Hofstra Labor & Employment Law Journal

Volume 39 | Issue 1 Article 5

9-1-2021

# Who's Checking? A Proposal to Protect Employee Health Screening Data

Andrew Schuman
*Maurice A. Deane School of Law at Hofstra University*

# WHO'S CHECKING? A PROPOSAL TO PROTECT EMPLOYEE HEALTH SCREENING DATA

## INTRODUCTION

Bob Grewal, the owner of a Subway restaurant in Los Angeles, steps inside his establishment's employee food prep area.[1] He is quickly recognized by a camera and its corresponding tablet, PopID.[2] Not only did PopID have the ability to recognize his face, but it was also able to detect Bob's temperature, deeming him safe to enter the workplace.[3] Bob implemented PopID in his restaurant for this purpose, as many employers have done in an effort to promote safety.[4]

The COVID-19 pandemic has radically changed the American workplace since April of 2020.[5] In an effort to promote the health and safety of employees, a significant portion of the workforce has temporarily transitioned to a remote style of work.[6] While companies start to return their employees to the workplace, employers have begun to take measures promoting a more socially distant and sanitized workplace.[7] They have also started to institute various forms of employee health screenings.[8] One such method is checking the temperature of employees to identify a fever or elevated temperature.[9]

---

1. Natasha Singer, *Employers Rush to Adopt Virus Screening. The Tools May Not Help Much.*, N.Y. TIMES, https://www.nytimes.com/2020/05/11/technology/coronavirus-worker-testing-privacy.html (May 14, 2020).

2. *Id.*

3. *See id.*

4. *Id.*

5. Erik Brynjolfsson et al., *COVID-19 and Remote Work: An Early Look at US Data* 2 (Nat'l Bureau of Econ. Rsch., Working Paper No. 27344, 2020), https://www.nber.org/system/files/working_papers/w27344/w27344.pdf.

6. *See id.* at 3, 24.

7. *See* Sara Aridi, *How to Prepare for Your Return to the Office*, N.Y. TIMES, https://www.nytimes.com/2020/08/08/at-home/office-return-coronavirus.html (Oct. 26, 2020) (discussing businesses rearranging seats to ensure social distancing and setting up sanitizer dispensers at building entry points).

8. *See id.* ("C.D.C. suggests employees fill out daily health surveys and disclose whether they have COVID-19 symptoms before coming into work.").

9. *See id.*

Temperature checks have been touted by government officials as necessary measures going hand in hand with testing regiments,[10] and as a "new normal," to become ingrained in the standard operating procedure of the workplace.[11] Temperature checks are becoming so ubiquitous that a new position has sprung out of the need for establishments to screen anyone from employees to visitors alike.[12]

However, when health information is being recorded, privacy concerns begin to arise.[13] For example, workers at some grocery stores feared that the information collected during their temperature check was being used against them.[14] In addition to the facial issue of being able to monitor an employee's health through their temperature, there may be broad implications of surveillance, as temperature data can also be used to infer stress, heart conditions, pregnancy, and other diseases.[15] There are privacy concerns regarding the normalization of physiological surveillance to the extent that said surveillance continues in a post-COVID-19 world.[16] There is also the unsettling reality that some technologies used to detect temperature are able to collect other kinds of personalized data.[17] It is possible that the collection of health information

10. Julia Marsh, *Workplace Temperature Checks will be Key After Coronavirus Crisis, de Blasio Says*, N.Y. POST (Apr. 20, 2020, 8:36 AM), https://nypost.com/2020/04/20/temperature-checks-may-come-to-nyc-offices-after-coronavirus/.

11. Eyewitness News, *Reopening NY: Cuomo Lets Workplaces Conduct Temperature Checks*, ABC7 N.Y. (June 6, 2020), https://abc7ny.com/ny-workplace-temperature-checks-reopen-new-york-nyc-coronavirus/6234972/.

12. *See* Jane Wells, *The Coronavirus Pandemic Has Created a New Job: Temperature Taker*, CNBC (June 5, 2020, 3:45 PM), https://www.cnbc.com/2020/06/05/the-coronavirus-pandemic-has-created-a-new-job-temperature-taker.html; Anya Sostek, *COVID-19 Creates a New Job: Temperature Taker*, PITTSBURGH POST-GAZETTE (Sept. 6, 2020, 6:45 AM), https://www.post-gazette.com/news/health/2020/09/06/COVID-19-new-job-temperature-taker-Baptist-Homes-in-Mt-Lebanon/stories/202009030088.

13. *See* Erin Mulvaney, *Worker Safety, Privacy Clash as Temperature Checks Become Norm*, BLOOMBERG L. (May 29, 2020 5:40 AM), https://news.bloomberglaw.com/daily-labor-report/worker-safety-privacy-clash-as-temperature-checks-become-norm (discussing privacy concerns and the confidentiality of employee records resulting from temperature checks).

14. *Id.*; *see also* Brianna Sacks, *Harris Teeter Won't Tell Employees What Their Temperature is During New Health Screenings*, BUZZFEED NEWS, https://www.buzzfeednews.com/article/briannasacks/grocery-workers-coronavirus-temperature-checks (May 19, 2020 1:15 PM).

15. Mulvaney, *supra* note 13.

16. JAY STANLEY, ACLU, TEMPERATURE SCREENING AND CIVIL LIBERTIES DURING AN EPIDEMIC 5 (2020), https://www.aclu.org/sites/default/files/field_document/aclu_white_paper_-_temperature_checks.pdf.

17. *See* TAURI, https://www.gotauri.com/ (Oct. 13, 2020) (advertising optional facial recognition and the ability to store 5,000 face recognitions on all tablets) [https://perma.cc/3XAF-CAWB]; *PAR-P2TEMPTABLET: 2MP HD Temperature Measurement & Face Recognition Terminal*, INVID TECH, https://invidtech.com/products/par-p2temptablet-2mp-hd-temperature-

does not stop with temperature.[18] If our society accepts the collection of temperature data in the name of curbing the threat posed by COVID-19, more invasive tests that may promise better results, such as the measurement of blood oxygenation, could become normalized by the same rationale.[19]

Americans are increasingly concerned about unprotected health data.[20] CynergisTek, a cybersecurity firm which services the healthcare industry and concentrates primarily on privacy and security issues, recently conducted a survey of over 5,000 U.S. adults.[21] Seventy percent of respondents said they would likely sever healthcare provider ties if they found that their personal health data was not being properly protected.[22] The responses in that survey also indicated that forty-five percent of Americans expressed concerns about wanting to keep their personal health information private from their employer.[23] In addition, nearly sixty percent of respondents expressed anxiety related to the disclosure of data, namely, that their employer may share personal data without their consent.[24]

This note will show that there exists a gap in the law that leaves data unprotected if it is collected during employee health screenings.[25] Employers that conduct temperature checks in their role as an employer do not have to abide by the regulations promulgated in the Health Insurance Portability and Accountability Act (hereinafter "HIPAA") for protecting Protected Health Information[26] (hereinafter "PHI") of their employees.[27] Due to the limited number of states that have enacted biometric data privacy statutes,[28] and the limited language of those

---

measurement-face-recognition-terminal (last visited Sept. 18, 2020) (advertising "highly accurate face recognition using deep learning algorithm" with a capacity to hold 20,000 faces).

18. *See* STANLEY, *supra* note 16, at 5.

19. *See id.*; *see also* VITACORPO, https://vitacorpo.com (last visited Oct. 24, 2020) (advertising the ability to track various testing and vaccination processes through software).

20. *See Survey Says: Patients and Employees Agree – No Privacy, No Go*, CYNERGISTEK (Sept. 24, 2020), https://cynergistek.com/news/survey-says-patients-and-employees-agree-no-privacy-no-go/.

21. *Id.*

22. *Id.*

23. *Id.*

24. *Id.*

25. *See infra* Section I.D.

26. 45 C.F.R § 160.103 (2021).

27. *See* Practical Law Employee Benefits & Executive Compensation, *COVID-19 Compliance for Health and Welfare Plans*, WESTLAW, https://us.practicallaw.thomsonreuters.com/w-025-1497?documentSection=co_anchor_a658135 (last visited Sept. 19, 2020).

28. *See infra* Section II.B.

statutes,[29] existing state laws may not provide adequate protections either. This note's proposed solution to this need for protection is for states to add or modify existing data privacy laws with the intent to provide protection for data collected during employee health screenings.[30] Section I of this note will provide background information on historical constitutional rights of privacy, and guidance issued by various federal, state, and local government entities with respect to temperature checks.[31] Section II will analyze various existing state biometric data privacy laws, how courts have considered privacy rights in light of these laws, and how products on the market today have application to these laws.[32] Section III proposes a model for states to adopt in order to ensure that employee data is protected.[33] Finally, Section IV will conclude with a discussion on the importance of privacy and how the law must keep pace with new technologies and new practices that may come as a result.[34]

## I. BACKGROUND

Historically, the law has established a right to privacy that extends to situations involving employees and testing their health.[35] In light of these privacy considerations, the recommendations, guidelines, and regulations promulgated by various bodies in government during the pandemic ought to be viewed through the lens of privacy rights they might implicate.[36] Agencies of the federal government have set forth guidelines with respect to how an employer should operate reopening their business with instituted health screening.[37] States have also issued orders and regulations that set standards for what type(s) of screening should be recommended or required.[38] Certain localities have instituted their own guidelines, usually building on the state's guidelines and requiring a heightened standard of screening.[39] Given the matter's nature of privacy with respect to health issues, intuitively, HIPAA could be the law to

29. *See infra* Section II.B.
30. *See infra* Section III.A.
31. *See infra* Section I.
32. *See infra* Section II.
33. *See infra* Section III.
34. *See infra* Section IV.
35. *See infra* Section I.A.
36. *See infra* Section II.
37. *See infra* Section I.B.
38. *See infra* Section I.C.
39. *See infra* Section I.C.

consult. Yet, a closer reading of the statute's text shows it is not tailored to protect data obtained during employee health screenings.[40]

### *A. Privacy as a Fundamental Right*

A right to privacy in the workplace has long been recognized by the Supreme Court, having roots in Fourth Amendment protections against unreasonable search and seizures.[41] In 1987, the Supreme Court decided *O'Connor v. Ortega*, a case in which Dr. Magno Ortega sued the executive director of his hospital, claiming that the hospital's search of Dr. Ortega's office violated the Fourth Amendment.[42] Prior to *O'Connor*, Fourth Amendment protections had only gone so far as applying to the conduct of governmental officials.[43] Justice O'Connor linked the expectation of privacy to constitutional jurisprudence, stating "searches and seizures by government employers or supervisors of the private property of their employees, therefore, are subject to the restraints of the Fourth Amendment."[44] The Court in *O'Connor* reasoned that Dr. Ortega had a reasonable expectation of privacy in his own office.[45] Although the Court in *O'Connor* remanded the case to the District Court to find if there were work-related reasons to search Dr. Ortega's office,[46] Justice O'Connor found that Dr. Ortega had an expectation of privacy for materials kept in his desk and file cabinets.[47] Justice O'Connor included medical files in an enumerated list of such private materials.[48] This would indicate the recognition of medical information as worthy of protection under the law.[49]

However, courts have not held that a right to privacy is absolute,[50] especially in the face of government interest. Just two years after

40. *See infra* Section I-d.

