Wyoming Law Review

Manuscript 1511

Out of Hand: Why Federal Protection of Biometric Privacy is a Pressing Issue in U.S. Employment

Emily Harmon

WYOMING LAW REVIEW

VOLUME 24 2024 **NUMBER 2**

Out of Hand: Why Federal Protection of Biometric Privacy is a Pressing Issue in U.S. Employment

Emily Harmon [*]

[*] J.D. Candidate, University of Wyoming College of Law, Class of 2025.

I would like to thank the dedicated efforts of the *Wyoming Law Review* Editorial Board in bringing this Comment to its full potential, and Professors Alan Romero and Jacquelyn Bridgeman for their guidance in the formation of this topic. Thank you to my parents Lance and Amy for your endless love and support; I owe so much to your strength, generosity, and sacrifices. Finally, thank you to my partner Ty for consistently being my sounding board and for providing sugar reinforcements when needed.

ABSTRACT

The practice of using biometric identifiers such as fingerprints, facial recognition, and eye scans in place of usernames and passwords is becoming widespread in the workplace. Because of the lack of federal protection, employers may compel employees' participation in biometric-enabled systems as a term of employment. A person's biometric data cannot be replaced and is often linked to personal and financial accounts. Additionally, employers collecting biometric data often rely on third parties for information technology service and storage. Biometric data collection creates the potential for data breaches, for system malfunctions, and for third parties to learn additional information about the person surrendering biometric data. Federal regulation of employers' collection of biometric data is critical because of the magnitude of the risks inherent to data breaches and the continual encroachment of technology on privacy interests in the workplace. This Comment examines the evolution of conceptions of privacy and the law, and state regulation of personal and biometric data under the Illinois Biometric Information Privacy Act and the California Consumer Privacy Act to demonstrate the critical need for federal regulation of biometric data, particularly within employment. After pointing out the inadequacies of these Acts discussed as applied to the workplace, this Comment suggests a series of mandatory federal procedures that would better safeguard employees' privacy. Employers should be subject to policies that increase transparency of biometric data retention, inform employees of potential risks before enrolling, provide time for consideration, and offer alternatives.

I. INTRODUCTION

Imagine you start a new job.[1] On your first day, your boss mentions in passing that you must hand over a spare set of your car keys, house keys, and electronic login credentials to his colleague, Clark, to finalize your orientation. Your first thought is, "who is Clark?" Sensing your discomfort, he assures you that it isn't as if Clark will drive your car, enter your home, or access your accounts, but rather he will simply hold your personal belongings and information.

Now imagine a different scenario. You start a new job, and your boss mentions in passing that you must register your fingerprints on the company database to finalize your orientation. How are these two scenarios different? In the modern day and age of biometric authentication, there is virtually no difference. Because biometric data is

[1] *Cf.* Eliza Simons, Note, *Putting a Finger on Biometric Privacy Laws: How Congress Can Stitch Together The Patchwork of Biometric Privacy Laws in the United States*, 86 BROOK. L. REV. 1097, 1097 (2021).

often used for authentication across personal accounts and devices, it provides direct access to the intimate and personal aspects of an employee's life.[2] Employees' privacy interests must be protected when employers compel biometric data collection as a term of employment.[3]

This Comment suggests the federal government should protect employees' privacy to mitigate the inherent risks of biometric data collection.[4] Congress should enact federal protection through combining elements of the Illinois Biometric Information Privacy Act (the BIPA) and the California Consumer Privacy Act (the CCPA) to restrict employers' collection of biometric data.[5] Furthermore, Congress should require employers to inform employees of potential risks before enrolling in biometric data collection, provide time for consideration, and offer alternatives to collecting biometric data.[6] The proposed regulations should acknowledge employers' reliance on third-party manufacturers while requiring employers' compliance with procedures that increase the likelihood that employees can understand the risks and process of biometric data collection before agreeing to participate.[7]

Part II of this Comment will define biometric data and why the benefits of biometric authentication have led to its widespread use in employment.[8] The risks of this practice will demonstrate why federal

---

2 *See About Touch ID Advanced Security Technology*, APPLE (Nov. 15, 2023), https://support.apple.com/en-us/105095 [https://perma.cc/UH4X-MHUD]; *see also* Seyede Samine Hosseini & Shahriar Mohammadi, *Review Banking on Biometric in the World's Banks and Introducing a Biometric Model for Iran's Banking System*, 2 J. BASIC & APPLIED SCI. RSCH. 9152, 9155–56 (2012) (providing a list of 121 banks that use biometric authentication globally).

3 *See* Maayan Niezna & Guy Davidov, *Consent in Contracts of Employment*, 86 MODERN L. REV. 1134, 1134–35, 1141 (2023); Drew Robb, *The Future of Biometrics in the Workplace*, SOC'Y HUM. RES. MGMT. (Feb. 22, 2022), https://www.shrm.org/resourcesandtools/hr-topics/technology/pages/the-future-biometrics-workplace.aspx [https://perma.cc/5BQH-L39P].

4 *See FTC Warns About Misuses of Biometric Information and Harm to Consumers*, FED. TRADE COMM'N (May 18, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-warns-about-misuses-biometric-information-harm-consumers [https://perma.cc/7Y4P-PX7R]; Illinois Biometric Information Privacy Act of 2008, 740 ILL. COMP. STAT. § 14/5(f) (2023) ("The full ramifications of biometric technology are not fully known."); *see* Morey J. Haber, *Is Your Identity at Risk from Biometric Data Collection?*, BEYOND TR. (Mar. 21, 2019), https://www.beyondtrust.com/blog/entry/is-your-identity-at-risk-from-biometric-data-collection [https://perma.cc/U547-3F8S]; National Biometric Information Privacy Act of 2020, S.B. 4400, 116th Cong. (2020) (federal bill modeled on state biometric privacy legislation was proposed and failed to pass in 2020).

5 740 ILL. COMP. STAT. §§ 14/1–/99; California Consumer Privacy Act of 2018, CAL. CIV. CODE §§ 1798.100–.199 (West 2023) (amended in 2020).

6 *See infra* Part IV; MARTA OTTO, THE RIGHT TO PRIVACY IN EMPLOYMENT: A COMPARATIVE ANALYSIS, 182, 185 (2016); 740 ILL. COMP. STAT. § 14/15(a).

7 *See infra* Part IV; OTTO, supra note 6, at 185.

8 *Infra* Part II.

protection of biometric data is crucial to protect the privacy interests of employees.[9] Part III will discuss the intersection between privacy and technology to illuminate the gaps in current conceptions of privacy legislation and caselaw.[10] This Part will then address two comprehensive state privacy laws to be used as a model for federal protection of biometric data collection.[11] Part IV will incorporate aspects of current privacy legislation to propose conditions for employers' collection of biometric data that will fortify employees' privacy interests in the wake of biometric technology.[12] Part V will then conclude by advocating for regulation surrounding employers' collection of biometric data.[13]

II. BIOMETRICS IN EMPLOYMENT

A. What Does Biometric Data Look Like?

The term "biometrics" is rooted in two Greek words: "bio" means life and "metric" means to measure.[14] In the modern context, biometric data includes fingerprints, DNA (blood, skin, bone, saliva, urine, etc.), scans of a person's eyes, facial images and recognition, and voice matching.[15] People's behavioral characteristics, such as their walking gait, are sometimes included within the scope of this term.[16] Although biometric data has a wide scope, it generally excludes data such as an individual's medical records, physical descriptors, or written materials.[17] Thus, biometric data does not encompass what may be termed traditional conceptions of "personal information." In sum, biometrics is the science of identifying people based on their innate attributes.[18]

---

9 *See* infra Part II.D.

