesses suffer a data breach); Sonya Sellmeyer, *Consumer Connection: The Impact of Data Breaches on Consumers*, IOWA INS. DIV. (May 28, 2024), https://iid.iowa.gov/consumer-connection/2024-05-28/impact-data-breaches-cons ("Once in the wrong hands, sensitive information can lead to various forms of identity theft, fraud, and financial loss for affected consumers.").

The threat and consequences of breaches are significant enough that the GDPR allows for a company to be fined up to €20 million or 4% of the company's worldwide annual revenue, whichever is higher, if the company fails to comply with basic principles for data processing.[498] Some factors used by the EU in determining the degree of the penalty include:

> [1] the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them; [2] the intentional or negligent character of the infringement; . . . [3] the categories of personal data affected by the infringement; . . . [and 4] any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.[499]

The United States focuses more on the need for notification to regulators and to potential victims of the breaches rather than on the actual damages the breach may have caused to the people exposed in the breach.[500]

Should an employer suffer a breach within the timeframe that it inappropriately retained biometric identifiers, any statutory misappropriation damages awarded under this Article's recommendations should double. This would change the range of damages to be between $1,500 and $60,000 per day.[501] This breach-based doubling effect would be separate from the willfulness or recklessness factor. While the willfulness or recklessness factor could become subject to this doubling effect, the breach factor should instead consider whether the employer has taken adequate

---

[498] GDPR, *supra* note 8, art. 83.

[499] *Id.*

[500] *See* Nuala O'Connor, *Reforming the U.S. Approach to Data Protection and Privacy*, COUNCIL ON FOREIGN RELS. (Jan. 2018), https://www.cfr.org/report/reforming-us-approach-data-protection (arguing that America's "breach-notification laws" are insufficient to protect consumers because they do not result in significant financial harm to companies when they are violated and thus insufficiently incentivize companies to protect consumers' data). *See generally Security Breach Notification Laws,* NAT'L CONF. OF STATE LEGISLATURES (Jan. 17, 2022), https://www.ncsl.org/technology-and-communication/security-breach-notification-laws (listing each state's security breach notification laws).

[501] *See supra* notes 471–73 and accompanying text (containing the suggested damage awards for typical violations under this Article's proposed statutory framework).

steps to safeguard the employee's biometric information. The safeguarding steps, or lack thereof, should then be used to determine if the employee would be entitled to additional damages from a breach. By separating the two damage factors (willfulness and breach) in this way, the damages independently assess separate ways in which the employer has caused harm to the employee.

The protection of one's identity requires more than mere notification of a breach.[502] Breaches may have extensive impacts on the people whose information was exposed to the world at large.[503] Employment-related breaches would expose some of the employees' most sensitive information tied to their identities. The resulting damages would be comparable to damages used to calculate actual damage awards in copyright infringement cases,[504] though the data on the extent of damages would still be insufficient to truly calculate actual damages as per traditional copyright cases.[505] In lieu of actual damages, doubling the statutory damages when a breach occurs after the termination of the license, but before the disposition of the biometric identifiers, is appropriate.

C. Retained Private Right of Action Under Privacy Torts and License Provisions

Any statute implemented should preserve the employee's right of action under these theories and under the terms of their license. It is imperative that employees are able to take private action to protect their rights and their identities rather than leaving their protection solely to a government agency.[506] To establish a statute

---

[502] *See* Nuala O'Connor, *supra* note 500. *See generally* Yasmine Agelidis, Note, *Protecting the Good, the Bad, and the Ugly: "Exposure" Data Breaches and Suggestions for Coping with Them*, 31 BERKELEY TECH L.J. 1057, 1059 (2016) (analyzing the shortcomings of notification-only laws in protecting consumers' personal data).

[503] Agelidis, *supra* note 502, at 1057 (explaining the rise of exposure breaches and the irreparable harm that these breaches can cause).

[504] *See supra* notes 460–63, 466–67 and accompanying text.

[505] *See* Carter v. Vivendi Ticketing U.S. LLC, No. SACV 22-01981-CJC (DFMx), 2023 U.S. Dist. LEXIS 210744, at *15–17 (C.D. Cal. 2023) (discussing how damages can be hard to ascertain in data breaches due to limited data); *supra* notes 460–63, 466–67 and accompanying text.

[506] *See* Michael Bloom, Note, *Protecting Personal Data: A Model Data Security and Breach Notifications* Statute, 92 ST. JOHN'S L. REV. 977, 994–996 (2018) (arguing that private rights of action must be included in data security and breach statutes in order to incentivize companies to comply and to provide

imposing fines and penalties for an employer's violation of an employee's rights, yet barring an employee's right of action, would subject the employee to exploitation by their employer while also preventing the employee from recovering for the violation committed against them.[507] Such a statute would shift the balance sought between the employer and employee to a balance between the employer and the government—the employer would have no, and therefore feel no, obligation to the employee. To permit wronged employees to recover and to keep employers accountable to individual employees, any statutes on this matter should protect the employees right of action.

IX. CONCLUSION

The dynamic between employer and employee regarding the employer's use and collection of biometric information remains imbalanced in favor of the employer due inadequate privacy laws and the sparse coverage of laws addressing biometrics.[508] Technology has progressed to the point where it has become commonplace for law enforcement agencies and private companies alike to use facial recognition software,[509] and facial recognition software has the potential to further imbalance the dynamic between employer and employee by allowing for that further employee exploitation.

Each person has a right to their identity and how it may be shared or withheld.[510] That choice should remain with each person; a person's identity should not be readily relegated to a commercial product for an employer to use as its sole discretion. Employees must prevent employers from exploiting their identities by exercising their rights over their identity and their privacy in the employment context.[511] Through these privacy rights, recognized through the name, image, likeness (NIL) subset of intellectual property law, employees may bargain for a stronger position

adequate protection for harmed consumers); Bock, *supra* note 86, at 327 (identifying the private right of action as one of "the most crucial provisions" of the GDPR and the CCPA because a private right of action "ensures that consumers can be compensated for violations . . . and greatly increases the effectiveness of the statute.").

[507] *See* Bloom, *supra* note 506, at 994–96.

[508] *See supra* notes 22–30 and accompanying text.

[509] *See supra* notes 103–09, 119–122 and accompanying text (examining use of facial recognition software by law enforcement agencies and private companies).

[510] *See* discussion *supra* Part IV.

[511] *See* discussion *supra* Part VI.

should their employers seek to collect and use facial recognition software in the workplace.[512]

One mechanism of protecting those rights is for the employee to license their likeness to their employer strictly within the limits of their employment.[513] Each employee's biometrics is one form of their likeness and can be subject to licensure.[514] In particular, the employee's likeness should only be exploitable by the employer within a limited framework and returned fully to the employee when employment terminates; the employer should retain no further rights to a person's identity and biometric information beyond the term of their employment.[515] To allow otherwise would be to rip those rights away from employees and convert them to little more than a commodities for employers to exploit.

The rights of the People demand that they not become merely a tool for commercial profit. Technology should not remove the implicit right to privacy.[516] The spread of facial recognition software should not lack such restriction that each person has no semblance of control over who collects, uses, controls, and shares their identity. Ultimately, preserving the essence of humanity requires safeguarding the autonomy and dignity of each individual against the encroachments of ubiquitous surveillance technologies.

---

[512] *See* discussion *supra* Part VII.
[513] *See* discussion *supra* Section VI.B.
[514] *See* discussion *supra* Sections V.A., VI.B.
[515] *See* discussion *supra* Part VI.
[516] *See supra* notes 1–7 and accompanying text.