A Healthy Mistrust: Curbing Biometric Data Misuse in the Workplace

Elizabeth A. Brown*

23 STAN. TECH. L. REV. 252 (2020)

ABSTRACT

This article addresses the best ways to mitigate the various privacy and discrimination risks inherent in the use of biometric monitoring in the workplace. While the federal and state regulation of monitoring workers is in its infancy, biometric monitoring itself is expanding rapidly. Innovations in wearables, rising health care costs, personalized medicine and the use of health data clearinghouses are among the factors fueling this expansion. This article analyzes the harms of misusing biometric and health data in the workplace as well as the limitations of current regulatory schemes, and offers three possible ways to curb those harms, varying in degrees of interventionism.

* Associate Professor, Department of Law, Taxation and Financial Planning, Bentley University; A.B. Harvard University, J.D., Harvard Law School. I thank the Bentley University Health Thought Leadership Network for their research support, Leora Eisenstadt for her invaluable insights and helpful feedback during the development of this article and Amanda Pine for her editorial contributions.

TABLE OF CONTENTS

I. INTRODUCTION

Increasingly, employers are using biometric monitors and wearable devices to gather data about their workforce. Employers now use facial

recognition, heart monitoring, eyeball tracking, and other measures in an effort to improve productivity and reduce health insurance costs over time. To what extent should employers be allowed to evaluate or fire workers based on their heart rate, sleeplessness, fertility, or other health data these monitors help them gather? In the wake of the coronavirus pandemic, the benefits of monitoring workers' health have come into sharp relief, as health monitoring practices may help determine whether a workplace can reopen at all. One hidden cost of health-related biometric data collection in the workplace, however, is the potential mismeasurement of workers due to inaccurate data and biased algorithms. Another is the possibility of data-driven adverse consequences, unchecked by federal or state legislation or by worker objection. Such consequences undermine the trust relationship inherent in and unique to the employer-employee relationship, yet trends in wearables designed for the workplace, health data clearinghouses, personalized medicine and insurers' use of monitoring tends to entrench these practices. As companies deploy increasingly sophisticated methods of collecting biometric and health data, we must ask how companies can best balance their need to reduce skyrocketing health insurance costs with the potential harms of adverse employment decisions that could result from the expansive data that they can now collect.

This article analyzes the harms of misusing biometric and health data in the workplace and offers three possible ways to curb those harms, varying in scope. The least interventionist option would be to broaden the scope of planned federal consumer data privacy legislation to encompass employee data privacy protection as well. An alternative regulatory option would be to amend the Affordable Care Act (ACA) to clarify that neither employers nor their business associates can collect biometric and health-related data as part of even "voluntary" workplace wellness programs. The most radical and interventionist solution would be to decouple health insurance from employment altogether. The first and second options could be combined to provide more comprehensive protection against misuse of workers' biometric data. The third option, while the

most difficult to put in place, might reduce much of the incentive for biometric data collection to begin with. Whether we choose a broad or narrow solution, involving one or more of these options, we should make an informed decision based on full knowledge of the risks involved rather than letting the biometric monitoring market chart the course.

In Part II, this article explores recent advances in both monitoring technology and personalized medicine. These increase the range and accessibility of employees' biometric and health data now available to employers. It also explores the ways in which employers might put that data to use. Part III examines the ways in which such data might be misused to the disadvantage of both workers and employers. It assesses the likelihood of such misuse and the consequences both to surveilling employers and to the surveilled employees. Part IV describes the ways in which current laws fail to protect against such misuse. Part V suggests three potential regulatory and legal reforms that could protect effectively and efficiently against the consequences of such misuse and which are practical in light of ongoing legal reforms in the data privacy sphere. Part VI concludes.

II. EMPLOYERS COLLECT HEALTH DATA AT SKYROCKETING RATES.

There is a special relationship between employers and workers that goes to the heart of most people's waking lives. The decisions employers make have profound impacts on workers, their families, and their economic futures. Those futures, and the future of the workplace in general, may be determined as much by what workers wear as with what they do. In January 2019, at CES, the world's biggest technology show, hundreds of companies displayed and discussed the newest forms of wearables coming to the market for potential use in the workplace.[1] These include not only fitness bands and smart watches with an ever-increasing range of tracking functions, but also new wearables such as temporary tattoos

1. The reference to CES 2019 rather than CES 2020 is due to the author's personal attendance at the 2019 convention.

designed to track sun exposure,[2] smart glasses that integrate virtual assistant technologies,[3] smart shoes that provide early warnings of diabetes-related symptoms,[4] and sensor-enhanced clothing designed to increase productivity.[5]

Employers are embracing many of these technologies in workplace wellness programs. One in five large employers reported using some kind of biometric monitoring in their wellness programs in 2018, an increase of 50% compared with just one year earlier.[6] The increased data available through such measurement opens the door to a whole new world of employer inference. Employers who have access to the data these new wearables can provide might be curious to know how well their workers are sleeping, for example, or when their blood pressure is spiking. These employers might infer that workers experiencing regular spikes in their blood pressure are experiencing too much stress, which may be undesirable and lead to lower productivity.

Diana Diller's experience provides a powerful example of potentially harmful employer inference. Diller, an event planner for a video game company in Los Angeles, used a popular app called Ovia to help track her pregnancy.[7] Every night, she recorded data about how she felt, what medications she had taken, and her level of sex drive.[8] When her daughter was born, she charted the baby's first medical data using the Ovia app before she left the recovery room.[9] Her employer, however, was also checking this data, tracking its employees' efforts to conceive, the progression of their pregnancies and their well-being during their first

2. LOGICINK, https://perma.cc/8VJ9-5Q6Z (last visited May 14, 2020).

3. GLASS, https://perma.cc/78QW-5EYH (last visited May 14, 2020).

4. BONBOUTON, https://perma.cc/7YL5-F4A2 (last visited May 14, 2020).

5. SEISMIC, https://perma.cc/PKT4-TQML (last visited May 14, 2020).

6. KAISER FAMILY FOUND., EMPLOYER HEALTH BENEFITS 2018 ANNUAL SURVEY 198 (Oct. 3, 2018), https://perma.cc/4Y2Z-V5PV.

7. Drew Harwell, *Is Your Pregnancy App Sharing Your Intimate Data with Your Boss?*, WASH. POST (Apr. 10, 2019) https://perma.cc/R428-U8BW.