10 *Infra* Part III.

11 *See infra* Part III.B.

12 *Infra* Part IV.

13 *Infra* Part V.

14 SINJINI MITRA, BO WEN & MIKHAIL GOFMAN, BIOMETRICS IN A DATA DRIVEN WORLD TRENDS, TECHNOLOGIES, AND CHALLENGES 16 (Sinjini Mitra & Mikhail Gofman eds., 2016); Simons, *supra* note 1, at 1098.

15 Sterling Miller, *The Basics, Usage, and Privacy Concerns of Biometric Data*, THOMSON REUTERS (July 20, 2022) https://legal.thomsonreuters.com/en/insights/articles/the-basics-usage-and-privacy-concerns-of-biometric-data [https://perma.cc/4N3U-7EDR]; *What is Biometrics? How is it Used in Security?,* KASPERSKY (2023) https://www.kaspersky.com/resource-center/definitions/biometrics [https://perma.cc/VE79-AY3E] [hereinafter KASPERSKY]; *see* S.B. 4400 § 2(1)(A).

16 *See* S.B. 4400 § 2(1)(A)(v).

17 *Id.* at § 2(1).

18 Antitza Dantcheva, Petros Elia & Arun Ross, *What Else Does Your Biometric Data Reveal? A Survey on Soft Biometrics*, 11 INST. ELEC. & ELEC. ENG'RS TRANSACTIONS ON INFO. FORENSICS & SEC. 441, 441 (2015); NAT'L ACAD. SCIS., BIOMETRIC RECOGNITION: CHALLENGES AND OPPORTUNITIES 16, 18 (Joseph N. Pato & Lynette I. Millett eds., 1st ed., 2010) [hereinafter Pato & Millett].

B. How is Biometric Data Captured and Authenticated?

The standard process for the collection of biometric data involves: (1) enrollment; (2) upload; (3) match; and (4) decision.[19] Broadly, the early stages of enrollment and upload involve employees giving up their biometric data.[20] Specifically, the enrollment phase entails the capture of biometric identifiers.[21] In the case of fingerprint identifiers, the enrollment phase means capturing the image of an individual's fingerprint.[22] Next, in the upload stage, the biometric data given by a user during enrollment is uploaded to a reference database where it is stored, managed, and maintained.[23] Companies may store biometric data on either local or network databases.[24] Companies producing biometric-enabled systems often maintain network databases and may disclose the biometric data to third parties that provide backup storage and other information technology services.[25] Later in this Comment, these third parties will be referred to as "processors" of data while the companies hiring the processors will be referred to as "controllers" of data.[26]

The final two stages, match and decision, detail how the system uses the collected data.[27] While the data must only be enrolled and uploaded once, the system will match the data collected to the data existing within the database each time a person accesses the system.[28] In the matching stage, a recent biometric capture is compared against other images in the reference database.[29] The system's determination of whether the recent capture matches data already enrolled in the database occurs in the final stage.[30] Therefore, in the decision stage, the system determines whether

---

19 MITRA, WEN & GOFMAN, *supra* note 14, at 5–6; *see* Pato & Millett, *supra* note 18, at 25 (referring to enrollment as "capture").

20 MITRA, WEN & GOFMAN, *supra* note 14, at 5–6.

21 *Id.*

22 *Id.*

23 *See, e.g.*, Johnson v. NCR Corp., No. 22-C-3061, 2023 U.S. Dist. LEXIS 19327, at *2–3 (N.D. Ill. Feb. 6, 2023) ("Workers' biometric data is automatically uploaded to . . . [a] database, where it is managed, maintained, and stored on . . . servers.").

24 Pato & Millett, *supra* note 18, at 25. Third parties are often involved in the storage, maintenance, and management of biometric systems. *See id.* at 19–20.

25 *See, e.g.*, *Johnson*, 2023 U.S. Dist. LEXIS 19327, at *2–3. ("NCR also discloses the biometric data to third parties that provide it with back up storage and other IT services."); *see* Pato & Millett, *supra* note 18, at 19–20.

26 *See infra* Part III.B.

27 MITRA, WEN & GOFMAN, *supra* note 14, at 5–6.

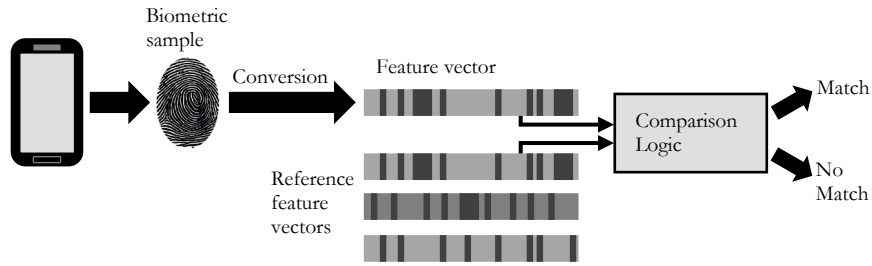
28 Pato & Millett, *supra* note 18, at 25 (referring to "match" as "matcher" and using "action" in place of "decision.").

29 *Id.* at 22 ("A biometric system establishes a probabilistic assessment of a match indicating that a subject at hand is the same subject from whom the reference was stored."); MITRA, WEN & GOFMAN, *supra* note 14, at 5–6; *see* KASPERSKY, *supra* note 15.

30 Pato & Millett, *supra* note 18, at 25.

the user is genuine or an imposter.[31] If the image captured in enrollment matches an image existing in the reference database, the system determines that the user is genuine (see Figure 1).[32] Once a user is determined to be genuine, the user may access all protected information.[33]

Figure 1: The process of biometric authentication.[34]



C. The Growing Use of Biometric Data Collection in Employment

The benefits of collecting biometric data as a means of authentication correspond to the downfalls of using traditional usernames and passwords.[35] For instance, a significant data problem for employers is the vulnerability of their employees' passwords to hackers.[36] Biometric data as a form of authentication increases an employer's security by mitigating the chances of employees' passwords being lost or compromised.[37] Further, biometric data used for "clocking in" prevents time theft by ensuring employees are physically present to manage their time cards.[38] In response

31 MITRA, WEN & GOFMAN, *supra* note 14, at 5–6.

32 *Id.*

33 *See id.*

34 Figure 1 is adapted from *id.* at 6 tbl.2 (demonstrating the process of biometric authentication for a mobile phone).

35 KASPERSKY, *supra* note 15; *see* Robb, *supra* note 3. *But see* Pato & Millett, *supra* note 18, at 19–20 (noting the complexities and variability inherent in biometric systems).

36 *See* SPECOPS, 2022 WEAK PASSWORD REPORT 1, 12 (2022), https://specopssoft.com/wp-content/uploads/2022/02/Specops-Software-Weak-Password-Report-2022-2.pdf [https://perma.cc/VWT8-MAV9]; Jan Lunter, *How Multimodal Biometric Authentication Technology Can Benefit Your Company*, SPICE WORKS (Sep. 26, 2022), https://www.spiceworks.com/it-security/identity-access-management/guest-article/multimodal-biometric-authentication-benefits-your-company/ [https://perma.cc/SZM3-JK2B]; Robb, *supra* note 3.