41. *See* O'Connor v. Ortega, 480 U.S. 709, 716 (1987).

42. *Id.* at 714.

43. *See, e.g.*, New Jersey v. T.L.O., 469 U.S. 325, 334-35 (1985).

44. *O'Connor*, 480 U.S. at 715.

45. *Id.* at 718.

46. *Id.* at 732.

47. *Id.* at 718.

48. *Id.*

49. *See generally id.* (concluding that there is a reasonable expectation of privacy in a personal desk and file cabinets containing medical files).

50. *See, e.g.*, Van Patten v. State 359 P.3d 469 (Or. App. 2015). Oregon state employees of the Public Employees' Benefit Board were required to fill out "health risk assessment" questionnaires to obtain state subsidized health insurance. *Id.* On the question of Fourth Amendment concerns, the court stated, "In short, at least for now, there is no such thing as a Fourth Amendment right to be free from intrusive questioning, and plaintiffs provide no reason why this court should be the first to find one." *Id.* at 476.

*O'Connor*, the Supreme Court upheld a federal regulation that required railroad workers to undergo blood and urine tests as a safety standard.[51] In *Skinner*, the Court held that there was an important governmental interest furthered by the intrusion of privacy.[52] The Court also mentions a level of individualized suspicion, which is required to make a search reasonable, absent an important governmental interest.[53] This level of individualized suspicion is not met when the need for the intrusion of privacy is "symbolic, not 'special.'"[54] In *Chandler*, the Supreme Court held that the Fourth Amendment precluded a Georgia law that required candidates running for Georgia state office to submit to a drug test.[55] Unlike the regulations in *Skinner* and *Von Raab*, the tests in *Chandler* did not require any suspicion, nor was there pre-existing evidence of a drug usage problem with Georgia state officeholders.[56] The Court noted that there was no concrete danger or real hazards justifying the statute.[57] The Court held that the Fourth Amendment prevents the state from "diminish[ing] personal privacy for a symbol's sake."[58] These Fourth Amendment concerns could be implicated with temperature checks today, if they are invading employees' privacy while proving more useful for alleviating anxiety in the workplace than actually detecting COVID-19.[59]

### *B. Federal Guidelines*

The Centers for Disease Control and Prevention (hereinafter "CDC") is a federal agency operating under the Department of Health and Human Services.[60] The CDC works to fight the spread of disease by conducting critical science and providing health information.[61] The CDC has maintained a crucial role in the monitoring and preventing of COVID-19

51. *See* Skinner v. Ry. Lab. Execs.' Ass'n, 489 U.S. 602, 609 (1989).

52. *Id.* at 624.

53. *See id.*; *see also* Nat'l Treasury Emps. Union v. Von Raab, 489 U.S. 656 (1989) (holding that the government's need to conduct searches outweighs the privacy of the employees of the United States Customs Service that were required to complete drug tests upon being promoted to positions involving drug interdiction).

54. Chandler v. Miller, 520 U.S. 305, 322 (1997).

55. *Id.* at 309.

56. *Id.* at 319.

57. *Id.*

58. *Id.* at 322.

59. *See infra* Section II.A.

60. *About CDC 24-7*, CTRS. FOR DISEASE CONTROL & PREVENTION, https://www.cdc.gov/about/organization/cio.htm (May 2, 2021).

61. *Id.*

since the virus' arrival in the United States in January of 2020.[62] Since the COVID-19 pandemic has been underway in the United States, employers have been looking to the CDC for guidance on standards to abide by when reopening their workplaces.[63] The organization has issued guidelines outlining how businesses and employers can go about allowing workers to return, while implementing appropriate safety measures.[64]

In addition to encouraging sick employees to stay home,[65] the CDC recommends that businesses consider conducting daily in-person or virtual health checks such as symptom or temperature screening.[66] While this is obviously a departure from the norm, the CDC recognizes that privacy still ought to be valued when conducting these health checks.[67] With respect to confidentiality, the CDC recommends following Equal Employment Opportunity Commission (hereinafter "EEOC") guidance.[68]

When asked about specifically screening for COVID-19 symptoms via temperature checks, the CDC acknowledged the limitations of doing so.[69] Since individuals may be asymptomatic or may exhibit mild non-specific symptoms, it is possible that an infected person passes the screening.[70] With that in mind, the CDC reiterates that "screening and health checks are not a replacement for other protective measures such as social distancing."[71] Alternatively, a visual inspection may be performed or employees can take their own temperature before coming to work.[72]

---

62. *See First Travel-related Case of 2019 Novel Coronavirus Detected in United States*, CTRS. FOR DISEASE CONTROL & PREVENTION (Jan. 21, 2020), https://www.cdc.gov/media/releases/2020/p0121-novel-coronavirus-travel-case.html; *see also 2020 News Releases*, CTRS. FOR DISEASE CONTROL & PREVENTION, https://www.cdc.gov/media/releases/2020/archives.html (Oct. 15, 2019).

63. *See* Kevin Freking and Mike Stobbe, *CDC Compiles New Guidelines to Help Organizations Reopen*, ABC NEWS (Apr. 28, 2020 10:30 AM), https://abcnews.go.com/Health/wireStory/cdc-compiles-guidelines-organizations-reopen-70377133.

64. *See Guidance for Businesses and Employers Responding to Coronavirus Disease 2019 (COVID-19)*, CTRS. FOR DISEASE CONTROL & PREVENTION, https://www.cdc.gov/coronavirus/2019-ncov/community/guidance-business-response.html (Mar. 8, 2021).

65. *See* U.S. DEP'T OF LAB., OCCUPATIONAL SAFETY & HEALTH ADMIN., GUIDANCE ON PREPARING WORKPLACES FOR COVID-19 8 (2020), https://www.osha.gov/Publications/OSHA3990.pdf.

66. CTRS. FOR DISEASE CONTROL & PREVENTION, *supra* note 64.

67. *Id.* "To prevent stigma and discrimination in the workplace, make employee health screenings as private as possible." *Id.*

68. *Id.*; *see infra* Section I.B.1.

69. *See General Business Frequently Asked Questions*, CTRS. FOR DISEASE CONTROL & PREVENTION, https://www.cdc.gov/coronavirus/2019-ncov/community/general-business-faq.html (May 24, 2021).

70. *Id.*

71. *Id.*

72. *Id.*

The CDC also refers to the Occupational Safety and Health Administration's (hereinafter "OSHA") Guidance on Mitigating and Preventing the Spread of COVID-19 in the Workplace.[73] OSHA is an agency under the United States Department of Labor, dedicated to "ensur[ing] safe and healthful working conditions for workers by setting and enforcing standards and by providing training, outreach, education and assistance."[74] OSHA's guidance was originally non-specific, providing that employers promptly identify and isolate potentially infectious individuals to prevent the unnecessary spread of the pandemic.[75] As a result, OSHA came under criticism for their lack of issuing temporary emergency standards to deal with the pandemic.[76] Although they have been criticized, President Biden and his administration asked OSHA to pursue a new course of action, this time mandating certain health standards, rather than just advising.[77] In June of 2021, OSHA finally issued an Emergency Temporary Standard in the form of regulations which only apply to workplaces where employees provide healthcare services or healthcare support services.[78]

1. Equal Opportunity Employment Commission (EEOC)

The EEOC was created under Title VII of the Civil Rights Act of 1964, for the purpose of interpreting the Act.[79] The EEOC is responsible for enforcing federal discrimination laws relating to employees and job applicants.[80] The Commission investigates complaints filed with it and assures compliance with its own regulations.[81] As the pandemic has given rise to workplace discrimination[82] and adherence to EEO laws take on a

73. *See* CTRS. FOR DISEASE CONTROL & PREVENTION, *supra* note 64.

74. *About OSHA*, U.S. DEP'T OF LAB., https://www.osha.gov/aboutosha (last visited Sept. 19, 2020).

75. *See* U.S. DEP'T OF LAB., OCCUPATIONAL SAFETY & HEALTH ADMIN., *supra* note 65, at 9.

76. *See* Dave Jamieson, *How OSHA Failed its Biggest Test Ever With COVID-19*, HUFFPOST (Sept. 17, 2020, 11:03 AM), https://www.huffpost.com/entry/osha-failing-biggest-test-50-year-history_n_5f6257dec5b6ba9eb6e8ae0d.

77. *See* Sarah Chaney Cambon, *Biden Moves to Set Covid-19 Workplace-Safety Rules*, WALL ST. J. (Jan. 21, 2021, 1:14 PM), https://www.wsj.com/articles/biden-moves-to-set-covid-19-workplace-safety-rules-11611252898.

78. 29 C.F.R. § 1910.502(a)(1) (2021).

79. *See* JOSEPH A. SEINER, EMPLOYMENT DISCRIMINATION: PROCEDURE, PRINCIPLES, AND PRACTICE 8 (Rachel E. Barkow et al. eds., 2d ed. 2019).

80. *See Overview*, U.S. EQUAL EMP. OPPORTUNITY COMM'N, https://www.eeoc.gov/overview (last visited Sept. 19, 2020).

81. *See id.*

82. *See generally Message From EEOC Chair Janet Dhillon on National Origin and Race Discrimination During the COVID-19 Outbreak*, U.S. EQUAL EMP. OPPORTUNITY COMM'N, https://

new form, the EEOC has issued advice on how traditional EEOC situations such as layoffs, harassment, and reasonable accommodations are applied in the context of COVID-19.[83] The EEOC has recently published their variation on guidance for temperature checks to be administered in the workplace.[84]

The EEOC's Pandemic Preparedness guidance document was originally issued in 2009, in response to the H1N1[85] virus outbreak.[86] Over a one year period, the H1N1 virus was responsible for over 12,000 deaths in the United States,[87] a number almost thirty-four times less than the number of deaths caused by COVID-19 in the United States in one year since the CDC's first confirmed case.[88] Yet, even back then, the EEOC accounted for situations that have become universal today, such as telework, health screenings, and "infection-control" practices.[89] The EEOC's original guidance on the H1N1 pandemic called for temperature checks if conditions worsened from the state of the pandemic in the spring and summer of 2009, or if the CDC or state and local health authorities determined the pandemic to be widespread.[90] When updated to meet COVID-19 concerns, the EEOC affirmatively stated "employers may measure employees' body temperature."[91] The Commission goes even further and allows employers to institute post-offer, pre-employment temperature checks as part of a medical exam.[92]

---

www.eeoc.gov/wysk/message-eeoc-chair-janet-dhillon-national-origin-and-race-discrimination-during-covid-19 (last visited Jan. 24, 2021) (discussing that during COVID-19 there has been an increase in reports of harassment of Asian Americans and the importance of anti-discrimination laws at this time).

83. *See What You Should Know About COVID-19 and the ADA, the Rehabilitation Act, and Other EEO Laws*, U.S. EQUAL EMP. OPPORTUNITY COMM'N, https://www.eeoc.gov/wysk/what-you-should-know-about-covid-19-and-ada-rehabilitation-act-and-other-eeo-laws (Oct. 13, 2021).