8. *Id.*

9. *Id.*

months of motherhood.[10] Having access to this data allowed Diller's employer to determine how many of its employees had high-risk pregnancies or premature deliveries, when they planned to return to work, and what medical questions they researched.[11]

Diller had allowed her employer to access that pregnancy-related information as part of a workplace wellness program, in which she was paid the equivalent of $1 a day in gift cards in exchange for granting that access.[12] Her employer paid Ovia Health, the developer of the Ovia app, to get access to aggregated information about the employees using Ovia. Ovia Health had promised to de-identify the data so that it would be more difficult to determine which inputs belonged to specific employees.[13]

While Ovia markets itself as a resource to help women navigate pregnancy, it also supplies employers with data that can be used for assessment in unregulated and potentially harmful ways. Diller's employer, for example, could have inferred which employees were likely to rack up greater health insurance costs because certain aspects of their pregnancies correlated with a higher likelihood of more expensive treatments. It may then have been able to use that information, for example, by retaining employees who are likely to be less expensive to insure in the long run. That sort of employment decision is not prohibited by any federal law, but it poses significant risks for workers and undermines the long-term interests both of individual firms and the economy in general.

While data privacy concerns are the focus of much recent scholarship,[14] the potential misuse of biometric health monitoring in the workplace is unique because of both the trust relationships inherent in the

10. *Id.*
11. *Id.*
12. *Id.*
13. *Id.*
14. *See, e.g.*, Kimberly A. Houser & W. Gregory Voss, *GDPR: The End of Google and Facebook or a New Paradigm in Data Privacy?*, 25 RICH. J.L. & TECH. 1 (2018); Jay P. Kesan & Carol M. Hayes, *Liability for Data Injuries*, 2019 U. ILL. L. REV. 295; Laura Palk & Krishnamurty Muralidhar, *A Free Ride: Data Brokers' Rent-Seeking Behavior and the Future of Data Inequality*, 20 VAND. J. ENT. & TECH. L. 779 (2018).

workplace and the immutability of biometric data. Biometric and health data monitoring is also unique because it is uniquely unalterable. Unlike social security numbers, which can be changed, or social media postings, which can be deleted, biometric data such as a facial scan or a fingerprint is nearly impossible to change. While some kinds of physical activity monitoring data can be faked,[15] other kinds of health data that is more continuously monitored, such as blood pressure or sleep patterns, are relatively difficult to fabricate on an ongoing basis.

A. Workplace Wellness Programs Facilitate Biometric Data Collection.

Most employers monitor worker health data through workplace wellness programs like the one in which Diana Diller was enrolled. According to the Kaiser Family Foundation, 82% of large firms and 53% of small firms offer some kind of workplace wellness program.[16] These programs commonly incentivize workers to stop or reduce smoking, join a gym, exercise more often, eat healthier foods, try meditation programs, or lose weight.[17] Workplace wellness are, according to one estimate, an $8 billion industry in the United States.[18]

Employers use workplace wellness programs for at least two reasons. First, there is a widespread belief that healthy workers are more productive, and productivity benefits the business.[19] This belief is bolstered by research including one recent study showing that workers who improved

15. Jen Wieczner, *Fitbit Users Are Finding Creative Ways to Cheat*, FORTUNE (June 10, 2016, 1:40 PM), https://perma.cc/8TRE-GH5Y.

16. KAISER FAMILY FOUND., *supra* note 6, at 15.

17. *Id.*

18. Julie Appleby, *How Well Do Workplace Wellness Programs Work?*, NPR: SHOTS (Apr. 16, 2019, 11:31 AM), https://perma.cc/B5QM-8PUK.

19. Lauren Weber, *Wellness Programs Pay Off, Study Says*, WALL ST. J., (Aug. 9, 2017, 3:14 PM), https://perma.cc/DZ3X-XT2D; Julie Appleby, *Workplace Wellness Plans Offer Big Incentives, But May Cost Your Privacy*, NPR: SHOTS (Sept. 22, 2018, 7:02 AM), https://perma.cc/6GLK-FELC.

their health by eating better, exercising more and reducing their stress levels increased their productivity by approximately 10%.[20]

More important is the belief that high rates of participation in workplace wellness programs will result in lower health insurance costs for the business in the future.[21] Although there is some evidence to suggest that employees who take part in workplace wellness programs do not experience the kind of long-lasting health benefits that would lower such costs as a result of the programs,[22] these programs are still common.[23] This ubiquity is due largely to the skyrocketing cost of health insurance for employers who must provide it. Health insurance is an enormous expense for employers in the United States, and the costs are rising. In 2018, analysts reported that annual premiums for employer-sponsored family health coverage averaged out to $19,616, an increase of 5% over 2017, with workers paying an average of $5,547 toward that cost.[24]

Workplace wellness programs often use a carrot and stick approach to maximize compliance. Until recently, the sizes of the carrots and sticks were limited by federal law. Under the Affordable Care Act (ACA), employers are allowed to provide financial incentives to employees in connection with "voluntary" workplace wellness programs.[25] In May 2016, the Equal Employment Opportunity Commission (EEOC) provided

20. Timothy Gubler et al., *Doing Well by Making Well: The Impact of Corporate Wellness Programs on Employee Productivity*, 64 MGMT. SCI. 4967, 4967 (2018).

21. *Id.*

22. *See, e.g.*, Zirui Song & Katherine Baicker, *Effect of a Workplace Wellness Program on Employee Health and Economic Outcomes: A Randomized Clinical Trial*, 321 JAMA 1491, 1492 (2019) (finding that employees exposed to wellness programs experienced "no significant effects on clinical measures of health, health care spending and utilization, or employment outcomes after 18 months" compared with a control group); *see also* Damon Jones et al., *What Do Workplace Wellness Programs Do? Evidence from the Illinois Workplace Wellness Study* (Nat'l Bureau of Econ. Research, Working Paper No. 24229, 2018), https://perma.cc/7P95-RDYW (finding no "significant causal effects of treatment on total medical expenditures, health behaviors, employee productivity, or self-reported health status in the first year" of a comprehensive workplace wellness program).

23. KAISER FAMILY FOUND., *supra* note 6, at 15.

24. *Id.* at 9.

25. Regulations to Implement the Equal Employment Opportunity Provisions of the Americans With Disabilities Act, 29 C.F.R. § 1630 (2016).

guidance that employers could offer incentives or penalties amounting to a maximum of 30% of the employee's share of the group health plan coverage fee without violating the Americans with Disabilities Act (ADA), while maintaining the voluntariness of the plan.[26] On the same day, the EEOC provided similar guidance with regard to the Genetic Information Nondiscrimination Act (GINA).[27] Under these rules, if an employee's health care costs were $1,000 as part of a group coverage plan, the employer could offer a bonus of up to $300 for participating in a workplace wellness program or penalize the employee up to $300 for failing to participate.