37 Robb, *supra* note 3; Lunter, *supra* note 36.

38 Sam Blum, *Biometric Monitoring is Booming in the Workplace, Raising Ethical and Legal Questions 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 [https://perma.cc/J5JB-YHH3]; *see* Lunter, *supra* note 36.

to these advantages, many manufacturers are now creating technology that enables employers to use biometric data for authentication purposes.[39]

While medical records do not fall within the scope of biometric data, biometric identifiers can often be used to independently assess health.[40] For example, some employers have expanded biometrics collection to include voluntary participation in company fitness programs.[41] Certain employers further attempted to expand biometric data collection to mandatory wellness screenings during the COVID-19 pandemic.[42]

With the recognized efficiency of biometric authentication, the market for biometric data sees continued growth.[43] The global biometric data market was valued at $35.39 billion in 2020 and is projected to reach a value of $95.33 billion by 2028.[44] As the uses of biometrics in the workplace continue to be realized, the collection and uses of biometric data by employers will likely broaden, which emphasizes the need for federal protection of this sensitive data.

D. What Risks are Unique to Biometric Authentication?

While biometric data is unique, it is not private.[45] Today, people are constantly surveilled and recorded, and their fingerprints are left on every surface they touch.[46] A person's biometric data is routinely linked to the

---

[39] Chuck Leddy, *Next Level Security: Should You be Using Biometric Technology?* AUTOMATIC DATA PROCESSING, https://www.adp.com/spark/articles/2017/03/next-level-security-should-you-be-using-biometric-technology.aspx [https://perma.cc/AV8H-DD46] (last visited Aug. 9, 2024); *see* 740 ILL. COMP. STAT. § 14/5(b) ("Major national corporations have selected the City of Chicago and other locations in this State as pilot testing sites for new applications of biometric-facilitated financial transactions, including finger-scan technologies at grocery stores, gas stations, and school cafeterias."); Blum, *supra* note 38; *see, e.g.*, Smith v. Signature Sys., No. 2021-CV-02025, 2022 U.S. Dist. LEXIS 34383, at *1–2 (N.D. Ill. Feb. 28, 2022) (describing Signature Systems Inc.'s development of biometric-enabled point of sale systems for use in commercial enterprises, including restaurants, casinos, and other hospitality venues).

[40] *See* Blum, *supra* note 38.

[41] *Id.* (providing examples of a range of biometric monitoring systems used in United States work environments).

[42] *See e.g.*, Naughton v. Amazon.com, Inc., No. 20-cv-6485, 2022 U.S. Dist. LEXIS 8 (N.D. Ill. Jan. 3, 2022); *see also* Simons, *supra* note 1, at 1098.

[43] *See Global Biometric Market Size, Projections of Share, Trends, and Growth for 2023-2030*, LINKEDIN (Sep. 2, 2023), https://www.linkedin.com/pulse/global-biometric-market-size-projections-share [https://perma.cc/V55R-PDVS].

[44] *Id.*

[45] A.K. Jain & U. Uludag, *Hiding Biometric Data*, 25 INST. ELEC. & ELEC. ENG'RS TRANSACTIONS ON PATTERN ANALYSIS & MACHINE INTEL. 1494 (2003).

[46] *See id.* (describing eight potential types of attack that may attempt to manipulate biometric data collection systems).

authentication of personal and financial accounts.[47] A breach of a person's biometric data could lend access to any account, device, or building to which they had used biometric identifiers to authenticate entry.[48] But if a person's biometric data is breached, it cannot be corrected as simply as a compromised password; a breach of biometric data leaves the victim without any true recourse.[49] Because a biometric data breach may lead to financial loss, increased risk of identity theft, and the inability to use biometric authentication in the future, federal regulation around the collection of biometrics must be developed.[50]

III. CURRENT PRIVACY LAW

A. Constitutional Privacy

The laws regarding collecting and storing an employee's biometric data for something akin to a password or a company wellness program is yet to be addressed in most jurisdictions.[51] Instead, privacy protections have been somewhat solidified through interpretations of constitutional provisions, and state legislation relating to privacy generally.[52] This sub-part reconciles the constitutional background of generally recognized privacy rights and two comprehensive state statutory schemes on privacy.[53]

---

47 *What are the Consequences of a Biometric Data Leak?*, WORKING CAP. REV., https://workingcapitalreview.com/2019/09/what-are-the-consequences-of-a-biometric-data-leak/ [https://perma.cc/W6FW-Z7ZS] (last visited Aug. 9, 2024) [hereinafter *Data Leak*]; *see e.g.*, Zoe Kleinman, *Politician's Fingerprint 'Cloned From Photos' By Hacker*, BRIT. BROAD. CO. NEWS, (Dec. 29, 2014) https://www.bbc.com/news/technology-30623611 [https://perma.cc/C8QP-MQZY] (describing a hacker's replication of German Defense Minister's fingerprints from a series of high-resolution photos); Alex Hern, *Hacker Fakes German Minister's Fingerprints Using Photos of Her Hands*, THE GUARDIAN (Dec. 30, 2014) https://www.theguardian.com/technology/2014/dec/30/hacker-fakes-german-ministers-fingerprints-using-photos-of-her-hands [https://perma.cc/NZ7Y-LK9E].

48 *Data Leak, supra* note 47.

49 Miller, *supra* note 15; 740 ILL. COMP. STAT. § 14/5(c); Bruce Schneier, *Stealing Fingerprints,* VICE (Sept. 29, 2015, 9:25 AM), https://www.vice.com/en/article/78x5va/stealing-fingerprints%20 [https://perma.cc/RRC9-D76L]; KASPERSKY, *supra* note 15; *see FTC Warns About Misuses of Biometric Information and Harm to Consumers*, *supra* note 4; 740 ILL. COMP. STAT. § 14/5(f) ("The full ramifications of biometric technology are not fully known."); Haber, *supra* note 4.

50 *See* 740 ILL. COMP. STAT. § 14/5(c) ("Biometrics . . . are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions.").

51 Blum, *supra* note 38; *see* OTTO, *supra* note 6, at 183.

52 *See* Simons, *supra* note 1, at 1106.

53 *See infra* Part III.A–B; CAL. CIV. CODE §§ 1798.100–.199; 740 ILL. COMP. STAT. §§ 14/1–/99.

1. Generally Recognized Privacy Rights

Privacy is not explicitly mentioned in the United States Constitution;[54] however, Congress and courts have created a "patchwork" of privacy laws.[55] This patchwork of constitutional provisions, state statutes, and caselaw regarding privacy creates vague yet narrow protections.[56] The Constitution only protects people from invasions of privacy by a government actor and thus constitutional privacy protections are often restricted to the context of public workplaces or criminal law.[57] However, the modern interpretation of the caselaw on privacy protections within public employment indicates how the legal framework of private-sector employment should be adjusted.[58] This sub-part will examine constitutional claims to privacy for the public employee against government intrusion through technology to emphasize what federal regulations are needed in private sector employment.[59]

2. Privacy for the Public Employee

Public employees' expectations of privacy at work are contingent on the reality of office practices and procedures.[60] Courts examining privacy

54 Simons, *supra* note 1, at 1105; *see* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 1 KINGSTON L. REV. 66, 67 (1968); *see also* 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, 44 (2021).