84. *See Pandemic Preparedness in the Workplace and the Americans with Disabilities Act*, U.S. EQUAL EMP. OPPORTUNITY COMM'N (Oct. 9, 2009) https://www.eeoc.gov/laws/guidance/pandemic-preparedness-workplace-and-americans-disabilities-act#q7.

85. *See The 2009 H1N1 Pandemic: Summary Highlights, April 2009-April 2010*, CTRS. FOR DISEASE CONTROL & PREVENTION (June 16, 2010), https://www.cdc.gov/h1n1flu/cdcresponse.htm. First detected in America in April of 2009, H1N1, more commonly known as "swine flu" was a combination of influenza viruses never before seen in humans or animals. *Id.*

86. U.S. EQUAL EMP. OPPORTUNITY COMM'N, *supra* note 83.

87. *2009 H1N1 Pandemic (H1N1pdm09 virus)*, CTRS. FOR DISEASE CONTROL & PREVENTION, https://www.cdc.gov/flu/pandemic-resources/2009-h1n1-pandemic.html (June 11, 2019).

88. *See Mortality Analyses*, JOHNS HOPKINS UNIV., CORONAVIRUS RES. CTR. (Jan. 21, 2021), https://coronavirus.jhu.edu/data/mortality [https://web.archive.org/web/20210121163824/https://coronavirus.jhu.edu/data/mortality].

89. *See* U.S. EQUAL EMP. OPPORTUNITY COMM'N, *supra* note 83.

90. *See id.*

91. *Id.*

92. *Id.*

The EEOC also conducted an Outreach Webinar in March of 2020 to answer questions about following public health directives and complying with EEO laws.[93] Attorneys for the Americans with Disabilities Act[94] (hereinafter "ADA") and Genetic Information Nondiscrimination Act[95] (hereinafter "GINA") elaborated on the Act's continuing application with regard to employee treatment in the workplace.[96] Under the ADA, if an employee refuses to permit the employer to take his temperature, or "refuses to answer questions about whether he has COVID-19, symptoms associated with COVID-19, or has been tested for COVID-19," an employer can bar that employee from physical presence in the workplace.[97]

With respect to whether an employer can test individual employees, as opposed to all employees, the attorneys suggested that the ADA requires the employer to have a reasonable belief based on objective evidence that an individual might have a disease in order to test them.[98] Since employers can take notice that employees have certain symptoms, such as a cough, they can thereby inquire further about the employees' condition and even test them based on these observations.[99] The ADA also permits employers to report an employee to public health authorities if the employer learns that an employee has COVID-19.[100] The rationale for this comes from the direct threat that the disease poses not only to oneself but to others.[101]

### *C. State and Local Guidelines*

In addition to the guidance put out by various arms of the federal government, state governments and localities have set forth different

93. *See Transcript of March 27, 2020 Outreach Webinar*, U.S. EQUAL EMP. OPPORTUNITY COMM'N (Mar. 27, 2020), https://www.eeoc.gov/transcript-march-27-2020-outreach-webinar#q9.

94. *A Guide to Disability Rights Laws*, U.S. DEP'T OF JUST., C.R. DIV., DISABILITY RTS. SECTION, https://www.ada.gov/cguide.htm#anchor62335 (Feb. 24, 2020). "The ADA prohibits discrimination on the basis of disability in employment." *Id.* Employers with fifteen or more employees must provide equal opportunity to qualified individuals with disabilities. *Id.*

95. *GINA Help*, GENETIC INFO. NONDISCRIMINATION ACT (June 2010), http://www.ginahelp.org/GINAhelp.pdf "GINA is a federal law that protects individuals from genetic discrimination in health insurance and employment." *Id.*

96. *See* U.S. EQUAL EMP. OPPORTUNITY COMM'N *supra* note 93.

97. *Id.*

98. *Id.*

99. *See id.*

100. *Id.*

101. *Id.*

standards for temperature and health screening.[102] All states generally fit under the framework of either requiring temperature screening, recommending temperature screening, or neither of the two.[103] Of the twenty-nine states that require or recommend temperature screening, sixteen distinguish their requirements depending on the type of business in terms of essentialness or riskiness.[104]

For example, Delaware requires temperature checks for high risk businesses,[105] but simply "strongly recommend[s]" it for others.[106] Compare this to Washington, which takes into consideration not only risk, but the essentiality of a business.[107] Washington has also taken steps indicating they value privacy, expressing a preference for less intrusive methods of taking one's temperature such as asking employees to take their temperature prior to arriving to work and utilizing "no contact" thermometers to the greatest extent possible.[108] Other states such as New Hampshire adopt a more overarching approach, requiring all employers to institute temperature checks as part of their screening process.[109]

Localities may also have their own guidelines that differ from their state's advising.[110] In Texas, temperature checks are recommended as a state-wide measure,[111] however, the City of El Paso requires employers to conduct temperature checks as part of their health checks.[112]

---

102. *See generally* Littler, *This Won't Hurt a Bit: Employee Temperature and Health Screenings – A List of Statewide Orders*, JD SUPRA (Sept. 4, 2020), https://www.jdsupra.com/legalnews/this-won-t-hurt-a-bit-employee-64371 (emphasizing that different States have enacted varying laws and orders regarding the temperature checking and health screening of employees).

103. *See id.*

104. *See id.*

105. *See id.*; *High-Risk Essential Businesses*, DEL. HEALTH & SOC. SERV., DIV. OF PUB. HEALTH (Apr. 2, 2020), https://coronavirus.delaware.gov/wp-content/uploads/sites/177/2020/04/High-Risk-Business-List_04.2.20.pdf. High risk businesses are those considered to be Health Care businesses and necessary retail and service establishments — mostly schools and medical services. *See id.*

106. *Essential Services Screening Recommendations for COVID-19 Pandemic*, DEL. HEALTH & SOC. SERV., DIV. OF PUB. HEALTH, https://coronavirus.delaware.gov/wp-content/uploads/sites/177/2020/07/7.21-Essential-Services-Screening-Policy_final.pdf (Nov. 19, 2020).

107. *See* Littler, *supra* note 102.

108. *See id.*; GOVERNOR.WA.GOV., PHASE 1 CURBSIDE RETAIL COVID-19 REQUIREMENTS 3 (2020), https://www.governor.wa.gov/sites/default/files/FINAL%20Phase%201%20Curbside%20Retail%20Employee%20Safety%20and%20Health.pdf.

109. *See* Littler, *supra* note 102; STATE OF N. H., GOVERNOR'S ECON. REOPENING TASKFORCE, COVID-19 REOPENING GUIDANCE, https://www.covidguidance.nh.gov/sites/g/files/ehbemt381/files/files/inline-documents/guidance-universal.pdf (Oct. 6, 2020).

110. *See generally* Littler, *supra* note 102 (listing localities within Alaska and California that have health screening measures that go beyond what is required by their states).

111. *See id.*

112. CITY OF EL PASO, DEP'T OF PUB. HEALTH, CITY OF EL PASO HEALTH AUTH. ORD. FOR WORKPLACES (July 27, 2020), http://epstrong.org/documents/covid19/2020.07.27%20Orders%20for%20Workplaces.pdf?1595973293.

Conversely, the state of New York recommends temperature checks as part of an employer's mandatory health screening assessment,[113] but New York City has put forth guidance in its Sample Screening Tool stressing the confidentiality of the information collected from employees, advising they be kept separate from the employee's personnel file.[114]

### *D. HIPAA's Lack of Application to Workplace Health Screening*

In 1996, Congress enacted HIPAA.[115] Congress expressed a purpose of HIPAA was to "improve portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud, and abuse in health insurance and health care delivery."[116] With respect to the protection of health information, the Committee on Ways and Means stated, "[h]ealth information is considered relatively 'safe' today, not because it is secure, but because it is difficult to access. These standards improve access and establish strict privacy protections."[117] HIPAA's definition of "health information" is broad, including information either recorded or given orally.[118] To qualify as "health information," HIPAA looks to the institution handling the information[119] and whether the information pertains to past, present, or future physical or mental health.[120] Since an employer is listed as one of the institutions that can create or receive health information,[121] temperature checks or any other kind of health questionnaires meant to ascertain symptoms of illness would be considered "health information."[122]

As a work of federal legislation, HIPAA allows for the U.S. Secretary of Health and Human Services to set regulations adopting

113. *See* Littler, *supra* note 102.

114. *Sample COVID-19 Screening Tool*, NYC HEALTH 2 (Aug. 21, 2020), /https://www1.nyc.gov/assets/doh/downloads/pdf/imm/covid-19-symptom-screening-businesses.pdf [https://web.archive.org/web/20201101132741/https://www1.nyc.gov/assets/doh/downloads/pdf/imm/covid-19-symptom-screening-businesses.pdf].

115. *See Health Insurance Portability and Accountability Act of 1996 (HIPAA)*, CTRS. FOR DISEASE CONTROL & PREVENTION, https://www.cdc.gov/phlp/publications/topic/hipaa.html (Sept. 14, 2018).

116. H.R. REP. NO. 104-736, at 1 (1996).

117. H.R. REP. NO. 104-496, at 99 (1996).

118. 42 U.S.C. § 1320d(4).

119. *See id.* § 1320d(4)(A). Information "created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse." *Id.*

120. *Id.* § 1320d(4)(B).

121. *Id.* § 1320d(4)(A).

122. *See id.* § 1320d(4).

standards, including security standards for health information.[123] The regulations must take into account various practical concerns in maintaining health information.[124] HIPAA tasks "persons" described in 42 U.S.C. § 1320d-1(a) with providing far-reaching security protections.[125] These protections include maintaining safeguards to ensure that the information remains confidential, protecting from threats and unauthorized use, and securing the compliance of employees and officers of said persons.[126] However, although HIPAA's definition of "health information" is inclusive of information maintained by employers, in § 1320d-1(a), standards[127] adopted under the statute only apply to health plans, health care clearinghouses, and health care providers.[128]

HIPAA contains separate[129] provisions on wrongfully using, obtaining, or disclosing "individually identifiable health information" (hereinafter "IIHI").[130] IIHI is defined in almost the exact same terms as "health information," but IIHI also identifies the individual or provides a reasonable basis to do so.[131] The penalty for violating § 1320d-6(a) can result in fines of up to $250,000 depending on the circumstance.[132] However, persons are only punishable under this section if the information is maintained by a "covered entity" (hereinafter "CE").[133] CEs are defined by the HIPAA privacy regulation in § 1320d-9(b)(3),[134] which refers to regulations promulgated by the Secretary under the Act.[135] Akin to § 1320d-1(a), CEs only include health care plans, health care clearinghouses, and health care providers.[136] Thus, an employer would not be considered a CE, liable for misusing any obtained IIHI.

123. *Id.* §1320d-2(d)(1).

124. *See id.* § 1320d-2(d)(1)(A)(i)-(v).

125. *See id.* § 1320d-2(d)(2).

126. *Id.*

127. *Id.* § 1320d(7). (referring to data elements or transactions adopted or established by the Secretary under §§ 1320d-1 through 1320d-3).

128. *Id.* § 1320d-1(a).

129. *See id.* Since HIPAA's security protections do not apply to employers because the definition of "standard" only applies to §§ 1320d-1 through 1320d-3, a separate analysis is required to determine if an employer is subject to HIPAA's wrongful disclosure provisions under § 1320d-6.