In practice, these incentives might have taken the form of some reward, like a gift card, for employees who met certain activity goals or recorded their caloric intake for some period of time. Health insurers also commonly provide incentives for behaviors that are associated with improved health. For example, Harvard Pilgrim Health Care reimburses part of the cost of a fitness center membership every year.[28] These workplace wellness programs often reward the use of wearable devices such as Apple Watches or Fitbits[29] that track employees' biometric data and physical activity.[30] Wellness programs that include biometric screenings or ask participants to complete health risk assessments are subject to the ADA.[31] They may also be subject to GINA, depending on the kind of data they collect.[32]

---

26. *Id.* § 1630.14(d)(3) (2016); *see* Elizabeth A. Brown, *Workplace Wellness: Social Injustice*, 20 N.Y.U. J. LEGIS. & PUB. POL'Y 191, 218–20 (2017) (providing a more thorough description of this coverage).

27. Genetic Information Nondiscrimination Act, 29 C.F.R. § 1635.8(b)(2) (2016).

28. *Fitness Reimbursement*, HARV. PILGRIM HEALTH CARE, https://perma.cc/Y8ZV-5RY7 (last visited May 14, 2020).

29. In November 2019, Fitbit announced that Google intended to purchase the company for approximately $2.1 billion. *Fitbit to be Acquired by Google*, FITBIT (Nov. 1, 2019), https://perma.cc/Y7N2-MX2N.

30. *See, e.g.*, Steve Aldana, *50 Employee Wellness Program Examples for Any Budget*, WELLSTEPS (Mar. 24, 2020), https://perma.cc/GK9R-GGD7.

31. Lisa Klinger, *Wellness Program Incentive Amounts for 2019: What to Do?*, LEAVITT GROUP (July 31, 2018, 6:41 PM), https://perma.cc/9WFH-2HZX.

32. *Id.*

As of January 1, 2019, however, the 30% incentive rule was invalidated, subject to a December 2017 ruling in the *AARP v. EEOC* case by the District Court for the District of Columbia[33] In that case, the AARP had challenged the 30% incentive rules as being coercive in that they made health insurance substantially more expensive for workers who did not want to submit to health screening and other elements of workplace wellness programs that might compromise their privacy.[34] The 30% incentive/penalty allowance, the AARP argued, meant that such programs could not be truly voluntary, as the ACA initially intended them to be.[35] The district court decided that vacating the incentive guidance as of January 2019 would be the least disruptive course even though the EEOC had no plans to finalize new rules before 2021. The decision "strongly encouraged" the EEOC to "move up its deadline for issuing the notice of proposed rulemaking" to ensure that new rules could be put in place "well before the current estimate of sometime in 2021."[36] As of this writing, the EEOC has not issued a notice of proposed rulemaking in this area.

As a result of that December 2017 ruling, in December 2018 the EEOC removed both the workplace wellness incentive rules relating to the ADA and to GINA that the Court had vacated in *AARP v. EEOC*. As of January 2019, employers had no guidance from the EEOC as to what kinds of incentives or penalties, if any, might be acceptable in a "voluntary" workplace wellness program. This caused great uncertainty among employers offering these programs, requiring them to "decide what level of risk they are comfortable with," according to one industry analyst.[37] The most conservative approach would be to offer no incentives or penalties, and the riskiest approach would be to offer an incentive or penalty equal to or

33. AARP v. EEOC, 292 F. Supp. 3d 238 (D.D.C. 2017).

34. *Id.*

35. Compl. ¶¶ 76-78, 86-88, AARP v. EEOC, 292 F. Supp. 3d 238 (D.D.C. 2017) (No. 16-cv-2113).

36. AARP, 292 F. Supp. 3d at 245.

37. Klinger, *supra* note 31.

greater than 30% of the employee's cost of the group health plan coverage.[38]

The use of advanced technology in workplace wellness programs is on the rise despite this lack of clarity. In 2018, 21% of large employers used biometric monitoring to collect information about their workers, a 50% increase over 2017 when only 14% of large employers used such monitoring. [39] The sharp increase is likely to continue for several reasons, each of which is discussed below.

B. Biometric and Health Tracking Is the New Normal.

Biometric tracking is becoming normal. Apple, for example, offers Face ID as a security option on several iPhone models. This requires a user to "enroll" her face to set up the authentication system, although Apple says that the recognition data is not uploaded to the cloud.[40] Facial recognition is being used to secure payments in stores and online in China.[41] In the near future, we can expect to see facial recognition technology adopted in hotel concierge systems, the delivery of health care to patients with Alzheimer's and other memory impairments, and in school security systems, among other applications.[42] Facial recognition is already so ubiquitous that one in two American adults are already in a law

38. *Id.*

39. KAISER FAMILY FOUND., *supra* note 6, at 198.

40. *About Face ID Advanced Technology*, APPLE (Mar. 2, 2020), https://perma.cc/HH9X-KX6W.

41. Yusho Cho, *Alibaba Brings Face-Scan Payments to Tablet for Shopkeepers*, NIKKEI ASIAN REV. (Dec. 14, 2018), https://perma.cc/EN6L-HJCA.

42. Michael Xie, *The Future of Biometric Facial Recognition*, FORBES (Sept. 19, 2018, 8:00 AM), https://perma.cc/53RA-YURU.

enforcement facial recognition database.[43] In some communities, however, there has been a backlash against widespread facial recognition usage.[44]

Despite such concerns, many employers put these technologies to use in order to keep track of various aspects of workforce behavior. Alibaba uses facial identification to recognize its employees[45] and sells "Face ID Time Attendance Systems" on its website.[46] Because employees are increasingly accustomed to being scanned by their phones, they may not see workplace scans as unusually intrusive. They may be more accepting of these screenings in the workplace than they might have been five or ten years ago.

C. New Wearables Help Employers Collect Biometric and Health Data.

Workers are also more accustomed to wearables, many of which employers can leverage for data. According to one study, the global market for wearable technology grew nearly 30% in 2018.[47] The success of the Apple Watch is a key driver of this industry growth.[48] Another study shows that the market has grown from eighty-four million units shipped in 2015 to a projection of 245 million units shipped in 2019.[49] Analysts predict that greater adoption of wearables different from fitness bands like the Fitbit, including "smart hearables and smart shoes," will lead to

43. Sahil Chinoy, *We Built an 'Unbelievable' (But Legal) Facial Recognition Machine*, N.Y. TIMES (Apr. 16, 2019), https://perma.cc/XT2C-URLS (noting too that the authors identified a college professor by collecting public images using a system that cost them $60 to build).

44. Rachel Metz, *Beyond San Francisco, More Cities Are Saying No to Facial Recognition*, CNN (July 17, 2019), https://perma.cc/2WHQ-UVD8.