55 Simons, *supra* note 1, at 1105; Buresh, *supra* note 54, at 63 ("Congress has passed privacy laws on a topic-by-topic basis predicated on practical political needs, such as adopting the Fair Credit Reporting Act, the Health Insurance Portability and Accountability Act, and the Gramm-Leach-Bliley Act."); *see* Katz v. United States, 389 U.S. 347, 350 (1967) ("[P]rotection of a person's general right to privacy – his right to let alone by other people – is like the protection of his property and of his very life, left largely to the law of the individual States.").

56 *See* Griswold v. Connecticut, 381 U.S. 479, 484 (1965) (explaining the enumerated rights within the Constitution create a penumbra which defines the "zone of privacy."). *Griswold* first extended the protections of the Fourteenth Amendment to include a person's right to privacy in home and family life. Rights to privacy have continued to expand and be redefined over time. Warren & Brandeis, *supra* note 55, at 66–67. Because the right to privacy is not explicitly defined by current law, and continues to expand, the "zone of privacy," is paradoxically vague and narrow. *See id.*

57 *See, e.g.*, Carpenter v. United States, 585 U.S. 296, 309–13 (2018) (holding law enforcement's access to defendant's cell phone records violated his reasonable expectation of privacy under the Fourth Amendment); O'Connor v. Ortega, 480 U.S. 709, 717 (1987) (holding where a doctor was suspended for misconduct, the search of his office did not violate a violation of his "reasonable expectation" of privacy under the Fourth Amendment).

58 *See id.*

59 *See infra* Part III.A.2.

60 *O'Connor*, 480 U.S. at 717 (holding where a doctor was suspended for misconduct, the search of his office did not violate a violation of his "reasonable expectation" of privacy under the Fourth Amendment).

in the workplace explore the issue through a factor test that determines "reasonableness" and the nature of the intrusion to evaluate whether there is a loss of privacy.[61] Factors assessed under this inquiry include the *environment* where the intrusion occurred, the practices of the employer, and communications between the employer and employee.[62] The limitations on employees' expectation of privacy in the workplace have similarly been conditioned for electronic information.[63]

However, when applying this factor test to an invasion of electronically stored information, the consideration of the environment where the intrusion occurred is complicated by technology.[64] In *United States v. Hamilton*, the United States District Court for the Eastern District of Virginia, found that employees of a public school district had no reasonable expectation of privacy on district computers that displayed a login disclaimer that any electronic communications could be viewed by the employer.[65] Because employees presumably only have access to district computers at work, it was reasonable to assume the employer would have ultimate control over the information stored on the computers.[66] Accordingly, a lack of limitations on privacy within the physical workspace and on company-owned electronics seems clear cut, particularly where an employer informs employees of the scope of the limitation on privacy.[67]

However, current case law fails to anticipate the complex intrusions of privacy presented by an employer's collection of biometrics.[68] While an employer collects biometrics in the workplace, an intrusion or breach of an employee's biometric data at work opens the employee up to virtually limitless invasions of privacy in their personal life.[69] Current case law only addresses employers' invasions of public employees' privacy that occur in the workplace.[70] Congress must recognize this analysis fails to address the

61 *See* Vega-Rodriguez v. P.R. Tel. Co., 110 F.3d 174, 178–80 (1st Cir. 1997); *see also O'Connor*, 480 U.S. at 717–20.

62 *See Vega-Rodriguez*, 110 F.3d at 178–80.

63 *See, e.g.*, United States v. Hamilton, 778 F. Supp. 2d 651, 652–53 (E.D. Va. 2011) (holding employees of a public school district had no reasonable expectation of privacy on work computers that displayed a login disclaimer that any electronic communications could be viewed by the employer.); *Vega-Rodriguez*, 110 F.3d at 184 (finding a quasi-public employer's surveillance of a common workspace reasonable where employees were given notice.); Laura K. Donohue, *The Fourth Amendment in a Digital World*, 71 N.Y.U. ANN. SURV. AM. L. 553, 554 (2016).

64 *See, e.g.*, Carpenter v. United States, 585 U.S. 296, 306 (2018); Donohue, *supra* note 63, at 612–13.

65 *Hamilton*, 778 F. Supp. 2d at 654–55.

66 *See id.*

67 *See id.*

68 *See* Simons, *supra* note 1, at 1107–08.

69 *See infra* Part II.D.

70 *See, e.g.*, *Hamilton*, 778 F. Supp. 2d at 652–53; Vega-Rodriguez v. P.R. Tel. Co., 110 F.3d 174, 178–80 (1st Cir. 1997).

potential for infringements on privacy within the workplace and thereby creates a domino effect on an employee's personal life.[71]

B. State Privacy Legislation

Regulation of biometric data remains largely unaddressed by the vast majority of jurisdictions.[72] Despite a lack of congressional action and common law supporting employees, the dangers of surrendering biometric data have primarily been anticipated by select states in the context of consumerism.[73] California is one of a few states that have passed statutes regulating how businesses handle biometric data collected from consumers.[74] Illinois is among the extreme minority of states expressly regulating biometric data collected from employees in addition to consumers.[75] The varying approaches among these states that have adopted privacy legislation emphasize the need for a federal floor of protection.[76] This sub-part will discuss the comprehensive privacy legislation in both California and Illinois to support a proposed model for federal protection of biometric data privacy.[77] The discussion of this state legislation will be narrowly tailored to support a proposal that existing state privacy protections should be federally fortified in an employment relationship.[78]

---

71 *See* Donohue, *supra* note 63, at 612–13.

72 *See* Simons, *supra* note 1, at 1101.

73 *See, e.g.*, CAL. CIV. CODE §§ 1798.100–.199; Consumer Data Protection Act, VA. CODE ANN. §§ 59.1-575 to -584 (2024) (legislation enacted as of 2023 takes a similar approach to consumer privacy protections as stated in the CCPA.); Colorado Privacy Act, COLO. REV. STAT. § 6-1-1302(III–V) (2024) (taking a similar approach to California and Virginia, Colorado's Act protects personal information of consumers in the wake of new technology); CONN. GEN. STAT. § 42-521(d) (2024). Enacted as of 2023, the Connecticut Act takes a similar approach to the previous acts, like California and Virginia differentiating between the duties of "processors" and "controllers" of data. *Id.*

74 CAL. CIV. CODE §§ 1798.100–.199.

75 740 ILL. COMP. STAT. §§ 14/1–/99; *accord* WASH. REV. CODE § 40.26.020 (2024) (regulating the retention procedures, notice, and consent required before a state government actor may collect biometric data). Unlike the BIPA, Washington's regulation does not apply to private entities. WASH. REV. CODE § 40.26.020(7)(a); TEX. BUS. & COM. CODE ANN. § 541.001–.205 (enacted June 18, 2023, effective July 1, 2024). Texas's legislation is similar to Virginia, California, and Colorado, but includes the collection of biometric data and offers a pro-business approach, simply requiring controllers to post a notice that they may sell a consumer's biometric personal data. *Id.* at § 541.102(c). *But see* § 541.107(a) (prohibiting "small businesses" from selling a consumer's personal data without consent).

76 *Cf.*, WASH. REV. CODE § 40.26.020 (applying only to government entities' collection of people's personal and biometric data.); TEX. BUS. & COM. CODE ANN. § 541.004 (exempting only "personal" or "household" collection of personal data from application of the Texas statute).

77 *Infra* notes 79–122 and accompanying text.

78 *See* OTTO, *supra* note 6, at 185.