130. *Id.* § 1320d-6(a).

131. *See id.* § 1320d(7).

132. *Id.* § 1320d-6(b).

133. *Id.* § 1320d-6(a).

134. *Id.*

135. *Id.* § 1320d-9(b)(3).

136. 45 C.F.R. § 160.103 (2021).

## II. ISSUE

With temperature checks and health screenings becoming the dominant methods employers are using to alleviate the fear of COVID-19 spreading in the workplace, an issue may arise when employees begin to question the use of the information they provide during these screenings.[137] Employees may be worried about whether this information is shared with third parties, where exactly the information is being stored, or for how long the information is being retained.[138] Some of these questions depend on the nature of the screening, as the data collected may range from temperature data to facial patterns to questionnaire answers.[139] Multiple states have enacted laws concerning biometric privacy, which may protect some types of data at issue.[140] Illinois is generally considered to have the most robust biometric data privacy statute, and its private right of action has facilitated many lawsuits that emphasize the importance of biometric data privacy as a fundamental right.[141] Other states have incorporated a variety of different protections, some of which may be favorable for a model statute.[142] However, the standard of "uniqueness" in most existing biometric data privacy laws may not encompass points of data such as temperature or answers to health questionnaires.[143]

### *A. The Methods and State of Temperature Checks and Other Health Screenings*

Since the start of the COVID-19 pandemic, there has been a large increase in demand for non-contact thermometers.[144] The sudden demand, coupled with a supply chain breakdown in China, resulted in a

137. *See* Jason C. Gavejian et al., *COVID-19 Screening Program Can Lead to Litigation Concerning Biometric Information, BIPA*, NAT'L L. REV. (Oct. 15, 2020), https://www.natlawreview.com/article/covid-19-screening-program-can-lead-to-litigation-concerning-biometric-information.

138. *See* Linn Freedman, *Data Privacy Considerations for Employers Collecting Health Data from Employees During Pandemic*, EHS TODAY (Oct. 30, 2020), https://www.ehstoday.com/covid19/article/21145909/data-privacy-considerations-for-employers-collecting-health-data-from-employees-during-pandemic.

139. *See infra* Section II.A.

140. *See infra* Section II.B.

141. *See infra* Section II.B.1.

142. *See infra* Section II.B.2.

143. *See infra* Section II.B.2.

144. Hayley Fowler, *Where Have All the Thermometers Gone? Suppliers Can't Keep Up as the Pandemic Drags On*, CHARLOTTE OBSERVER (May 19, 2020), https://www.charlotteobserver.com/news/coronavirus/article242838076.html [https://web.archive.org/web/20201117181930/https://www.charlotteobserver.com/news/coronavirus/article242838076.html].

supply shortage at multiple large retailers as of the spring of 2020.[145] In April of 2020, The Food and Drug Administration (hereinafter "FDA") released guidance to address this shortage of temperature measurement products.[146]

The FDA is an agency of the U.S. Department of Health and Human Services.[147] The agency is responsible for ensuring the safety of food, drugs, medical devices, and a host of other products.[148] One way the FDA accomplishes this is through "fostering development of medical products to respond to deliberate and naturally emerging public health threats."[149] The FDA differentiates between Non-Contact Infrared Thermometers[150] (hereinafter "NCITs") and telethermographic systems.[151] Both NCITs and telethermographic systems use forms of infrared technology to measure temperature.[152] Unlike NCITs, telethermographic systems do not require the operator to be close to the person being evaluated.[153] Telethermographic systems also utilize imaging to measure temperature differences across multiple locations of the body, as opposed to NCITs, which measure temperatures in a single location.[154]

Telethermographic systems can be marketed for non-medical purposes, and some are used in construction and other industrial applications.[155] When they are marketed for medical purposes they are considered "devices" under 21 U.S.C. § 321(h), which defines a "device" as "intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease, in man or other

145. *Id.*

146. U.S. DEP'T OF HEALTH & HUMAN SERVS., FOOD & DRUG ADMIN., ENFORCEMENT POLICY FOR TELETHERMOGRAPHIC SYSTEMS DURING THE CORONAVIRUS DISEASE 2019 (COVID-19) PUBLIC HEALTH EMERGENCY (2020), https://www.fda.gov/media/137079/download.

147. Office for Human Research Protections, *Food & Drug Administration*, HHS.GOV, https://www.hhs.gov/ohrp/regulations-and-policy/regulations/fda/index.html (Mar. 18, 2016).

148. *What We Do*, U.S. FOOD & DRUG ADMIN., https://www.fda.gov/about-fda/what-we-do (Mar. 28, 2018).

149. *Id.*

150. *See Non-contact Infrared Thermometers*, U.S. FOOD & DRUG ADMIN., https://www.fda.gov/medical-devices/general-hospital-devices-and-supplies/non-contact-infrared-thermometers (Apr. 23, 2020).

151. *Thermal Imaging Systems (Infrared Thermographic Systems / Thermal Imaging Cameras)*, U.S. FOOD & DRUG ADMIN., https://www.fda.gov/medical-devices/general-hospital-devices-and-supplies/thermal-imaging-systems-infrared-thermographic-systems-thermal-imaging-cameras (Jan. 12, 2021).

152. *Id.*

153. *Id.*

154. *Id.*

155. FOOD & DRUG ADMIN., *supra* note 146, at 4.

animals."[156] Unlike telethermographic systems intended for non-medical purposes, the FDA requires "devices" to be compliant with various regulations that authorize device marketing.[157] The FDA's guidance here states that it "does not intend to object to the distribution and use of telethermographic systems . . . without compliance with the following regulatory requirements where such devices do not create an undue risk in light of the public health emergency."[158] The FDA still sets forth performance and labeling guidelines for these devices, but is ultimately sacrificing traditional compliance for the sake of availability.[159]

NCITs, on the other hand, are generally easier to use and clean.[160] NCITs are handheld products that are meant to be held up to a person's forehead to measure their temperature.[161] These thermometers can discern a person's temperature by measuring the infrared energy coming off of their body.[162] These cheap, easy-to-use, non-invasive, and accurate hand-held no touch thermometers were the most popular method for screening during the Ebola pandemic in 2014.[163]

However, products used to measure temperature via infrared technology are far from a perfect screening method.[164] Dr. Anthony Fauci of the National Institute for Allergy and Infectious Diseases has spoken out against the popular infrared thermometers, saying "temperatures are notoriously inaccurate many times."[165] A more accurate reading would come not from a person's forehead, but from their tongue or rectum.[166] Temperature checks have also come under criticism in relation to curbing the spread of COVID-19, as the virus is contagious before symptoms

156. 21 U.S.C. § 321(h)(2).

157. *See* FOOD & DRUG ADMIN., *supra* note 146, at 4.

158. *Id.*

159. *See id.* at 5.

160. *See* U.S. FOOD & DRUG ADMIN., *supra* note 150.

161. *See id.*

162. Alison Bruzek, *How a No-Touch Thermometer Detects a Fever*, NPR (Oct. 15, 2014), https://www.npr.org/sections/health-shots/2014/10/15/356398102/how-a-no-touch-thermometer-detects-a-fever.

163. *Id.*; *see also* Eleanor Klibanoff, *Why a Thermometer is a Good Tool for Airport Ebola Screenings*, NPR (Oct. 2, 2014), https://www.npr.org/sections/goatsandsoda/2014/10/02/353230343/why-a-thermometer-is-a-good-tool-for-airport-ebola-screenings.

164. *See* Lisette Voytko, *Fauci Says Coronavirus Temperature Checks 'Notoriously Inaccurate'*, FORBES (Aug. 13, 2020), https://www.forbes.com/sites/lisettevoytko/2020/08/13/fauci-says-coronavirus-temperature-checks-notoriously-inaccurate.

165. *Id.*

166. *Id.*

appear.[167] Thus, critics have characterized these tests as misleading, despite trying to be reassuring.[168]

Some experts are skeptical of effectiveness of fever checks, questioning its ability to screen out infected individuals.[169] An infectious disease specialist at Johns Hopkins University School of Medicine has likened temperature checks to getting an oil change in your car, stating "[i]t makes you feel better, but it's not going to keep you from wrecking the car or prevent the tires from falling off. It's not going to make your trip any safer."[170] Since fever is not a reliable indicator, it has been suggested that employers are implementing temperature screening merely to alleviate employee anxiety.[171]

Some products that utilize telethermographic systems in the form of tablets with scanners may also collect data that implicates existing biometric data privacy law.[172] Glory Star is a leading developer of commercial tablets[173] and is the manufacturer of TAURI, a popular tablet capable of determining an employee's temperature.[174] TAURI uses face detection to tell if a human face is before its camera, and an infrared sensor to detect a person's temperature.[175] However, the tablet also has facial recognition capabilities.[176] TAURI stores up to 5,000 faces and uses this feature in the event "an employee runs a high temperature, time and location is marked and an email alert is sent to facilitate tracking and decrease the spread of infection."[177]

Pairing an employee's unique biometric identifier such as facial patterns may subject employers to the protections of state biometric data

167. James Hamblin, *Paging Dr. Hamblin: Everyone Wants to Check My Temperature*, THE ATLANTIC (Aug. 12, 2020), https://www.theatlantic.com/health/archive/2020/08/paging-dr-hamblin-temperature-checks-coronavirus/615190.

168. *See id.*

169. *See* Roni Caryn Rabin, *Fever Checks Are No Safeguard Against Covid-19*, N.Y. TIMES, nytimes.com/2020/09/13/health/covid-fever-checks-dining.html (Sept. 14, 2020).

170. *Id.*

171. Michelle T. Olson & Cara J. Ottenweller, *Temperature Screening: New Guidance From the CDC, FAQs, and Best Practices*, NAT'L L. REV. (May 14, 2020), https://www.natlawreview.com /article/temperature-screening-new-guidance-cdc-faqs-and-best-practices.

172. *See infra* Section II.B.

173. *About Glory Star*, GLORY STAR, https://www.glorystartouch.com/copy-of-why-us (last visited Oct. 24, 2020).

174. *See* https://google.com (search "temperature scan tablets") (last visited Oct. 24, 2020) [https://perma.cc/2FQC-Z33Q]. The first page of Google search results reflects many different sites selling TAURI, indicating popularity. *See id.*

175. *See* TAURI, *supra* note 17.

176. *Id.*

177. *Id.*

privacy law.[178] TAURI advertises features "coming soon" that allow employers to view staff temperature check results paired with their respective profiles, as well as analysis charts.[179] Other tablets, such as InVid, store up to 20,000 faces,[180] and have demonstrated the capability to deny physical access to the workplace when an employee fails a screening.[181]

Alternative methods of temperature checking may be used by employers that want to screen their employees before they come to work. For example, VitaCorpo has emerged as a mobile application that uses a Bluetooth connected thermometer to register an employee's temperature and blood oxygen levels, which are sent to the employer.[182] The company's Chief Product Officer sees the detriment to employees congregating at the entrance of workplaces to be screened, saying "you've already brought everyone together and possibility cross-contaminated your employees."[183]

Employers may opt to screen their employees by obtaining health-related information through questionnaires, rather than directly measuring it.[184] Many states and localities recommend, or even require, this practice of obtaining health related information via surveys or questionnaires for businesses to open.[185] For example, New York City's Sample COVID-19 Screening Tool outlines questions for employers to use in health screening questionnaires, such as the following: "Have you experienced a fever of 100.4 degrees Fahrenheit or greater, a new cough, new loss of taste or smell, or shortness of breath within the past 10 days?", and "In the past 14 days, have you traveled internationally or returned from a state identified by New York State as having widespread community transmission of COVID-19 (other than just passing through the restricted state for less than 24 hours)?"[186] The dual purposes of these surveys are to monitor the health and well-being of employees and to determine

178. *See infra* Section II.B.