45. Yiting Sun, *Meet the Company That's Using Face Recognition to Reshape China's Tech Scene*, MIT TECH. REV. (Aug. 11, 2017), https://perma.cc/Y48P-SMZ5.

46. *Secukey Facial Recognition Device Face ID Time Attendance System Time Clock*, ALIBABA, https://perma.cc/43PS-4K3D (last visited May 15, 2020).

47. *Optimistic Outlook for Wearables: 260 Million Unit Sales in 2023*, CCS INSIGHT (Mar. 20, 2019), https://perma.cc/TM9G-E8CT.

48. *Success of Apple Watch Means More Growth in Sales of Wearable Technology*, CCS INSIGHT (Oct. 23, 2018), https://perma.cc/RV2R-SG25.

49. *Wearables Market to be Worth $25 Billion by 2019*, CCS INSIGHT, https://perma.cc/3P9E-V3A6 (last visited May 15, 2020).

sales of 260 million units in 2023, resulting in a market worth almost $30 billion.[50]

The Apple Watch is a perfect example of the ease with which people have accepted the presence of wearable technology. It allows the user to access texts, emails, and other data that she would previously have used her phone to collect. The watch has "powerful sensors" that collect data from the user as well, notifying her of unusually high or low heart rates and irregular rhythms that may suggest atrial fibrillation (AFib), and the sensors may even be able to take an electrocardiogram reading.[51] Similarly, the Omron Heartguide looks like a smartwatch but has a built-in inflatable blood pressure cuff that tracks the wearer's blood pressure along with activity levels, pulse rate, and how well and for how long the wearer is sleeping.[52] It is easy to imagine an employer's interest in gathering such data about its workforce and using that data to make decisions about individual workers.

While employers have been using wearables for some time, wearable makers are now catering more expressly to their needs. Fitbit, for example, appeals directly to employers to "invest in healthy behavior change" and help those many employees who "struggle to get and stay healthy, which can drive higher rates of chronic conditions and disease."[53] Underscoring the expense of health insurance, it notes that "the associated healthcare costs – especially for those employees living with or at risk for chronic disease – are unsustainable."[54] Its dedicated corporate health platform, Fitbit Care, promises to "get employees moving" through devices and apps.[55]

---

50. *Optimistic Outlook for Wearables*, *supra* note 47.

51. *Apple Watch: Helping Your Patients Identify Early Warning Signs*, APPLE https://perma.cc/J3DZ-7LH3 (last visited May 15, 2020).

52. *HeartGuide*, OMRON, https://perma.cc/W6BT-GH39 (last visited May 15, 2020).

53. *Invest in Healthy Behavior Change*, FITBIT, https://perma.cc/QEX2-P3AT (last visited May 15, 2020).

54. *Id.*

55. *Engage, Inspire and Drive Healthy Habits*, FITBIT, https://perma.cc/Q8D2-M7J2 (last visited May 15, 2020).

Fitbit facilitates the entire employer monitoring process. The Fitbit Care division offers employers a "customized, online storefront" where employees can choose an incentive for getting a tracking device.[56] The employee is directed to join the employer's workplace wellness program while setting up their device.[57] Then the reporting begins. Fitbit Care's program dashboard provides the employer with reports on data collected from employees' devices and helps the employer motivate employees directly.[58] The dashboard helps the employer see "[c]ontinuous program participation levels and engagement data," "[a]ctivity level trends" and "[c]hallenge results and activity level changes."[59] Some of this activity may be generalized to groups of employees, as employers can monitor "group reporting on steps, floors climbed, active minutes and distance."[60] Other data is, however, collected and transmitted at the individual employee level, as Fitbit promises that both "individual and group data is also available for export."[61]

Fitbit also developed special models of their devices that workers can only get via their employers. The Fitbit Inspire and Inspire HR,[62] introduced in early 2019, were first described as only being available through employers and health plans as part of workplace wellness programs.[63] In announcing them, Fitbit's CEO noted that its revenue was increasingly linked with its corporate customers, and that 6.8 million people were in wellness programs incorporating Fitbit devices.[64]

---

56. *Id.* The legal limits on such incentives are discussed in more detail in Part IV.

57. *Id.*

58. *Id.*

59. *Id.*

60. *Id.*

61. *Id.*

62. HR apparently stands for heart rate rather than human resources in this instance. *See* Aaron Mamit, *Fitbit's New Fitness Tracker Is Its Cheapest, but You Can't Buy It Yourself*, DIGITAL TRENDS (Feb. 10, 2019), https://perma.cc/759X-3TRM (noting that the HR model adds 24/7 heart rate tracking and other features to the basic Inspire model).

63. Christina Farr, *Fitbit Has a New Health Tracker, but You Can Only Get It Through Your Employer or Insurer*, CNBC (Feb. 8, 2019, 4:32 PM EST), https://perma.cc/33QY-4Z8N.

64. *Id.*

Employers are not limited to wearables worn next to the skin. They can also collect data through a new form of sensor-loaded identification badges. Humanyze, a Boston-based company, sells ID badges that track employees' proximity throughout the day to other employees and the number of conversations employees have with each other.[65] Hitachi requires some manufacturing employees to wear special glasses and armbands that track their movements as well as sensor-equipped badges that collect behavioral data fifty times a second.[66] The modes employers can use to gather biometric and health data from their workers is likely to increase in scope, as are the data types they can collect as a result.

D. Female Employees Are Especially Measurable.

Some of the newly measurable data employers might access correlates with women's reproductive systems. A new range of monitors make it possible for employers to track women specifically with regard to their reproductive cycles, pregnancy and childbirth. The growth of "femtech" involves getting and storing such data largely through wearable devices.[67] The femtech market is expected to grow dramatically and could be worth $50 billion by 2025.[68]

Femtech monitoring takes many forms. Some newer Fitbit models can track data relating to a woman's period, along with other health data.[69] Similarly, the Ava bracelet tracks fertility and predicts ovulation

65. *Privacy by Design*, HUMANYZE, https://perma.cc/3EJQ-RF6J (last visited May 17, 2020) (explaining in FAQs that the Humanyze badge "has sensors to measure whether the participant is in motion or still, their proximity to other badged users and beacons, whether the participant is talking or not talking, and the frequency and duration of in-person interactions").

66. Ellyn Shook et al., *Putting Trust to Work*, ACCENTURE 10, https://perma.cc/P3S3-ZV8Z (last visited May 20, 2020).

67. Grace Gould, *FemTech: The Best New Gadgets in Women's Health*, EVENING STANDARD (Apr. 12, 2019, 4:22 PM), https://perma.cc/BS4C-L42V.