1. The California Consumer Privacy Act

The CCPA provides comprehensive protection for the personal information of California consumers.[79] The CCPA provides a helpful framework for federal protection. Specifically, the CCPA differentiates between parties who process data and businesses that control data.[80] "Controllers" of data are the businesses that define the purpose and procedure for processing data while also interacting directly with the subjects of the data collection.[81] "Processors" of data are the third parties selected by the controllers of data to assist in processing data on network databases.[82] Any measures taken by processors are defined by the parameters set by the controllers who have ultimate control authority over the data.[83] The CCPA provides consumers with a degree of control over their personal information as controllers provide consumers transparency and security, and processors must act in conformity with the expectations set by controllers.[84] This section will give an overview of the CCPA's provisions, further examine the differentiation between processors and controllers, and discuss some of the protections offered to consumers under the CCPA.[85]

i. The CCPA's Background

The CCPA gives consumers the right to know what personal information a business collects about them and the purpose behind the collection.[86] Under the CCPA, controllers of data must notify consumers prior to or at the time of the collection what information will be collected and for what purpose.[87] After consumers are informed of the purpose and scope of collection and agree to participate, the CCPA gives consumers the right to compel deletion of the collected data.[88] Controllers are

79 Cal. CIV. CODE §§ 1798.100–.199.

80 *See id.* at § 1798.100(d)(1)–(4) Although the CCPA does not use the terms "processors" or "controllers" of data, the CCPA's differentiation between "third-party service providers" or "contractors" and "businesses that collect" personal information closely mirrors the differentiation between "processors" and "controllers" of data in some state and European regulations. Commission Regulation 2016/679, 2016 J.O. (L 119) 1 (EU) (repealing Directive 95/46/EC). These terms will be used for brevity.

81 *Difference Between Data Controller and Data Processor*, DATA PRIV. MANAGER (Aug. 4, 2020) [hereinafter *Controller & Processor*], https://dataprivacymanager.net/difference-between-data-controller-and-data-processor/ [https://perma.cc/6AWR-RNU6] (explaining the difference between controllers and processors of data as defined by the European Data Protection Regulation).

82 *Id.*

83 *Id.*

84 CAL. CIV. CODE § 1798.110.

85 *See infra* notes 86–101 and accompanying text.

86 CAL. CIV. CODE § 1798.110.

87 *Id.* § 1798.100(a)(1).

88 *Id.* § 1798.105.

thereafter responsible for deleting consumer data when requested.[89] When a consumer requests deletion, controllers are responsible for notifying processors to ensure the deletion on the processor's end is fully in compliance with the consumer request.[90]

In conjunction with the right to compel deletion of collected data, the CCPA provides consumers the right to opt out of sharing information and to limit the use and disclosure of personal information collected.[91] A consumer who opts out of sharing personal information is protected from retaliation by the business.[92] In other words, if a consumer opts out, the CCPA prohibits a business from using incentives to coerce consumers into disclosing personal information or otherwise inconveniencing the consumer's interaction with the business.[93]

ii. The CCPA Differentiation Between Controllers, and Processors

The CCPA differentiates between the duties of processors and the duties of the controllers of data.[94] Under the CCPA, controllers of data engaging with processors of data must enter into a specified agreement.[95] These agreements limit the liability of processors of data by requiring that controllers only disclose data to processors for a limited purpose and independently monitor the compliance of the processors.[96] Therefore, the responsibility of maintaining compliance and transparency of data retention and handling is the primary responsibility of controllers under the CCPA.[97] While controllers must present consumers with the retention plan, processors of data need only provide the purpose and scope of the collection in a clear notice on the homepage of their main website.[98] Further, processors of data have no duty to interact directly with

89 *Id.* § 1798.105(a)–(c).

90 *Id.*

91 *Id.* §§ 1798.120, 1798.135(a).

92 *Id.* § 1798.125(a)(1).

93 *Id.*

94 *See id.* § 1798.100(d)(1)–(4); *accord* VA. CODE ANN. § 59.1-579.

95 *See* CAL. CIV. CODE § 1798.100(d)(1)–(5) (providing businesses must only: (1) disclose consumers' personal information to third parties for a limited business purpose; (2) the third party must independently comply with the Act; (3) the business retains the right to ensure that the third-party service provider or contractor's use of the information is in compliance with the Act; (4) requires that the third party to disclose if compliance with the Act is breached; and (5) grants the business the right to take remedial action to correct misuse of information).

96 *Id.*

97 *See id.*

98 *Id.* § 1798.100(b).

consumers, even if consumers mistakenly send requests for deletion to processors instead of controllers of data.[99]

The CCPA acknowledges the reality and extent to which parties may handle or control data and offers much-needed privacy protections to consumers.[100] However, Part IV will discuss why, within employment, the roles and liability of processors and controllers of data should be clarified, and employees should be given greater control over their data.[101]

2. The Illinois Biometric Information Privacy Act

The BIPA regulates businesses collecting biometric data from consumers and employees.[102] While the BIPA presents useful protections, the legislation fails to differentiate between the relative bargaining power and privacy needs of consumers in comparison to employees.[103] This sub-part discusses the BIPA's application to businesses generally to provide background for the proposed federal privacy protection within employment.[104]

i. The BIPA's Informed Consent

The BIPA requires a business or an employer to receive a person's informed consent before collecting biometric data.[105] Informed consent means the employee is told their biometric data will be collected and asked to formally agree to this process, often by signing a written release.[106] If a consumer or an employee does not provide informed consent, the business is prohibited from collecting the subject's biometric data.[107] However, the reasons why withholding consent may not be feasible for an employee will be discussed further in Part IV.[108] Additionally, the BIPA requires that a person be notified in writing that biometric information is

99 *Id.* § 1798.105(c).

100 *Id.* § 1798.100(d)(1)–(5).

101 *Infra* Part IV.

102 740 ILL. COMP. STAT. § 14/15(a).

103 *Id.* § 14/15(b)(1–3). Requiring the same consent and written release from all data collection subjects (both consumers and employees) fails to acknowledge that employers may leverage an employee's job on their compliance with the data collection, and this pressure does not exist in the context of consumerism. *See id.* § 14/10.

104 *Infra* Part IV.

105 740 ILL. COMP. STAT. § 14/15(b) (stating an entity cannot collect—by any means—a person's biometric identifier unless it: (1) informs the subject in writing that the biometric information is being collected or stored; (2) informs the subject in writing of the specific purpose and length for which the biometric data will be collected, stored and used; and (3) receives a written release).

106 *Id.* § 14/10 ("Written release" means informed consent or, in the context of employment, a release executed by an employee as a condition of employment).

107 *See id.*

108 *See infra* Part IV.

being collected and of the purpose behind the collection.[109] However, under the BIPA, a business is not required to inform a person of the risks associated with biometric authentication or the underlying process.[110] The underlying process includes processors of data accessing the subject's biometrics.[111] This apparent oversight gives rise to claimants asserting procedural violations of the BIPA where a controller does not inform subjects that processors will handle their data.[112]

ii. The BIPA's Uniform Application

Under the BIPA, Illinois courts hold third parties handling data to the same compliance standards as the businesses collecting data, thereby making its application uniform across the parties involved.[113] Because plaintiffs may enforce the BIPA standards against the processors and the controllers of data, an increasing number of lawsuits have been brought under the BIPA in both the consumer and employment contexts.[114]

Many of the claims brought under the BIPA are procedural violations.[115] For instance, the BIPA requires private entities to develop a written retention policy, available to the public, for the destruction of biometric data held by the company.[116] Because the same requirements for handling biometric data may be enforced against both processors and controllers, there is potential for procedural violations where multiple parties handle the same data, but only one party makes a written retention policy available to the public.[117] This increased litigation confuses the roles

---

109 740 ILL. COMP. STAT. § 14/15(b).