179. *See* TAURI, *supra* note 17.

180. *See* INVID TECH, *supra* note 17.

181. *See Tablet Demo Video*, INVID TECH, https://f.hubspotusercontent30.net/hubfs/4117135/Video/TabletDemo/TabletDemoVideo.mp4 (last visited May 26, 2021).

182. *See* Vanessa Ruffes, *Charlotte Company Develops COVID-19 App to Pre-screen Employees Before Coming to Work*, WCNC CHARLOTTE (Oct. 5, 2020), https://www.wcnc.com/article/news/health/coronavirus/charlotte-company-covid-19-app-pre-screen-employees-before-coming-to-work/275-23c1d38f-5ec4-415c-8a8f-5d9b140c65fd; *see also* VITACORPO, *supra* note 19.

183. Ruffes, *supra* note 182.

184. *See* Littler, *supra* note 102.

185. *See id.*

186. *See* NYC HEALTH, *supra* note 114.

whether they should be allowed to return to the workplace.[187] While a survey may seem less invasive than an employer checking temperatures using an NCIT, a survey's information is still being recorded and retained by the employer to maintain their records and potentially analyze.[188]

### *B. Biometric Data Privacy Law*

Data privacy policy goals used to be accomplished through laws requiring the notification of consumers and regulatory agencies when instances of unauthorized disclosures or misuses of data were detected.[189] More recently there has been a shift to protect the collection and usage of data, including data that is associated with biological identifiers.[190] Biometric data privacy law is an up-and-coming field of law, which only eight states make explicit reference to in their existing statutes.[191] Biometrics typically refer to physical characteristics that can be used to identify a person.[192] Data consisting of a person's DNA, retinal scans, or fingerprints is often captured in an employment context, and has been the subject of lawsuits.[193] Biometrics are often used for authentication protocol, as a person's biometric data is immutable and cannot be changed, unlike a password or social security number.[194]

These laws are most analogous to the issue of employee health screening, as they are more likely to be implicated in issues arising from the data collected from health screenings.[195] For example, in September of 2020, a former Amazon employee filed a class action lawsuit against

187. *Id.*

188. *See generally* e-mail from Student Health Screening, Hofstra Univ., to Shiddhartha Uddin, student (Oct. 9, 2020, 9:28 AM) (on file with author) (demonstrating a potential use of collected and analyzed data by an organization as related to one of its active members). Hofstra University sent e-mails to students that failed to fully comply with its policy of completing the mandatory health screening for each day they were on campus. *Id.* The e-mail states the number of days during the previous month that the student signed into the campus' Wi-Fi, and how many times the student completed the mandatory health screening. *Id.* The e-mail reminds students that "[n]ot complying with this policy is grounds for community standards sanctions up to and including removal from on-campus learning and residence halls." *Id.*

189. Erin Jane Illman, *Data Privacy Laws Targeting Biometric and Geolocation Technologies*, 73 THE BUS. L. 191, 191 (2018).

190. *See id.*

191. Kristine Argentine & Paul Yovanic, *The Growing Number of Biometric Privacy Laws and the Post-COVID Consumer Class Action Risks for Business*, JD SUPRA (June 9, 2020), https://www.jdsupra.com/legalnews/the-growing-number-of-biometric-privacy-62648.

192. *Id.*

193. *Id.*

194. John G. Browning, *The Battle Over Biometrics*, 81 TEX. B. J. 674, 674 (2018).

195. *See* Gavejian et al., *supra* note 137.

the tech giant under Illinois' biometric data privacy statute.[196] In the complaint filed, the plaintiff described Amazon's policy of conducting wellness checks on their employees before they were allowed access to the facility each day.[197] Amazon's devices that scanned and recorded workers' temperatures also captured biometric information such as the employees' facial geometry.[198] The suit contends that Amazon did not act in accordance with the Illinois' statute, which imposes requirements concerning the retention and destruction of that data, amongst other things.[199] With the prospect of more employers using devices similar to Amazon's in their wellness checks, the importance of laws concerning the privacy of information has never been higher.

Of the eight states that reference biometric data privacy in their laws, Illinois, Texas, and Washington are the only three that provide extensive protections that adopt standards of consent, disclosure, and retention of the biometric data.[200] California includes protections of biometric data, but as part of the California Consumer Privacy Act (hereinafter "CCPA"), it is restricted to consumers.[201] Oregon includes "physicals characteristics" akin to biometrics in its definition of "personal information" in its own Consumer Identification Protection Act.[202] New York, Louisiana, and Arkansas include biometric information in their definitions of "private" or "personal" information, but their laws are almost solely concerned with notification in the event of a security breach.[203]

### 1. Illinois' Biometric Information Privacy Act

In 2008, Illinois became the first state to enact a law addressing the collection of biometric data when it passed the Biometric Information Privacy Act (hereinafter "BIPA").[204] The Illinois General Assembly

196. Lauraann Wood, *Amazon COVID-19 Scans Ignore Workers' Rights, Ill. Suit Says*, LAW360 (Oct. 8, 2020, 5:05 PM), https://www.law360.com/articles/1318190/amazon-covid-19-scans-ignore-workers-rights-ill-suit-says.

197. Complaint at 2, Jerinic v. Amazon.Com, Inc. et al., No. 2020CH06036 (Ill. Cir. Sept. 28, 2020), https://www.law360.com/articles/1318190/attachments/0.

198. *Id.*

199. *Id.* at 8.

200. *See id.*; *see also* 740 ILL. COMP. STAT. ANN. 14/15(a)-(b) (West 2020); TEX. BUS. & COM. CODE § 503.001 (West 2019); WASH. REV. CODE ANN. § 19.375.020(1)-(4) (West 2020).

201. CAL. CIV. CODE § 1798.140(o)(1)(E) (West 2020).

202. OR. REV. STAT. ANN. § 646A.602(12)(a)(A)(v) (West 2020).

203. *See* N.Y. GEN. BUS. LAW § 899-aa(1)(b)(3) (McKinney 2020); LA. REV. STAT. ANN. § 51:3073(4)(a)(v) (2020); ARK. CODE ANN. § 4-110-103(7)(l)(E)(i) (West 2020).

204. Browning, *supra* note 194, at 674.

recognized the heightened risk of identity theft that comes as a consequence of using biometric identifiers in transactions, and as a result, it passed BIPA to provide protections for this information.[205] BIPA defines "biometric identifiers" as "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry."[206] BIPA protects biometric information by requiring entities that capture the information to inform the subject of the data's capture, its purpose, and length of term of the data's retention.[207] The entity must also receive a written release of the data from the subject.[208] The law also prohibits entities from profiting off of a subject's biometric information, and said information cannot be disclosed unless authorized by the subject or required by state or federal law.[209] Finally, the provision of BIPA that sets the law apart from its state counterparts is the statute allowing any person aggrieved by the Act to have a private right of action against the offending party.[210]

A private right of action is important because while some relevant statutory schemes (such as HIPAA) provide protection, without a private right of action, only the state's attorney general can bring forth a lawsuit.[211] Under BIPA's private right of action, there have been multiple class action lawsuits against companies for the wrongful collection or sharing of data.[212] The plaintiffs in these cases span a range from consumers to employees, but the defendants are typically companies instituting new policies with new technology.[213] In recent years, various federal courts have taken these lawsuits to develop the importance of privacy under law with respect to Article III standing.[214]

In constitutional law jurisprudence, the Supreme Court has held that "general factual allegations of injury resulting from the defendant's

205. *See* 740 ILL. COMP. STAT. ANN. 14/5(c) (West 2020).

206. *Id.* 14/10.

207. *Id.* 14/15(b).

208. *Id.* 14/15(b)(3).

209. *Id.* 14/15(d)(3)-(4) (disclosure may be required pursuant to a law, or a valid warrant or subpoena).

210. *Id.* 14/20.

211. *See, e.g.*, Lee-Thomas v. LabCorp., 316 F. Supp. 3d 471, 474 (D.D.C. 2018) ("While [HIPAA] provides both civil and criminal penalties for improperly handled or disclosed information, the language of the statute specifically limits enforcement action to HHS and individual states' attorneys general.").

212. *See, e.g.*, Patel v. Facebook, Inc., 932 F.3d 1264, 1268 (9th Cir. 2019); Rosenbach v. Six Flags Ent. Corp., 129 N.E.3d 1197, 1204 (Ill. 2019); Dixon v. Washington & Jane Smith Cmty., No. 17 C 8033, 2018 U.S. Dist. LEXIS 90344, at *1 (N.D. Ill. May 31, 2018).

213. *See, e.g.*, *Rosenbach*, 129 N.E.3d at 1200 (Six Flags implemented the scanning of fingerprints to verify customer identities more quickly); *Dixon*, 2018 U.S. Dist. LEXIS 90344, at *2 (Dixon's employer required employees to clock in and out of work by scanning their fingerprints).

214. *See, e.g.*, *Patel*, 932 F.3d at 1274; *Dixon*, 2018 U.S. Dist. LEXIS 90344, at *33.

conduct" are needed to survive a defendant's motion to dismiss.[215] An "injury" can still be concrete even if the harm is intangible, as opposed to a tangible injury such as monetary loss or physical harm.[216] As applied to BIPA violations, these plaintiffs have had to argue that they have been aggrieved in an intangible way, claiming that an invasion of privacy in and of itself should confer standing under Article III.[217]

In *Dixon v. Washington & Jane Smith Cmty.*, the plaintiff sued her employer, a senior living home, that required employees to scan their fingerprint upon entering the workplace.[218] Like most other cases involving BIPA, Dixon's employer did not make information available about their data retention and destruction policies.[219] However, in that case, the question of standing also involved a clearer injury of the technology's third-party vendor gaining access to the data.[220] This was sufficient to distinguish it from the 2017 decision in *Rosenbach v. Six Flags Entertainment Corp.*, when violations of the notice and consent provisions of BIPA were considered "technical violations" that ultimately did not confer standing.[221] The *Dixon* court described the privacy violation stemming from the disclosure to a third party as "the very right that the drafters of BIPA sought to protect"[222] and thus concluded the plaintiff did allege an actual and concrete injury.[223]

The *Rosenbach* case also represents a step the courts have taken to solidify that violations of privacy are in fact an injury.[224] In *Rosenbach*, a mother sued Six Flags for violating BIPA's notice and consent provisions when they captured her son's fingerprint for his season pass to the park.[225] The 2017 decision was appealed to the Supreme Court of Illinois in 2019 and the court reversed the lower court's decision.[226] The *Rosenbach* court engaged in a statutory analysis, looking at the language of Section 20 which states that a person "aggrieved" shall have a private

215. Lujan v. Defenders of Wildlife, 504 U.S. 555, 561 (1992).

216. *See* Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1549 (2016).