68. *Femtech: Digital Revolution in Women's Health*, FROST & SULLIVAN, https://perma.cc/8KHY-RPP3 (last visited May 20, 2020).

69. Danielle Kosecki, *One of Your Most Requested Features Is Here! Introducing Female Health Tracking*, FITBIT NEWS (May 20, 2018), https://perma.cc/ZPQ8-9KKY.

based on the physiological parameters it monitors.[70] It does so by detecting key changes in the wearer including skin temperature, heart rate, respiratory rate and skin perfusion.[71] Its manufacturer claims that it can detect the wearer's fertile window with 90% accuracy.[72] The Clue app is a popular platform used to track periods, fertility and the likelihood of developing premenstrual syndrome (PMS).[73]

Other wearables track the wellbeing of fetuses. The Owlet band, for example, can provide a range of information about fetuses from twenty-four weeks to the end of term.[74] Pregnant women can wear these Owlet bands, embedded with thin sensors in the fabric, to get information on how the number of kicks, contractions, fetal heartbeat, and other kinds of data without going to their obstetricians.[75]

It is hard to think of any good reason for why employers would want to know when a female employee has her period, when she may have PMS, or when she tracks her fertility. Indeed, most women would consider that kind of information deeply private. Although these employees may have agreed to the terms and conditions of these monitoring programs, opting out of them may be virtually impossible in practice, so the programs may not be truly voluntary. This is especially true for lower income workers.[76] In addition, some analysts predict that monitoring programs may become mandatory in future workplaces, further minimizing the role of consent.[77] It is easy to imagine the negative consequences of employer access to that data. Pregnancy discrimination is common, especially in the kind of large companies which might be most

70. AVA, https://perma.cc/AL5M-K9PG (last visited May 17, 2020).

71. Cathy Russey, *Ava Bracelet Can Detect Changes in Physiology and Predict Fertility: Study*, WEARABLE TECH. (Apr. 19, 2019), https://perma.cc/F58D-DWF3.

72. *Id.*

73. *The App to Track Your Period, and So Much More*, CLUE, https://perma.cc/786M-UUGX (last visited May 10, 2019).

74. *Pregnancy Band FAQs*, OWLET, https://perma.cc/CW9U-DS9T (last visited April 28, 2020).

75. *Id.*

76. Brown, *supra* note 26, at 212.

77. Erika J. Nash, *Notice and Consent: A Healthy Balance Between Privacy and Innovation for Wearables*, 33 BYU J. PUB. L. 197, 213 (2019).

likely to adopt monitoring programs, despite the fact that it is illegal.[78] Employers who consciously or unconsciously believe in certain stereotypes about women, including the beliefs that women who are menstruating are distracted or incompetent, that women who are trying to get pregnant are poor candidates for investment and promotion, or that mothers are less committed to their work than fathers, could use this data to bolster those prejudices.

The new remote trackability of women's reproductive functions grants employers access to additional information that they might be able to use against women. An employer, for example, might assume that a woman who is tracking her fertility is more likely to become pregnant in coming years. An employer who holds conservative views might therefore perceive her as less committed to her career. A management consulting firm might think twice about sending a woman experiencing bouts of severe nausea, as is commonly associated with the first two trimesters of pregnancy, on a demanding business trip that might exacerbate her symptoms.

If employers can tap into this data stream along with other biometric data, they can now evaluate and compare performance among women taking into account a level of detail about their most intimate body functions that has never before been accessible to their employers. It is unlikely that existing laws would protect women against the misuse of this data, as explained in Part IV.

E. Health Insurers and Data Aggregators Facilitate Biometric Data Collection.

Another trend enabling employers to collect more health data is the increasing interest health insurers are showing in such data. Some insurance now requires monitoring. John Hancock, one of the largest life insurers in the United States, announced in late 2018 that it intended to sell

78. Natalie Kitroeff & Jessica Silver-Greenberg, *Pregnancy Discrimination Is Rampant Inside America's Biggest Companies*, N.Y. TIMES (Feb. 8, 2019), https://perma.cc/HV3Z-W27Y.

only interactive policies that track fitness and health data through wearable devices and smartphones.[79] These interactive policies offer special discounts for reaching certain activity targets.[80] Wearing trackers may become a precondition for all life insurance policies in coming years. New York already allows life insurers to use social media data in setting premium rates for applicants in some circumstances,[81] so using health data may not be much of a stretch.[82]

Employers who offer health insurance may now partner in data collection with those insurers, since many of them are now making it easier for employers to offer wellness programs that include various forms of biometric data collection. In August 2018, the Blue Cross Blue Shield Association (BCBSA) announced that it was partnering with Fitbit in order to make Fitbit activity trackers more affordable to insured workers and their beneficiaries.[83] Ominously, BCBSA called this new discount and promotion the initiative the "Blue365 program," implying that the plan might track information from users 365 days a year.[84] Mark Talluto, BCBSA's vice president of strategy and analytics, noted that the partnership would "bring personalized health and wellbeing to the next level."[85]

One insurance industry group, the National Association of Insurance Commissioners (NAIC), admits that insurers and employers are using the data from wearables to contain health insurance costs. NAIC staff actively work with startups and technology companies to help them develop new ways to use data from these wearables as "the competitive

79. Suzanne Barlyn, *Strap on the Fitbit: John Hancock to Sell Only Interactive Life Insurance*, REUTERS (Sept. 19, 2018, 7:11 AM), https://perma.cc/U8WN-DRC9.

80. *Id.*

81. Leslie Scism, *New York Insurers Can Evaluate Your Social Media Use—If They Can Prove Why It's Needed*, WALL ST. J. (Jan. 30, 2019, 9:00 AM EST), https://perma.cc/KX8X-PKTB.

82. Sarah Jeong, *Insurers Want to Know How Many Steps You Took Today*, N.Y. TIMES (Apr. 10, 2019), https://perma.cc/G3H3-ADNF.

83. *Blue Cross Blue Shield Association Partners with Fitbit to Deliver Special Offer on Fitbit Devices to over 60 Million Members*, BLUE CROSS BLUE SHIELD (Aug. 7, 2018), https://perma.cc/FLR2-8RLA.

84. *Id.*

85. *Id.*

advantage."[86] It does note that insurance regulators are wary of how data collection from such wearables might lead to "cherry picking" from among the healthiest beneficiaries.[87] When John Hancock announced that it would make all of its life insurance policies interactive, some wondered about the extent to which collected data might be used to select for or against certain potential customers.[88] To the extent that regulations require the insurance industry to justify its reasons for rate increases or policy changes, there may be a need for such regulations to be revised and/or enforced to protect the privacy of the insureds' health data.