110 *See id.*

111 *See* Smith v. Signature Sys., No. 2021-CV-02025, 2022 U.S. Dist. LEXIS 34383, at *2 (N.D. Ill. Feb. 28, 2022).

112 *See, e.g.*, Johnson v. NCR Corp., No. 22-C-3061, 2023 U.S. Dist. LEXIS 19327, at *7 (N.D. Ill. Feb. 6, 2023); *Smith*, 2022 U.S. Dist. LEXIS 34383, at *2–3.

113 *See, e.g.*, *Johnson*, 2023 U.S. Dist. LEXIS 19327, at *17; *Smith*, 2022 U.S. Dist. LEXIS 34383, at *12.

114 Blum, *supra* note 38 ("In 2019, there were 28 complaints filed in federal court over BIPA violations, but that number grew to 80 in 2020").

115 *See, e.g.*, Horn v. Method Prods., PBC, No. 21-C-5621, 2022 U.S. Dist. LEXIS 67354, at *1–2 (N.D. Ill. Apr. 12, 2022); *Smith*, 2022 U.S. Dist. LEXIS 34383, at *2–3; Fernandez v. Kerry, Inc., No. 17-C-8971, 2020 U.S. Dist. LEXIS 64070, at *1, *1–3 (N.D. Ill. Apr. 10, 2020); Bryant v. Compass Grp. USA, Inc., 958 F.3d 617, 619–20 (7th Cir. 2020); Fox v. Dakkota Integrated Sys. LLC, 980 F. 3d 1146, 1154–55 (7th Cir. 2020); *see also* DAVID OBERLY, BIOMETRIC DATA PRIVACY COMPLIANCE AND BEST PRACTICES § 2.05 (MB 2024).

116 740 ILL. COMP. STAT. § 14/15(a).

117 OBERLY, *supra* note 115, § 2.05[2] (describing a significant problem with the BIPA as the failure to define "collection" or "possession" of biometric data and the failure to delineate the related terms for compliance standards of controllers and processors).

of employers and third parties and creates unnecessary strain on the courts.[118]

The BIPA specifically addresses biometric data and protects both consumers and employees.[119] However, as a framework, the BIPA's provisions should be modified to clarify the role of third parties handling data and offer stronger privacy protections to employees.[120] Overall, current common law and statutes do not adequately address new privacy concerns associated with the collection of biometric data in the private-sector workplace.[121] While the repercussions of biometrics in the workplace will continue to unfold, action must be taken to educate employees of potential risks in surrendering their biometrics.[122]

IV. PROPOSAL

To fortify the privacy interests of employees, the common conception of these interests must recognize the relative inequality between employers and employees.[123] "Such an approach shifts the policy focus away from preventing invasions into various privacy interests towards the establishment and preservation of conditions that make the exercise of those interests possible."[124] By placing an emphasis on securing certain privacy interests of employees, employees' privacy interests will be less subject to change with technological advancements.[125] This Comment suggests a series of conditions for an employer's collection of biometric data that will work to create transparency and ensure the privacy interests of employees are protected: (1) employers should bear the brunt of liability regarding biometrics; (2) employers should be required to take defined steps to educate employees of the risks of biometric data collection; and (3) employers should be required to provide employees alternative means of authentication.[126]

---

118 *See id.*

119 *See* 740 ILL. COMP. STAT. § 14/15(b).

120 *Cf. infra* Part IV.

121 *See id.*

122 *See infra* Part IV.

123 *See* 740 ILL. COMP. STAT. § 14/10.

124 OTTO, *supra* note 6, at 185; Richard B. Bruyer, *Privacy: A Review and Critique of the Literature*, 43 ALTA. L. REV. 533, 558 (2006). Regarding the drive behind the publication of *The Right to Privacy*, "one can be sure that part of [Warren and Brandeis's] motivation was to ensure that privacy was seen as a free-standing right worthy of protection in its own right and not derivative of some other more recognizable cause action that required judges . . . to resort to legal fictions if predisposed to protect privacy." Bruyer, *supra*.

125 *See id.*

126 *Supra* Part III.A–B.

A. Compliance of Processors and Controllers Handling Data

Employers, acting as controllers of biometric data, must engage with both their employees and the processors of data.[127] This relationship places employers in the middle of employees and processors.[128] Neither the employees nor the processors have direct access to each other, but rather only have access to the employer-controllers of data.[129] As one court noted, "[i]f anything, the Illinois legislature's findings that '[t]he use of biometrics is growing' and '[t]he full ramifications of biometric technology are not fully known' reflect a recognition that multiple entities could control the same data."[130] Accordingly, regulation of biometrics within employment should recognize the interplay of entities handling data and their varying levels of accountability to employees.

Multiple entities controlling the same data does not make the storage of data any riskier.[131] By involving third party processors who are better equipped to secure biometric data, the databases are actually more likely to attain higher compliance standards.[132] However, because of the limited dealings of processors with the employees, processors should not be exposed to the same liability as that of the employer-controllers.[133] This reality of operations should be reflected in federal compliance standards for third parties.[134]

---

127 *See* Pato & Millett, *supra* note 18, at 20-1; *Biometric Authentication Software*, SOURCE FORGE, https://sourceforge.net/software/biometric-authentication/ (last visited Aug. 9, 2024); *Biometric Software Products and Solutions*, AWARE, https://www.aware.com/biometrics/ [https://perma.cc/6BL5-DNGV] (last visited Aug. 9, 2024).

128 *See* Smith v. Signature Sys., No. 2021-CV-02025, 2022 U.S. Dist. LEXIS 34383, at *2–3 (N.D. Ill. Feb. 28, 2022) (holding plaintiffs had standing to bring a procedural claim against Signature Systems, a producer of biometric-enabled systems, for handling their biometric data, although they had no direct contact with Signature Systems through their employer, Jimmy John's restaurant).

129 *See id.*

130 Heard v. Becton, Dickinson & Co. 440 F. Supp 3d 960, 965 (N.D. Ill. 2020) (alteration in original) (quoting 740 ILL. COMP. STAT. § 14/5(a) (2020)).

131 *See* Pato & Millett, *supra* note 18, at 20 ("[T]he ability to achieve the fingerprint scan's security objective depends not only on the biometric technology, but also on the robustness of the computing hard-ware to mechanical failures and on multiple decision by manufacturer[s] and employer[s] about when and how the biometric technology can be bypassed, which all together contribute to the systems context for the biometric technology."); *see also id.* at 25 (explaining that uploading biometric data to either network or local databases pose comparable privacy concerns).

132 *See* Pato & Millett, *supra* note 18, at 20 (explaining that the effectiveness of biometric technology is dependent on data management systems).

133 *See* CAL. CIV. CODE § 1798.100(d)(1)–(4).

134 *See, e.g.*, Johnson v. NCR Corp., No. 22-C-3061, 2023 U.S. Dist. LEXIS 19327, at *7 (N.D. Ill. Feb. 6, 2023) ("[C]ompliance . . . requirements may not be as straightforward for a third-party vendor . . . as it would be for a direct employer.").