217. *See, e.g.*, *Patel*, 932 F.3d at 1271; *Dixon*, 2018 U.S. Dist. LEXIS 90344, at *11.

218. *Dixon*, 2018 U.S. Dist. LEXIS 90344, at *2-3.

219. *Id.*

220. *Id.*

221. *Id.* at 38.

222. *Id.* at 27.

223. *Id. But see* Santana v. Take-Two Interactive Software, Inc., 717 F. App'x 12, 16-17 (2d Cir. 2017) (The Second Circuit does not adopt the same approach, holding that the plaintiffs "therefore have failed to show a 'risk of real harm' sufficient to confer an injury-in-fact.").

224. *See supra* Section II.B.

225. Rosenbach v. Six Flags Entm't Corp., 129 N.E.3d 1197, 1203 (Ill. 2019).

226. *Id.* at 1207.

right of action against the offending party.[227] In deciding whether the plaintiff was "aggrieved," the court noted that the statute does not provide a definition for "aggrieved."[228] Thus, the court assumed its popularly understood meaning, which is determined to be "having legal rights that are adversely affected."[229] The court further reasoned that it would be antithetical to the Act's purpose to require individuals to wait until they have sustained a compensable injury in order to sue, since their statutory rights have been violated.[230]

Courts outside the state of Illinois have also ruled in favor of recognizing BIPA violations as harms conferring Article III standing.[231] In 2019, the Ninth Circuit Court of Appeals issued a ruling in *Patel v. Facebook, Inc.*, stating that individuals have a privacy right not to be subject to the collection and use of biometric data.[232] In that case, the plaintiff sued Facebook under BIPA for its use of facial-recognition technology in its "Tag Suggestion" feature.[233] *Patel* clarified that violation of BIPA's Sections 15(a) and 15(b), which cover data retention protocols and informed consent before collection, were sufficient to show actual harm.[234] Over the last year, Illinois District Courts have extended this rationale to claims under BIPA's Sections 15(d) and 15(e), which concern the disclosure of data and the standard of care taken.[235] Most recently, the Illinois Southern District Court in *Roberson v. Maestro Consulting Servs. LLC* reasoned that these sections "form[] a piece of the retention regime" and can be understood to constitute a concrete injury.[236]

These decisions are notable in the context of employee health screenings because they illustrate an emphasis not only on the importance of data privacy as a right, but on the willingness of people to take legal

227. *Id.* at 1199; 740 ILL. COMP. STAT. ANN. 14/20 (West 2020).

228. *Rosenbach,* 129 N.E.3d at 1205.

229. *Id.* (quoting Black's Law dictionary).

230. *Id.* at 1207.

231. *See* Patel v. Facebook, Inc., 932 F.3d 1264 (9th Cir. 2019).

232. *Id.* at 1274.

233. *Id.* at 1268. Facebook's "Tag Suggestion" feature scans photos when they are uploaded to Facebook and detects whether it contains images of faces. *Id.* If so, the technology can map geometric points on each face, creating a "signature" for each person, enabling Facebook to recognize faces and suggest tagging recognized individuals in photos. *Id.*; *see also* Jared Bennett, *Saving Face: Facebook Wants Access Without Limits*, THE CTR. FOR PUB. INTEGRITY, https://publicintegrity.org/inequality-poverty-opportunity/saving-face-facebook-wants-access-without-limits/ (Aug. 1, 2017, 3:00 PM).

234. *Patel*, 932 F.3d at 1274.

235. *See* Roberson v. Maestro Consulting Servs. LLC, 507 F.Supp.3d 998, 1009-10 (S.D. Ill. 2020); Cothron v. White Castle Sys. Inc., 467 F. Supp. 3d 604, 610-11, 613 (N.D. Ill. 2020); *see also* 740 ILL. COMP. STAT. ANN. 14/15 (d), (e) (West 2008).

236. *See Roberson*, 207 F.Supp.3d at 1010.

action when that privacy has been invaded.[237] In the current state of biometric data privacy law, some devices used in temperature checks and health screenings will undoubtedly implicate existing provisions.[238] Although BIPA was originally passed under the pretense that biometrics were being used in Chicago as "pilot testing sites,"[239] the increasing prevalence (due to COVID-19) of technology capable of capturing biometric information[240] should warrant the expansion of laws protecting that information.

### 2. Biometric Data Privacy Laws of Other States

While Illinois has seen its share of lawsuits due to the statute's private right of action, both Texas and Washington have passed separate pieces of legislation codifying protections for biometric data.[241] Texas' Capture or Use of Biometric Identifier Act (hereinafter "CUBI") was passed in 2009, one year after BIPA.[242] The statute has similarities to BIPA, such as commonality between their definitions of biometric information and their standards of care with regard to the storage of biometric information.[243] However, the Texas statute imposes a harsher penalty for violations and does not distinguish between a negligent violation and an intentional violation.[244] Besides the lack of a private right of action, perhaps the most significant differentiation between BIPA and CUBI is that CUBI is more narrowly applied in that the statute only

237. *See generally Patel*, 932 F.3d at 1267; Rosenbach v. Six Flags Ent. Corp., 129 N.E.3d 1197, 1199-1200, 1206 (Ill. 2019); Dixon v. Washington & Jane Smith Cmty., No. 17 C 8033, 2018 U.S. Dist. LEXIS 90344, at *1-3 (N.D. Ill. May 31, 2018).

238. *See supra* Section II.A.

239. *See* 740 ILL. COMP. STAT. ANN. 14/5(b) (West 2008).

240. Gavejian et al., *supra* note 137. "COVID-19 screening programs, as well as the extensive technology at our disposal and/or in development are certainly helping organizations address the COVID-19 pandemic. . . . Nevertheless, organizations must consider the legal risks, challenges, and requirements with any such technology prior to implementation." *Id.*

241. *See* Browning, *supra* note 194, at 674-76.

242. *See* TEX. BUS. & COM. CODE ANN. § 503.001 (West 2019).

243. *Compare id.* § 503.001(c)(2) (for storing information, a person who possesses a biometric identifier shall use a reasonable standard of care, as or more protective than the manner in which they treat confidential information), *with* 740 ILL. COMP. STAT. ANN. 14/15 (West 2020) (an entity in possession of and storing biometric information shall maintain a reasonable standard of care within the private entity's industry).

244. *Compare* TEX. BUS. & COM. CODE ANN. § 503.001(d) (West 2019) ("A person who violates this section is subject to a civil penalty of not more than $25,000 for each violation"), *with* 740 ILL. COMP. STAT. ANN. 14/20(1), (2) (West 2020) (An entity that negligently violates the Act is subject to a $1,000 fine for each violation, with a reckless or intentional violation being subject to a $5,000 fine for each violation).

protects biometric information that is "captured for a commercial purpose."[245]

Washington State's biometric data privacy law was enacted in 2017 and was passed with the intent of protecting information that could identify people for "commerce, security, and convenience" purposes.[246] The Washington statute also differs from both BIPA and CUBI in its enforcement in that there is no private right of action, but the state's attorney general can enforce violations not under the statute itself, but rather under the state's consumer protection act.[247] Washington also takes a less stringent approach to retention of data, adopting a standard that data should be retained no longer than reasonably necessary to comply with the law, protect against fraud, or provide services.[248] This is a departure from the previous approaches by BIPA and CUBI, which specify a number of years that the data is allowed to be retained.[249] Notably, all protections the Washington statute provides are only applicable if the data is "enrolled" in a database.[250]

While Illinois, Texas, and Washington have separate laws protecting biometric data, other states implement biometric information into existing data protection schemes.[251] California's CCPA was passed with a more general intent to protect information collected or stored by businesses from consumers, not being limited to information collected electronically or over the internet.[252] The CCPA's definition of "biometric identifier" is particularly exhaustive,[253] but does not have specific exclusions the way

245. *See* TEX. BUS. & COM. CODE ANN. § 503.001 (West 2019).

246. *See* WASH. REV. CODE ANN. § 19.375.900 (West 2020).

247. *See id.* § 19.375.030.

248. *See id.* § 19.375.020(4)(b).

249. *See, e.g.*, 740 ILL. COMP. STAT. ANN. 14/15(a) (West 2020) (destruction period of within 3 years of the individual's last interaction with the private entity); TEX. BUS. & COM. CODE ANN. § 503.001(c)(3) (West 2019) (destruction period of no later than one year after the date of the purpose for collecting the identifier expires).

250. *See* WASH. REV. CODE ANN. § 19.375.020(6) (West 2020); WASH. REV. CODE ANN. § 19.375.010(5) ("'Enroll' means to capture a biometric identifier of an individual, convert it into a reference template that cannot be reconstructed into the original output image, and store it in a database that matches the biometric identifier to a specific individual.").

251. *See supra* Section II.B.

252. *See* CAL. CIV. CODE § 1798.175 (West 2020).

253. *See id.* § 1798.140(b). *Id.* § 1798.140(b) states as follows:

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

other statutes such as BIPA do.[254] The CCPA currently includes "biometric identifier" under its definition of "personal information,"[255] but on Election Day of 2020, California approved a measure to expand the CCPA, notably creating a new category of "sensitive personal information" which will include biometric information, when it goes into effect in 2023.[256] One component of the CCPA that differentiates it from its counterparts is its "opt-out" provision, which allows the consumer to opt out of the sale of their personal information when collected by a business.[257]

Three of the four remaining states (Arkansas, Louisiana, New York, and Oregon) with statutes that mention biometrics, are not concerned with the capturing of data so much as they concern the notification of breach of existing data.[258] Arkansas being the exception, has a Personal Information Protection Act (hereinafter "PIPA")[259] similar to California's statute in that PIPA provides protection for biometric data, but is neither centrally focused on biometrics like BIPA, CUBI, and Washington's statute, nor is it silent on all but notification in the event of breach like Louisiana, New York, and Oregon.[260] PIPA is most notable for having a relatively exhaustive provision on how the destruction of personal information should take place.[261]

The other state statutes' mention of biometric information come from amendments within the last six years, all relating to the notifications of a security breach.[262] When mentioned, the purpose of these statutes tends to be combating identity theft in a transactional setting,[263] but the language the statutes employ to define biometrics may prove useful when

---

extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information.

254. *Compare id.*, *with* 740 ILL. COMP. STAT. ANN. 14/10 (West 2020) (the definition for "biometric identifier" includes a list of exclusions, such as materials already regulated under GINA or information captured from a patient under HIPAA).

255. CAL. CIV. CODE § 1798.140(o)(1)(E) (West 2020).

256. *See* Matthew A. Diaz & Kurt R. Hunt, *California Approves the CPRA, a Major Shift in U.S. Privacy Regulation*, NAT'L L. REV. (Nov. 17, 2020), https://www.natlawreview.com/article/california-approves-cpra-major-shift-us-privacy-regulation.

257. *See* CAL. CIV. CODE § 1798.120(b) (West 2020).