Another development that makes it easier for employers to collect biometric and health data from workers is the rise of companies that act as intermediaries between employers and workers to centralize, filter and manage such data collection. One such company, Castlight, offers a customized worker interface that "securely analyzes claims data, HRA data, biometric data, and more to develop the most accurate picture possible" for its customers, the employers.[89] The interface sends notifications to users that are intended to "motivate [them] to participate in health programs, optimize care utilization, and improve their daily habits." Its "digital health ecosystem" offers employers the option to connect a range of health vendors through a single platform.[90] This centralizes employers' ability to track, or help, workers on tobacco cessation, weight management, mental health, "condition management," heart health, musculoskeletal health, weight coaching, maternal health, "resilience," nutrition, sleep and "lifestyle tracking."[91] While this system may benefit both em-

86. Diana Manos, *Health Plans Take Steps to Study Use of Fitness Wearables, Data,* DIGITAL INS. (Mar. 4. 2019, 5:29 AM EST), https://perma.cc/9VE9-Z4XF.

87. *Id.*

88. Barlyn, *supra* note 79.

89. *How It Works*, CASTLIGHT, https://perma.cc/549S-XEQT (last visited May 19, 2019).

90. *Id.*

91. *Ecosystem*, CASTLIGHT, https://perma.cc/U4V7-XYLG (last visited May 10, 2019).

ployers and workers, the wide scope of data collection that Castlight facilitates makes it easier for employers to collect and use such data in the workplace.

F. Personalized Medicine May Support Data-Driven Workplace Evaluations.

Another factor enabling the use of health data to influence workplace decisions is the rise of personalized medicine and the concept of "risk scores." Personalized medicine uses genetic and other information that is as specific as possible to the patient to help maximize the likely success of treatment.[92] By taking the patients' specific genetic and molecular profiles into account, the practice of personalized medicine aims to help doctors and other health practitioners make treatment choices that have the greatest benefit with the most minimal harmful side effects.[93] It also helps to reduce the costs associated with "trial and error" approaches.[94]

While personalized medicine may offer significant advantages, the fact that it relies on genetic, molecular and biometric data for its effectiveness may have consequences outside of the scope of medical treatment. Diagnostic companies developing new tools and tests to help analyze and interpret this data will be supported by the growing acceptance and funding of personalized medicine.[95] The federal personalized medicine initiative, "All of Us," expects to collect data from at least one million participants and had a budget of $290 million in 2018 alone, more than twice the budget allocated in the 2016 fiscal year.[96] These advanced diagnostic tools should increase the accuracy and detail with which personal data can be translated into health-based predictions about any given individual. Similarly, companies developing the tools and resources that

92. *The Age of Personalized Medicine*, PERSONALIZED MED. COALITION, https://perma.cc/8GN7-HGMK (last visited May 10, 2019).

93. *Id.*

94. *Id.*

95. *Id.*

96. *All of Us Research Program Backgrounder*, NAT'L INST. HEALTH, https://perma.cc/6MML-5FYF (last visited May 10, 2019).

will be used to collect and store this data will benefit from the personalized medicine economy. Whether those companies develop methods of protecting personal data confidentiality at the same rate and to the same extent that they develop methods of collecting and interpreting that data has yet to be determined.

Third-party data collectors already siphon off much of the health data that personalized medicine incentivizes. Companies such as LexisNexis, Milliman and HBI Solutions are reportedly amassing personal data collected from insurance claims, health records, housing records, and family or relationship records (such as the people a given individual may have in her household) to create what are known as "risk scores."[97] These risk scores are based on algorithms developed to estimate the relative risks of certain behaviors and illnesses an individual is likely to have, using data that includes but is not limited to health data, although the specifics of those algorithms are not made public.[98] The risk scores are sold to and used by health providers as well as health insurers, reportedly including major insurers such as Cigna and UnitedHealth's Optum.[99]

One benefit of "risk scores" is that they can help health care providers identify patients who have a higher risk of addiction to opioids, allowing the providers to make more informed decisions about prescribing opioids in general.[100] In its January 2019 National Drug Control Strategy, the Office of National Drug Control Policy announced plans to require health care providers to check databases that indicate likelihood of addiction before prescribing opioids to any patient.[101] This indicates the growing acceptance by the government of, and possibly the necessity of, using risk scores in some medical treatment in the future.

---

97. Mohana Ravindranath, *How Your Health Information is Sold and Turned Into 'Risk Scores*,' POLITICO (Feb. 3, 2019, 6:56 AM), https://perma.cc/H4AD-6KVE.

98. *Id.*

99. *Id.*

100. *Id.*

101. *National Drug Control Strategy*, OFF. NAT'L DRUG CONTROL POL'Y 6 (Jan. 2019), https://perma.cc/GT5C-XRKU.

Critics of using risk scores point out that there is no way to assess how reliable the algorithms used in calculating these scores may be. Companies selling this predictive technology have been reluctant to disclose their formulas, which provide their competitive advantages and may be protectable trade secrets.[102] There is also no way to determine what kinds of data are being collected by these predictive technology companies. Whether these risk scores are calculated using accurate or inaccurate data, and how the calculations weigh that data, is unknowable. Senator Ed Markey introduced the "Data Broker Accountability and Transparency Act" in 2017 that would have required data brokers to "establish procedure to ensure the accuracy of collected personal information," but it did not pass.[103] In short, there is no specific legal restriction on the data collected by these third parties or the uses to which they can put that data.

The more data employers have, the more detailed the conclusions they can draw about individual workers. As algorithms become more commonplace, they may become more inter-operational. Biometric and health data monitoring at work produces information that can be used to enrich, or to reinforce the biases of, other sources of data that may be available to the employer and used for adverse purposes. For example, researchers are already using social media to predict mental illness. In one 2017 study, two researchers used algorithms to successfully identify markers of depression based on Instagram data including face detection and color analysis.[104] The computer models did a better job of predicting depression than a human ratings model.[105] The advent of computer predictions of depression has been hailed as "a wonderful thing" and "a

102. Ravindranath, *supra* note 97.

103. Data Broker Accountability and Transparency Act of 2017, S. 1815, 115th Cong. (2017). Markey reintroduced the bill in 2019, revising the name accordingly. Data Broker Accountability and Transparency Act of 2019, S. 2577, 116th Cong. (2019), https://perma.cc/7JNF-GHG3.

104. Andrew Reece & Christopher Danforth, *Instagram Photos Reveal Predictive Markers of Depression*, 6 EUR. PHYSICAL J. DATA SCI., No. 15 (2017), https://perma.cc/J42L-8KY5.