Employers controlling the collection and handling of biometric data should bear the burden of properly vetting the third parties they contract with on behalf of their employees.[135] Federal regulation of biometric data should mirror the CCPA in terms of lowering the compliance threshold for third-party processors of biometric data.[136] Lowering compliance thresholds for processors of biometric data places increased accountability on employers controlling the data.[137] Because employees providing biometric data only have access to their employers, the employers should be responsible for making the use and disclosure of biometric data in the workplace clear to employees.[138] It should be sufficient that processors servicing biometrics follow the purpose and procedures for handling data outlined by the employers.[139] In essence, the burden should be on the employer to inform employees of retention policies regarding biometric data.[140]

Further, employers should be responsible for verifying the third party's compliance with reasonable security measures and care.[141] To effectively comply with these suggestions, employers should be competent enough in the processes of biometric-enabled systems to know where to look for compliance and be able to explain the processes and risks to employees.[142] Clarifying the role of processors of data will consequently clarify the duties of employers collecting biometric data from employees.[143]

B. Consent

What does consent mean in the employment context?[144] This sub-part seeks to point out the problems with giving the term consent legal

---

135 *Cf.* CAL. CIV. CODE § 1798.100(d)–(e) (requiring businesses collecting data must act reasonably to ensure a third party's compliance in handling the data and implementing security measures).

136 *See id.* at §§ 1798.100(b), 1798.105(c).

137 *See id.* at § 1798.100(d)(1)–(4).

138 Leddy, *supra* note 39.

139 *Cf.* CAL. CIV. CODE § 1798.100(b) (placing the liability of compliance in collecting data on employers would better incentivize employers to monitor processors of data and clarify employer's accountability to employees subject to data collection).

140 *See* Leddy, *supra* note 39.

141 *See* CAL. CIV. CODE § 1798.100(d)(3); *see also* VA. CODE ANN. § 59.1-578 (outlining the responsibilities of a "controller" of consumer data as distinct from a "processor" of consumer data).

142 *See* Leddy, *supra* note 39.

143 *See id.*

144 *See* Niezna & Davidov, *supra* note 3, at 1134–35, 1141; Steven L. Willborn, *Notice, Consent, and Nonconsent: Employee Privacy in the Restatement,* 100 CORNELL L. REV. 1423, 1439 (2014).

significance in the employment context and offers suggestions that may better serve the privacy interests of employees.[145]

The employer-employee relationship is inherently susceptible to coercion because of employees' economic reliance on their jobs.[146] The BIPA includes a provision requiring businesses to receive a signed waiver before collecting a person's biometric data.[147] Similarly, the CCPA includes an opportunity for consumers to opt-out of surrendering their personal information.[148] However, both methods have pitfalls in the employment context.[149] Consent can easily be obtained by employers implicitly or explicitly conditioning an employee's job on receipt of the waiver.[150] Similarly, an employee will have a difficult time opting-out of surrendering their personal information to their employer.[151]

A combination of the methods presented in the BIPA and the CCPA would likely be most effective to increase the chances that an employee will be informed before providing consent.[152] Employers collecting biometrics should: (1) provide employees time to review biometric collection processes; (2) educate employees about risks before receiving informed consent from employees; and (3) provide alternatives to biometric authentication.[153]

1. Time to Review

In most cases, employees register their biometric data on company databases during onboarding.[154] Employees are likely overwhelmed with

---

145 *See infra* notes 146–153 and accompanying text.

146 Niezna & Davidov, *supra* note 3, at 1134, 1141–42; Willborn, *supra* note 144, at 1432.

147 *See* 740 ILL. COMP. STAT. § 14/15(b) (stating an entity cannot collect (by any means), a person's biometric identifier unless it (1) informs the subject in writing that the biometric information is being collected or stored, (2) informs the subject in writing of the specific purpose and length for which the biometric data will be collected, stored and used, and (3) receives a written release).

148 *See* CAL. CIV. CODE § 1798.120.

149 *Cf.* Niezna & Davidov, *supra* note 3, at 1134, 1141–42 (delineating the balance between "free consent" and coercion in the context of employment).

150 *Id.* at 1144; OTTO, *supra* note 6, at 182 ("The economic and social value of work induces a unique dependence asymmetry between the contracting parties of the employment relationship, which in turn, has a bearing on employees' exercise of privacy claims."); *see* Willborn, *supra* note 144, at 1428–29.

151 *See id.*

152 *Cf.* Niezna & Davidov, *supra* note 3, at 1144 (suggesting a combination of procedural mechanisms "increase[] the chances that consent is informed").

153 *See supra* notes 146–52 and accompanying text.

154 *See, e.g.*, Figueroa v. Kronos Inc., 454 F. Supp. 3d 772, 779 (N.D. Ill. 2020) ("When beginning work for an employer that uses a . . . biometric timekeeping device, an employee must have her fingerprint or palm print scanned to enroll in the . . . database.").

new people, processes, tasks, and paperwork when beginning a new job and lack adequate time to consider problems with agreeing to participate in biometric authentication.[155] Employers should be required to give "cooling off" or "reflection periods" where an employee has a set period to consider registering their biometric data on company databases before committing to doing so.[156] This approach would increase the likelihood that employees are given the opportunity to provide informed consent before agreeing to participate.[157]

2. Informed Consent and Waiver

Employers should be required to obtain an employee's informed consent and signed waiver to collect their biometric data, as required under the BIPA.[158] Further, the written waiver should contain simple sentence structure and avoid legalese or complex words because the biometric jargon in the industry is convoluted.[159] Most employees are unlikely to understand or consider the risks of providing biometric identifiers to their employers.[160] Companies should have a designated person, such as a human resources representative, who can educate new employees about the process and associated risks of providing biometric data.[161] The information provided by a human resources representative should address long-term impacts that would result from a breach of biometric data.[162] Having a company representative available to walk employees through potential risks associated with biometric authentication will mitigate the chances of employees being ignorant of these dangers before enrolling.[163]

---

155 *See* Niezna & Davidov, *supra* note 3, at 1145–46.

156 *See id.*

157 *See id.*

158 *See* 740 ILL. COMP. STAT. § 14/15(a) (stating an entity cannot collect (by any means), a person's biometric identifier unless it (1) informs the subject in writing that the biometric information is being collected or stored, (2) informs the subject in writing of the specific purpose and length for which the biometric data will be collected, stored and used, and (3) receives a written release).

159 Niezna & Davidov, *supra* note 3, at 1144; *see* MITRA, WEN & GOFMAN, *supra* note 14, at 5–6.

160 *See* 740 ILL. COMP. STAT. § 14/5(f).

161 *See* Niezna & Davidov, *supra* note 3, at 1145 ("Another variation . . . would require a certain number of days between a request made by the employer to introduce a new term and the time an employee needs to reply; or some days between the time the employee received expert advice and the time they need to make a decision. During this time, the employee can presumably consult with additional people or just have more time to think about the agreement.").

162 *See id.* at 1146 ("If consent is sought in concrete terms close to the date it becomes relevant, that would significantly increase the likelihood that the employee understands the consequences of consenting.").