258. *See, e.g.*, OR. REV. STAT. ANN. § 646A.604 (West 2020); N.Y. GEN. BUS. LAW § 899-aa(2)-(3) (McKinney 2020); LA. REV. STAT. ANN. § 51:3074(C)-(E) (2020).

259. ARK. CODE ANN. § 4-110-101 (West 2020).

260. *See id.* § 4-110-104.

261. *See id.* ("[B]y shredding, erasing, or otherwise modifying the personal information in the records to make it unreadable or undecipherable through any means.").

262. *See, e.g.*, Stop Hacks and Improve Electronic Data Security Act (SHIELD Act), S.B. 5575, Legis. Sess. (N.Y. 2019); S.B. 361, 2018 La. Acts 382; S.B. 601, 78th Or. Legis. Assemb. (Or. 2015).

263. *See, e.g.*, LA. REV. STAT. ANN. § 51:3072 (2020).

crafting a model statute. For example, Oregon's definition of "personal information" is broader than just biometrics, it protects any "[d]ata from automatic measurements of a consumer's physical characteristics."[264] New York splits up the definitions of "personal information" and "private information," the former being used to identify a person, with the latter being personal information that is paired with biometric information used to authenticate that person.[265]

## III. SOLUTION

In light of growing concerns relating to data privacy,[266] coupled with the dramatic increase in workplace practices that accumulate health data,[267] the law must adapt in order to assure that the privacy of individuals remains protected. With the CDC acknowledging that health screenings ought to remain as private as possible, there is an implicit recognition that people may want that data to remain private.[268] Existing biometric data privacy laws are relevant to the solution because they have already begun to be implicated in lawsuits arising from employee health screenings.[269] With devices, such as the ones Amazon uses, becoming more prevalent,[270] along with the loosening of FDA restrictions on devices used in temperature screenings,[271] new laws are needed to curb any conceivable privacy violations.

Even after the COVID-19 pandemic is over, employers may opt to continue health screenings, in the interest of reducing health insurance costs.[272] Stress at work can cause multiple symptoms that may be observed or reported during employee health screenings such as a spike in temperature or cold-like symptoms.[273] Employers can use this data to infer which employees are more likely to rack up greater health insurance costs and make employment decisions accordingly.[274] Some employers

264. OR. REV. STAT. ANN. § 646A.602 (West 2020).

265. N.Y. GEN. BUS. § 899-aa(1)(b) (McKinney 2020).

266. *See* CYNERGISTEK, *supra* note 20.

267. *See, e.g.*, Singer, *supra* note 1; Wells, *supra* note 12.

268. *See* CTRS. FOR DISEASE CONTROL & PREVENTION, *supra* note 60.

269. *See* Wood, *supra* note 196.

270. *See, id.*; *see e.g.*, TAURI, *supra* note 17.

271. *See* FOOD & DRUG ADMIN., *supra* note 146, at 4.

272. *See* Elizabeth A. Brown, *A Healthy Mistrust: Curbing Biometric Data Misuse in the Workplace*, STAN. TECH. L. REV. 252, 257 (2020).

273. *See* Adrienne Santos-Longhurst, *Can Stress Make You Sick,* HEALTHLINE, https://www.healthline.com/health/can-stress-make-you-sick (July 31, 2018).

274. *See, e.g.*, Brown, *supra* note 272, at 256-57. Diana Diller was a user of an app called Ovia, which allowed her employer to track the progress of her pregnancy. *Id.* at 256. Data such as how she

may not even go as far as considering the health insurance cost, but may determine that workers with higher stress levels are likely to be less productive and therefore less desirable.[275]

### *A. Model Statute*

This section aims to propose a framework that states may choose to adopt to offer protections for employee health screening data. The model statute shall be known as the "Protecting Health Information and Screening History (PHISH) Act". Some have proposed federal regulations to protect biometric data generally, but lobbying by big technology corporations is likely to prevent this from coming to fruition.[276] Additionally, the legislative intent behind existing statutes generally covers either consumer privacy or concerns of entities misusing data that may result in identity theft.[277] The statute ultimately adopts methods used in state biometric data privacy statutes to govern the circumstances which employers and other entities may capture and use data.[278] The PHISH Act will also draw from the various statutes in outlining standards of retention and destruction of health screening data.[279] The Act includes a private right of action, in an effort to deter companies from misusing data, resulting in a lawsuit.[280]

#### 1. Legislative Intent

State legislatures will adopt the framework of the PHISH Act under the intention of promoting autonomy and transparency in all matters related to data obtained in health screenings. Similar to BIPA's expressed

felt and which medications she was taking was tracked through the app. *Id.* Using this information, her employer could have made determinations on Diller's or other employees' employment based on which employees were more likely to rack up high health insurance costs as a result of more expensive treatments associated with their pregnancies. *Id.* at 257.

275. *Id.* at 274.

276. *See* Carra Pope, *Biometric Data Collection in an Unprotected World: Exploring the Need for Federal Legislation Protecting Biometric Data*, 26 J. L. & POL'Y 769, 798 (2018). Additionally, Facebook spends far more money on lobbying at the federal level ($8.7 million) than they do lobbying state officials ($670,000). *See* Chris Burt, *Facebook Lobbying Against Facial Recognition Laws*, BIOMETRICUPDATE.COM (Aug. 1, 2017), https://www.biometricupdate.com/201708/facebook-lobbying-against-facial-recognition-laws.

277. *See, e.g.*, 740 ILL. COMP. STAT. ANN. 14/5(b)(c) (West 2020); LA. REV. STAT. ANN. § 51:3072 (2020).

278. *See infra* Section III.A.3.

279. *See infra* Section III.A.4.

280. *See infra* Section III.A.5.

legislative intent, the ramifications of these new practices of health screenings are not yet fully known.[281] The Washington statute's legislative intent recognizes a concern when citizens are increasingly asked to disclose identifying information.[282] The PHISH Act is meant to supplement existing protections that are more concerned with identity theft or narrowly applied to consumers only.[283]

2. Definitions

In the interest of covering a broad spectrum of information, the PHISH Act's definition of "health information" will be reflective of HIPAA's scheme, covering "any information, whether oral or recorded in any form or medium" that "relates to the past, present, or future physical or mental health or condition of an individual."[284] Similar to the CCPA, this definition contains no exclusions[285] in an effort to differentiate the PHISH Act from the existing laws that only focuses on identifiers that are unique and cannot be changed.[286] In order to be broad enough to cover the issue of scanners that take in more information (such as biometrics) being used in health screenings, "health information" shall also include "data from automatic measurements of a person's physical characteristics that is used to authenticate a person's identity," similar to Oregon's statute.[287]

The Act will define "informed consent" to be consistent with the Black's Law Dictionary definition, "[a] person's agreement to allow something to happen, made with full knowledge of the risks involved and the alternatives."[288] Like Washington's statute, the PHISH Act will define what it means to "capture" data[289] as "the process of collecting health information from an individual."[290] Reflecting HIPAA's structure of "covered entities," the PHISH Act shall define a "covered entity" as any "employer, health care provider, or business that captures or retains health information."[291]

281. *See* 740 ILL. COMP. ANN. 14/5(f) (West 2020).
282. WASH. REV. CODE ANN. § 19.375.900 (West 2020).
283. OR. REV. STAT. ANN. §§ 646A.602 – 646A.628 (West 2020).
284. *See* 42 U.S.C. § 1320d(4)(B) (2018).
285. *See* sources cited *supra* note 255.
286. *See, e.g.*, 740 ILL. COMP. STAT. ANN. 14/10 (West 2020).
287. *See* OR. REV. STAT. ANN. § 646A.602 (West 2020).
288. *Informed Consent*, BLACK'S LAW DICTIONARY (10th ed. 2014); *see infra* Section III.A.3.
289. *See* WASH. REV. CODE ANN. § 19.375.010(3) (West 2020).
290. *Id.* at § 19.375.010(5).
291. 45 C.F.R. § 160.103 (2021).

3. Capturing and Use of Information

The PHISH Act will provide that "no covered entity shall capture health information without the informed consent of the person identified. A written release is required to satisfy this requirement." Informed consent is necessary because an employee may not be aware of the implications of letting an employer capture their data.[292] For example, BIPA's original enactment was in response to the bankruptcy of Pay by Touch, a company operating a fingerprint scan system for use in grocery stores, gas stations, and school cafeterias.[293] As a result of the bankruptcy, Pay by Touch attempted to sell the biometric data it had collected.[294]

Even though an employer's original purpose for collecting health data may be for COVID-19 screening, employees should be informed of potential alternative uses this information may be put to.[295] This concept of notice is widely recognized as a "most fundamental principle" in privacy laws.[296] Adopting a statute that includes a provision emphasizing notice enables a more meaningful consent, which allows individuals a greater degree of agency and autonomy.[297]

Although the PHISH Act would require informed consent of the individual under normal circumstances, the EEOC has directed that an employer may take an employee's temperature "[b]ecause the CDC and state/local health authorities have acknowledged the community spread of COVID-19."[298] In order to avoid a potential conflict, the PHISH Act shall have an exception to the informed consent section,

292. *See* MARY MADDEN ET AL., PEW RSCH. CTR., AMERICANS' ATTITUDES ABOUT PRIVACY, SECURITY AND SURVEILLANCE 22 (2015), https://www.pewresearch.org/internet/2015/05/20/americans-views-about-data-collection-and-security.

293. Charles N. Insler, *How to Ride the Litigation Rollercoaster Driven by the Biometric Information Privacy Act*, 43 S. ILL. UNIV. L. J. 819, 819 (2019).

294. *See* Jay Schulman, *What You Need to Know About the Illinois Biometric Privacy Act (BIPA)*, RSM (Feb. 19, 2019), https://rsmus.com/what-we-do/services/risk-advisory/cybersecurity-data-privacy/what-you-need-to-know-about-the-illinois-biometric-privacy-act.html.

295. *See, e.g.*, Joyce E. Cutler, *How Can Patients Make Money Off Their Medical Data?*, BLOOMBERG L. (Jan. 29, 2019, 5:46 AM), https://news.bloomberglaw.com/pharma-and-life-sciences/how-can-patients-make-money-off-their-medical-data (discussing how some "companies have figured out . . . various ways to sell that data everyday.").

296. FED. TRADE COMM'N., PRIVACY ONLINE: A REPORT TO CONGRESS 7 (1998); *see* M. Ryan Calo, *Against Notice Skepticism in Privacy (and Elsewhere)*, 87 NOTRE DAME L. REV. 1027, 1028 (2013) ("there is a sense in which notice underpins law's basic legitimacy.").

297. *See* Brief of Amici Curiae the ACLU et al. in Support of Plaintiff-Appellant at 11, Rosenbach v. Six Flags Ent. Corp., 129 N.E.3d 1197, 1204 (Ill. 2019) (No. 123186).

298. *See* U.S. EQUAL EMP'T OPPORTUNITY COMM'N, *supra* note 83.

> In the event of a health crisis, during which, a local, state, or federal directive permits the capturing of health information, a written release and express consent is not required to capture health information. If a covered entity captures an individual's health information under this circumstance, they must still provide the individual with full knowledge of the risks involved and the alternatives.