105. *Id.* at 9.

boon for public health."[106] If biometric data collected through workplace wellness programs were added to this data collection, creating a superset for predictive analysis, that synthesis would strengthen the confidence with which employers categorize workers as more or less likely to have or develop conditions such as depression.

III. THE COSTS AND CONSEQUENCES OF MISUSING EMPLOYEES' BIOMETRIC DATA

Employers have a great deal of latitude, as a matter of law, as to what they do with the information collected through such monitoring. Some employers might want to direct more counseling, support or other resources to workers whose biometric data suggests that they are experiencing stress. Other employers could decide that workers with higher stress levels are likely to be less productive and therefore less desirable. The latter type of employer might use relative stress levels as a factor in worker evaluations. The use of similar algorithms in the workplace to predict employee character, performance and tenacity is well established.[107] The potential consequences of misusing the new range of biometric and health data collected from workers can cause serious harm to both employers and workers. These consequences range from adverse employment decisions based on monitored data to inaccurate assessment of workers, resulting in a workforce that is decreasingly diverse, inclusive and effective.

A. Misuse Could Produce Legal but Unethical Adverse Employment Decisions.

Without clear guidance as to the use of biometric and health data, and without a legal prohibition, employers are free to make decisions based

106. Zeynep Tufekci, *Think You're Discreet Online? Think Again*, N.Y. TIMES (Apr. 21, 2019), https://perma.cc/G29P-SR5Z.

107. *See, e.g.*, Quentin Hardy, *Using Algorithms to Determine Character*, N.Y. TIMES: BITS (July 26, 2015, 5:30 AM), https://perma.cc/R7XG-A2FJ.

on the data they collect either directly or indirectly. Given the high cost of health insurance, an employer that has to reduce its workforce might reasonably cull the employees who may be the most expensive to insure in the future.

For example, an employer reviewing biometric data might notice that of ten employees, two have relatively high resting heart rates as measured by the monitors they wear as part of the employer's workplace wellness program. While their high heart rates may not be impeding the quality of their work, and may not be detectable even to their coworkers with the naked eye, the employer might believe that high heart rates can be a predictor of, or at a minimum correlate with, a disease. Tachycardia (fast heart rate) can be associated with elevated likelihood of a cardiac arrest, serious mitral valve disease, cardiomyopathy or sarcoidosis (an inflammatory disease).[108] More commonly, people with tachycardia might be anxious, physically fatigued, heavy drinkers or heavy smokers.[109] The employer might reasonably conclude that the two workers with the undesirable characteristic of a high heart rate that could cause extra trouble and expense should be among the first to go, and include them in the first round of reductions in force.

In the absence of biometric and health data monitoring, the employer might never know that these two employees had faster than normal resting heart rates. The two employees might be just as productive and good at their jobs as their colleagues with lower resting heart rates and might therefore not have been singled out for any other reason suggesting their relative undesirability. The health data monitoring alone puts them at an elevated risk of adverse employment decisions.

From the employer's perspective, this may seem like a sensible strategy. An employer might decide that workers with higher heart rates are likely to be less productive than other workers. People with tachycardia may experience symptoms such as lightheadedness, shortness of breath

108. *Tachycardia: Fast Heart Rate*, AM. HEART ASS'N, https://perma.cc/HU6J-J9QC (last visited May 10, 2019).

109. *Id.*

and fatigue.[110] The employer might believe that such workers will make more mistakes or be less focused because of these symptoms. These workers might then be regarded as poor candidates for leadership positions or any further training or other investment. Alternatively, an employer might assume that because people who are fatigued, heavy drinkers or heavy smokers are more likely to have tachycardia,[111] and all of those people might be assumed to be less effective workers, that it is logical to let go of or fail to promote people with higher heart rates.

Firing workers based on their heart rate is a bad idea for several reasons. First, relying on stereotypes such as the ones described above is an overbroad and ineffective way to evaluate workers. Many workers with high resting heart rates will be just as good at their jobs as workers with lower resting heart rates. In fact, one recent study using wearables to track the anxiety levels and heart rates of construction workers found that "workers work more efficiently when they feel relatively high levels of stress and anxiety."[112] While many people with tachycardia experience lightheadedness, for example, many others with tachycardia experience no such symptoms.[113] It is easy for employers to confuse correlation with causation. An employer could assume, for example, that because many people who have tachycardia may be heavy smokers or drinkers, it is those undesirable behaviors that have caused the tachycardia. The employer might then mistakenly use tachycardia as an indicator of heavy smoking or drinking based on a logical error. As a result, the employer may be more likely to disqualify people who may be well qualified to do their jobs for reasons unrelated to actual performance, resulting in overall

110. *Id.*

111. *Id.*

112. Chao Mao et al., *Using Wearable Devices to Explore the Relationship Among the Work Productivity, Psychological State, and Physical Status of Construction Workers*, 35 INT'L SYMP. ON AUTOMATION & ROBOTICS CONSTRUCTION & MINING 1174, 1177 (2018) (emphasis added), https://perma.cc/H96U-23HY (observing positive correlations between anxiety and heart rate levels and work productivity among construction workers).

113. *Tachycardia: Fast Heart Rate*, *supra* note 108.

inefficiency. Companies culling workers in a misguided effort to minimize long-term health insurance costs are likely hurting themselves in terms of recruitment and retention.

Second, there is a potential cascading effect in that workers subject to data bias in one place will find it increasingly challenging to get and keep jobs elsewhere.[114] As biometric and health data monitoring becomes more common, it could be more difficult for workers whose data is flagged as potentially undesirable to get and keep jobs. This may produce a class of underemployed people who share biometric features unrelated to their objective potential. Conversely, workers who are well equipped to mask the kinds of data that employers might flag as undesirable, such as a high heart rate, will have a competitive advantage in the workplace. It is easy to imagine that a marketplace would develop for devices and techniques that could fool an employer into thinking that a worker is calmer, better rested, and less anxious than they actually are by manipulation of the health and biometric data being measured.