163 *See id.*

3. Mandatory Alternatives

Federal regulation of private sector employers' collection of biometric data should require employers to provide alternatives for an employee who is asked to surrender biometric data.[164] The need for alternatives has been addressed by some courts under Title VII.[165] In *United States Equal Employment Opportunity Commission v. Consol Energy, Inc.*, Consolidated Coal transitioned its timecard system to require that employees use biometric-enabled timecards.[166] An employee, Butcher, protested the transition claiming that participation in the biometric-enabled timecard violated his sincerely held religious beliefs.[167] Due to his religious stance as a practicing evangelical Christian, Butcher refused to enroll in the system fearing that a scan of his hand would link him to the Antichrist.[168] After Consol Energy declined to accommodate Butcher's demand for an alternative, he sued and recovered under Title VII in the United States Court of Appeals for the Fourth Circuit.[169]

In addition to religious reasons, the law must acknowledge the many reasons employees may opt-out of the collection of their biometric data.[170] Examples of other reasons include physical deformities that complicate the collection process.[171] Because of the intricacy of fingerprints, low-quality images can create problems for matching.[172] Further, fingerprint readers are prone to technical issues that are exaggerated by natural changes in the appearance of the skin.[173] In *Consol Energy*, at the same time Butcher protested enrollment into the biometric-enabled timecard, the company was already forced to offer alternative means of time entry for

---

164 *See* Leddy, *supra* note 39.

165 *See* U.S. Equal Emp. Opportunity Comm'n v. Consol Energy, Inc., 860 F.3d 131, 142–43 (4th Cir. 2017) (holding where an employee can demonstrate use of a biometric-enabled timecard violated his sincerely held religious beliefs, an employer must provide alternate means for the employee to log his time.); *see also* Press Release, U.S. Equal Emp. Opportunity Comm'n, Court Awards Over Half Million Dollars Against Consol Energy/Consolidation Coal in EEOC Religious Discrimination Lawsuit (Aug. 27, 2015), https://www.eeoc.gov/newsroom/court-awards-over-half-million-dollars-against-consol-energyconsolidation-coal-eeoc [https://perma.cc/N9YX-MV3A].

166 860 F.3d at 136.

167 *Id.* at 137.

168 *Id.* Butcher claimed enrollment on the database correlated to the biblical "Mark of the Beast," prophesied of in the Book of Revelation. *Id.* The Mark of the Beast is a mark said to be imprinted on the followers of the Antichrist, thereby making these individuals susceptible to manipulation by the devil. *Id.* at 138–39.

169 *Id.* at 151–52.

170 *See* Leddy, *supra* note 39.

171 *Id.*; *see Consol Energy, Inc.,* 860 F.3d at 138 ("[T]wo employees with hand injuries . . . could not be enrolled through a scan of either hand"); MITRA, WEN & GOFMAN, *supra* note 14, at 10.

172 MITRA, WEN & GOFMAN, *supra* note 14, at 10.

173 *Id.*; Pato & Millett, *supra* note 18, at 26–27.

two employees with hand injuries.[174] Because of the hand injuries, the employees could not be enrolled in the system through a scan of either hand.[175] Instead, the company allowed these employees to enter their personnel numbers on a keypad.[176]

Implementing alternative means of authentication will likely create no added costs for employers in most cases.[177] In *Consol Energy*, the company's own trial witness testified that allowing employees to enter numbers on a keypad, instead of using the biometric-enabled timecard, posed no additional cost or burden on the company.[178] Alternatives might look like entering numbers on a keypad as suggested in *Consol Energy*, scanning a keycard, or using login credentials in place of biometric identifiers.[179] While alternative forms of employee authentication may create the potential for a breach or additional costs, a keycard is replaced or a password is reissued much more simply than a fingerprint, a face, or a voice.[180] Although it is likely that providing mandatory alternatives would pose no additional costs, even if it did, employers should be aware of the risks of biometric data and bear the cost of employees choosing not to place their innate traits in the hands of employers.[181]

In conjunction with alternatives, an anti-retaliation provision—i.e., a provision that prohibits incentives or consequences for offering, or the refusal to offer, biometric data—should be incorporated into federal regulation of biometric data in employment.[182] Under the CCPA, businesses may not use incentives to coerce consumers into providing their personal information or to inconvenience their interaction with the business.[183] Retaliation would likely be amplified in the workplace, particularly where an employee's choice to use alternatives creates added procedures or otherwise inconvenience a supervisor.[184] Accordingly,

174 *Consol Energy, Inc.*, 860 F.3d at 138.

175 *Id.* at 138–39.

176 *Id.*

177 *See, e.g.*, *id.* at 138–39 ("[E]mployees . . . could . . . instead . . . enter their personnel numbers on a keypad attached to the system. According to Consol's own trial witness, this accommodation imposed no additional cost or burden on the company.").

178 *Id.*

179 *See id.*

180 Miller, *supra* note 15; Schneier, *supra* note 49; Simons, *supra* note 1, at 1098; *See* SPECOPS, *supra* note 36.

181 *See Consol Energy, Inc.*, 860 F.3d at 138.

182 *See* Brian A. Riddell & Richard A. Bales, *Adverse Employment Action in Retaliation Cases*, 34 U. BALT. L. REV. 313, 315 (2005).

183 CAL. CIV. CODE § 1798.125(a)(4).

184 *See, e.g.*, *Consol Energy, Inc.*, 860 F.3d at 139 ("Consol continued to resist making the same accommodation for Butcher . . . The disparity in treatment was highlighted by a single email . . . authorizing the keypad accommodation for . . . two employees with physical injuries and denying that accommodation to Butcher: '[L]et's make our religious objector use his left hand.'" (alteration in original)).

employees choosing to use alternatives should be provided security so that their general job functions and environment will not be adversely impacted as a result.[185] While the employee-plaintiff bears the burden of persuasion in a retaliation claim, at minimum employees should be provided the opportunity to opt-out of biometric authentication without the risk of employer retaliation.[186]

Ensuring privacy rights amid increasing technology will require a conceptual shift in the affirmative rights of employees.[187] Creating conditions that recognize the realities surrounding the implementation of biometric-enabled systems will increase the transparency and responsibility of employers choosing to collect biometric data from employees. Additionally, creating conditions for an employer's collection of biometric data could work to minimize the inherent pressures that may undercut an employees' opportunity to provide informed consent.[188]

V. CONCLUSION

Biometric authentication will likely continue to surge in popularity in the coming years because biometric-enabled software provides superior efficiency and security to businesses.[189] Illinois and California are among the few states that have acknowledged the need for greater biometric data privacy protections with new technology.[190] Because of the risks inherent to biometric authentication, there should be a federal standard of protection for employees presented with the opportunity to participate in biometric authentication.[191] Developments in technology demand that federal protection balance the practical and economic interests of employers against the privacy interests of employees.[192] Overall, there should be federal regulation of employers' collection of biometrics that increases transparency of biometric data retention, informs employees of potential risks before enrolling in the database, provides time for consideration, and offers alternatives.[193]

---

185 *See id.*; *cf.* CAL. CIV. CODE § 1798.125 (requiring a business may not retaliate against a consumer who chooses to opt out of sharing personal data).

186 *See* Riddell & Bales, *supra* note 182, at 315.

187 *See* OTTO, *supra* note 6, at 185.

188 *See Consol Energy, Inc.*, 860 F.3d at 138.

189 *See* Robb, *supra* note 3.

190 CAL. CIV. CODE §§ 1798.100–.199; 740 ILL. COMP. STAT. §§ 14/1–/99.

191 *See* OTTO, *supra* note 6, at 185.

192 *Supra* Part IV.

193 *See id.*