Notably, capturing health information under this exception will not alter the entity's duties in adhering to the retention and destruction of that information.[299]

4. Retention and Destruction

Another key section of the PHISH Act will be the Act's provisions on the retention and destruction of data. The PHISH Act will adopt Washington's standard, stating that "a covered entity that possesses health information shall not retain the information longer than reasonably necessary to achieve the purpose for which it was originally captured."[300] For example, under this statute, an employer that captures health information for the purpose of monitoring their employees' health to ensure a sanitary workplace, would not be permitted to retain an employee's data upon that employee's termination. As the retention period ends, the PHISH Act will take language from Arkansas' PIPA statute on the means of destruction, providing that "a covered entity in possession of health information, shall at the conclusion of the retention period, destroy the information by shredding, erasing, or otherwise modifying the personal information in the records to make it unreadable or undecipherable through any means."[301] A strong destruction provision is important, as data that could be possibly retained runs the risk of leaving individuals without any information as to how their data will be used. [302]

The retention section will also address disclosure, providing that "no covered entity shall disclose a person's health information without their written consent." Disclosure schemes that require consent are an integral part of protecting privacy rights.[303] This goes hand in hand with the idea

299. *See infra* Section III.A.4.

300. *See* WASH. REV. CODE ANN. § 19.375.020 (West 2020).

301. *See* ARK. CODE ANN. § 4-110-104 (West 2020).

302. *See* Justin O. Kay, *The Illinois Biometric Information Privacy Act*, FAEGRE DRINKER 1 n.1 (June 20, 2017), https://www.faegredrinker.com/-/media/files/insights_db/publications/2017/06/j-kay-acc-bipa-article.pdf?la=en&hash=697774CBE9B509662FF140Fz55FFC960F9EE88F8C.

303. *See, e.g.*, Michael I. Meyerson, *The Cable Communications Policy Act of 1984: A Balancing Act on the Coaxial Wires*, 19 GA. L. REV. 543, 612 (1985) ("The basic elements of this framework limit the collection and disclosure of information and guarantee the subscribers' right both

that people have a right to know what information is being maintained about them.[304] There will also be an exception modeled after a section of CUBI, stating "a person's written consent is not needed for disclosure when the disclosure is made to a law enforcement agency for a law enforcement purpose in response to a warrant."[305]

As part of its retention scheme, the PHISH Act will borrow the "opt-out" provision from the CCPA, which will state that "individuals have the 'right to opt-out' of the sale or sharing of their health information."[306] The ability for an individual to have a say in the sharing of information has been considered a general principle of fair information process.[307] To this point, the Federal Trade Commission's Privacy Report to Congress gives examples of both internal and external uses an entity might have for an individual's information.[308]

The PHISH Act must also model itself after the various state laws that focus on notification of breach.[309] The section resembles New York's SHIELD Act and will read "any covered entity that possesses an individual's health information shall disclose any breach of the security of a system that contains the health information to any individual whose health information was or is reasonably believed to have been accessed or acquired by a person without valid authorization."[310] Notifying individuals ties into previously mentioned notions of notice and informed consent.[311] As early as 1973, an advisory committee within the U.S. Department of Health, Education, and Welfare recommended a Code of Fair Information Practice Principles which found that personal data

---

to know what information is being maintained and to insure its accuracy"). The Cable Communications Policy Act of 1984 allows cable companies to disclose information when there has been "positive consent," meaning it can be written or electronic but cannot be implied. *Id.* at 614.

304. *See* Brief of Amici Curiae the ACLU et al. in Support of Plaintiff-Appellant, *supra* note 297, at 14.

305. *See* TEX. BUS. & COM. CODE ANN. § 503.001(c)(1)(D) (West 2019); *see also* Meyerson, *supra* note 303, at 613-14 (law enforcement purposes being a reason for disclosure in the context of The Cable Communications Policy Act of 1984).

306. *See* CAL. CIV. CODE § 1798.120(b) (West 2020).

307. *See* FED. TRADE COMM'N., *supra* note 296, at 8.

308. *See id.* ("Such secondary uses can be internal, such as placing the consumer on the collecting company's mailing list in order to market additional products or promotions, or external, such as the transfer of information to third parties.").

309. *See generally State Data Breach Notification Laws*, FOLEY & LARDNER LLP (Aug. 15, 2021), https://www.foley.com/-/media/files/insights/publications/2021/08/21mc35506-data-breach-chart-0803021.pdf?la=en (comparing different state data breach notification laws).

310. *See* N.Y. GEN. BUS. LAW § 899-aa(2) (McKinney 2020).

311. *See* U.S. DEP'T OF HEALTH EDUC. & WELFARE, SEC'YS ADVISORY COMM. ON AUTOMATED PERS. DATA SYS., RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS XX (1973), https://www.justice.gov/opcl/docs/rec-com-rights.pdf.

record-keeping systems should not remain secret and that individuals must find out about their information being in a record and how it is used.[312]

5. Private Right of Action

Perhaps the most vital section of the PHISH Act will be the section granting individuals a private right of action. Being the only model in existing law, the provision would read as BIPA's does, "[a]ny person aggrieved by a violation of this Act shall have a right of action in a State circuit court or as a supplemental claim in federal district court against an offending party."[313] Generally, the American legal system relies upon ex post private enforcement as an important complement to ex ante public regulation.[314] In this case, providing a private remedy is beneficial in that it creates strong incentives for entities to implement fair information practices, while ensuring compensation to those harmed by the information's misuse.[315]

The requisite mental element for a violation of the PHISH Act shall be one of strict liability, borrowing language from CUBI, "[a] person who violates this section is subject to a civil penalty of not more than $25,000 for each violation."[316] Imposing strict liability on violators of the PHISH Act aims to serve the purpose of bringing employers' attention to the issue. Strict liability itself has been known to incentivize those who engage in ultrahazardous activities to "cut back on the scale of the activity . . . to slow its spread while more is learned about conducting it safely."[317]

*B. Alternatives to the PHISH Act*

An alternative to enacting the PHISH Act may be to amend HIPAA. Being that HIPPA is an existing statute, its federal character would see the most sweeping impact. Filling the gap of employer-collected information not falling under PHI[318] would remedy a substantial part of the problem that the PHISH Act seeks to address. HIPAA's Privacy Rule

312. *Id.*

313. 740 ILL. COMP. STAT. ANN. 14/20 (West 2020).

314. *See* Brief of Amici Curiae the ACLU et al.in Support of Plaintiff-Appellant, *supra* note 297, at 19.

315. *See* FED. TRADE COMM'N, *supra* note 296, at 11.

316. TEX. BUS. & COM. CODE ANN. § 503.001(d) (West 2019).

317. Danielle Keats Citron, *Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age*, 80 S. CAL. L. REV. 241, 266 (2007).

318. *See supra* Section I.D.

already provides an extensive scheme with provisions for disclosure, notice, and retention.[319] The Privacy Rule's general principles on these matters are to limit the circumstances in which PHI can be disclosed.[320] Permitted disclosures are generally limited to disclosures to the individual who is the subject of the information and for various "national priority purposes" that are related to proceedings or law enforcement activities.[321]

## CONCLUSION

In a society where a pandemic has the potential to significantly impact the world, working habits changed quickly to adapt to new conditions.[322] While individuals and companies can quickly implement new social distancing policies and health screening regimes,[323] our lawmaking entities tend to suffer from the "pacing problem," when legal responsiveness lags behind modern technologies.[324] This problem occurs because legislatures lack the resources to adequately anticipate, understand, and act on emerging issues.[325]

New technologies such as temperature scanning tablets[326] and new practices such as health screening questionnaires,[327] bring about the need for a safer work environment. While innovation can be exciting, technology that appears to be a "knight in shining armor" should be cautiously adopted when there's risk that data collected for one purpose could get co-opted and employed for a different purpose.[328] Data collected from health screenings can be used to make a multitude of inferences, including stress level, pregnancy, heart conditions, and the potential healthcare costs to an employer.[329] Employers may choose to keep COVID-19 screening practices in place after the pandemic subsides,

319. *See* U.S. DEP'T OF HEALTH & HUM. SERVS., OFF. FOR CIV. RTS. SUMMARY OF THE HIPAA PRIVACY RULE 1 (May 2003).

320. *See id.* at 4.

321. *See id.* at 4-8.

322. *See* Brynjolfsson et al., *supra* note 5, at 3-4 (finding that as of May 2020 over thirty-five percent of those employed pre-COVID-19 switched from commuting to working at home).

323. *See* Aridi, *supra* note 7.

324. *See* Marci Harris, *Here's What Happens When Tech Outpaces Government*, APOLITICAL (Sept. 12, 2019), https://apolitical.co/en/solution_article/heres-what-happens-when-tech-outpaces-government.

325. *See id.*

326. *See* TAURI, *supra* note 17.

327. *See* Littler, *supra* note 102.

328. *See* Jennifer Daskal, *Good Health and Good Privacy Go Hand-in-Hand*, 11 J. NAT. SEC. & POL'Y 131, 153 (2020).

329. *See* STANLEY, *supra* note 16, at 5; *see* Santos-Longhurst, *supra* note 273.

which could potentially lead to employers misusing or making ultimate employment decisions based on this data.[330]

Existing rules on the protection of health information are adequate in their protections, but their scope of application leaves a gap when the health information is collected by employers instead of health care providers.[331] On the other hand, laws such as BIPA which extend to employers were passed with an intention more towards identity theft than protecting health information.[332] Even without a new statute, employers that implement devices for health screening, that also capture biometric information, may trigger privacy concerns and subsequent legal action in accordance with existing biometric data privacy laws.[333]

In light of these issues, states should adopt the proposed PHISH Act, recognizing the protection of data that employees and all individuals alike are entitled to. A general right to privacy has been a hallmark of the Constitution, the intrusion of which can only be justified in special circumstances.[334] In the more specified context of data privacy, courts of law have held that a right exists, so fundamental that a mere statutory violation constitutes a cognizable injury, sufficient to sustain Article III standing.[335] Taking these notions into consideration, passing the PHISH Act would serve a great purpose in protecting individuals and their right to privacy, in a time when mandatory health screenings are becoming a necessary condition to engage in daily life.[336]

*Andrew Schuman**

330. *See* Brown, *supra* note 272, at 274.
331. *See supra* Section I.D.
332. *See* 740 ILL. COMP. STAT. ANN. 14/5(c) (West 2020).
333. *See* Wood, *supra* note 196.
334. *See supra* Section I.A.
335. *See supra* Section II.B.1.
336. *See* Daskal, *supra* note 328, at 142.

* Andrew Schuman is a J.D. candidate at the Maurice A. Deane School of Law at Hofstra University, where he anticipates graduation in May of 2022. Mr. Schuman is the Managing Editor of Articles of the Hofstra Labor & Employment Law Journal. Mr. Schuman would like to dedicate his note to the Staff and Managing Board of Volume 39 of the *Hofstra Labor & Employment Law Journal*, for their excellent work during the publication process. Mr. Schuman would like to thank his Notes & Comments Editor, Melissa Yurisak, for all of her help providing feedback on the note and answering questions. Mr. Schuman would also like to thank his friends for always being there, in both good times and stressful times. Finally, Mr. Schuman would like to thank his parents, Michael and Stacie, for all of their love and support throughout law school.