Biometric and health data may play into subconscious discrimination, compounding this problem. If a manager learns that one of her employees smokes and another does not, she may remember that information at some level when making decisions about who to promote. The manager may like non-smokers more than she likes smokers. In making the promotion decision, however, the manager may strive to do her best to be fair, and promote based on merit or achievement. It is easy to imagine, however, that her general feelings about smoking may affect her conscious evaluation of merit or achievement. In such a case, it would be difficult to establish, at least at an individual level, that her promotion

114. *See, e.g.*, Elizabeth Chika Tippett, *Opportunity Discrimination: A Hidden Liability Employers Can Fix*, 23 EMPL. RTS. & EMPL. POL'Y J. 165 (2019) (arguing that "big" employment decisions such as promotions and raises are influenced by "smaller" opportunities which do not rise to the level of adverse employment actions within the meaning of Title VII of the Civil Rights Act, but which may be disparately distributed and give rise to late actionable discrimination).

decision was affected by her knowledge about her employees' smoking habits.[115]

A third reason why adverse employment decisions based on biometric data are unwise is that the practice of such data monitoring itself is likely to increase many of the illnesses about which employers could have a legitimate concern. While an elevated heart rate can be a sign of a serious medical condition, such as hyperthyroidism or AFib, it can also be triggered by stress. The fact of being tracked may be a stressor in itself. One cardiologist commenting on the use of wearables to track heart rates noted that while "[i]n general, I suspect this information is helpful, […] there are some rare cases where I've told patients to take their fitness trackers off because it's making things worse."[116]

The practice of biometric and health data monitoring in the workplace is likely to increase the stress, anxiety, and fatigue of the workforce because of the potential negative consequences that a bad set of data might cause. If these workers' elevated heart rates are due to anxiety, adverse employment actions and the job instability they perpetuate will certainly exacerbate the problem. Studies have shown that electronic performance monitoring tends to increase self-reported stress levels at work during difficult tasks.[117] Chronic job stress is certainly bad for employees, in that it is linked with various debilitating conditions including physical illness, mental illness and psychological distress.[118] In this regard, data monitoring that increases stress is likely to have the perverse effect of increasing the health insurance costs it is intended to reduce over time. It is

115. *See* JESSICA L. ROBERTS & ELIZABETH WEEKS, HEALTHISM 39-40 (2018).

116. Vanessa Hand Orellana, *Wearables Get Serious About Heart Rate*, CNET MAG. (Dec. 2, 2018, 4:15 AM), https://perma.cc/Q7VG-8U8Z.

117. Rick Davidson & Ron Henderson, *Electronic Performance Monitoring: A Laboratory Investigation of the Influence of Monitoring and Difficulty on Task Performance, Mood State, and Self-Reported Stress Levels*, 30 J. APPLIED SOC. PSYCHOL. 906, 911 (2006).

118. *See* Kamaldeep Bhui et al., *Perceptions of Work Stress Causes and Effective Interventions in Employees Working in Public, Private and Non-governmental Organisations: A Qualitative Study*, 40 BJ PSYCH. BULL. 318, 318 (2016).

also bad for the employer. The chronic stress caused by increased monitoring is likely to interfere with effective organizational functioning, in that it has been linked to high turnover and absenteeism.[119]

B. Biometric and Health Monitoring May Lead to Inaccurate Assessments.

Another hazard of widespread use of biometric and health data in the workplace is that the data may be wrong. As an initial matter, the devices may be recording inaccurate data. Fitbit, a market leader, is currently fighting a class-action lawsuit in the Northern District of California alleging that its popular devices equipped with the PurePulse heart rate tracking feature are inaccurate and ineffective. In June 2018, district court Judge James Donato denied Fitbit's motion to dismiss the lawsuit, which states claims for false advertising, unfair competition, fraud, and breach of warranty.[120] Another group of plaintiffs is suing Fitbit for fraud in connection with its sleep tracking function.[121] Those plaintiffs claim that Fitbit's devices only track motion as a proxy for sleep, rather than tracking actual "hours slept" and "sleep quality," as promised in Fitbit's advertising.[122]

A second cause for concern is the accuracy of interpretive algorithms. Health algorithms might make suggestions to employers about the likely preferences or qualities that workers with certain biometric features might share. These health algorithms could provide outputs that are similar to the "risk score" described in Part II.F above. Algorithms are already being used in other health-related contexts, such as interpreting

119. *See* Beatrice Brunner et al., *Who Gains the Most from Improving Working Conditions? Health-related Absenteeism and Presenteeism Due to Stress at Work*, 20 EUR. J. HEALTH ECON. 1165 (2019) (assessing effects of stress on absenteeism).

120. McLellan v. Fitbit, Inc., No. 3:16-CV-00036-JD, 2018 WL 2688781, at *1 (N.D. Cal. June 5, 2018).

121. Brickman v. Fitbit, Inc., No. 15-CV-02077-JD, 2016 WL 3844327, at *1 (N.D. Cal. July 15, 2016).

122. *Id.*

MRIs and other medical images.[123] Whether these algorithms will be accurate and/or useful is open to debate. The public is generally skeptical about the fairness and acceptability of using algorithms to make decisions with "important real-world consequences."[124] Whether a person can keep her job is one of the most important real-world consequences of computer-assisted decision making. The potential for bias is one of the most salient concerns. Approximately 60% of adults surveyed feel that algorithms will always reflect the biases of their designers, although younger Americans tend to be more supportive of the idea that bias-free programs can be developed.[125] Former Justice Abrahamson of the Wisconsin Supreme Court expressed skepticism about the use of algorithms such as COMPAS in assessing recidivism risks because of potential inaccuracies.[126] A company developing an algorithm to help employers evaluate the likely long-term health risks of its workers might err on the side of flagging risks, since doing so is more likely to be interpreted by its target customers as a cost-saving and therefore beneficial feature. Any bias in these algorithms is therefore likely to work against the target of the monitoring, who would have little direct knowledge of the bias inherent in the programming.

Another source of bias and therefore potential inaccuracy in algorithms stems from the fact that men and women often experience the same physical symptoms at different rates, under different conditions, and for different reasons, yet algorithms are not likely to differentiate

123. Rob Matheson, *Faster Analysis of Medical Images*, MIT NEWS (June 18, 2018), https://perma.cc/VC4Z-R5UR (reporting the development of "a machine-learning algorithm that can register brain scans and other 3-D images more than 1,000 times more quickly using novel learning techniques").

124. Aaron Smith, *Public Attitudes Toward Computer Algorithms*, PEW RES. CTR. (Nov. 16, 2018), https://perma.cc/9GBV-U5YF (reporting that between 56% and 68% of U.S. adults find certain forms of algorithmic decision-making unacceptable).

125. *Id.* at 8 (noting that half of people between the ages of 18 to 29 believe that computer programs can be developed free from bias, while that view is held by 43% of people ages 30 to 49 and only 34% of people 50 and older).

126. State v. Loomis, 881 N.W.2d 749, 774 (Wis. 2016) (Abrahamson, J., concurring).

based on gender. As Caroline Criado-Perez points out in her book, *Invisible Women: Data Bias in a World Designed for Men*, standard algorithms routinely exclude women's differences in a wide range of data sets.[127] Many of these contexts affect the correct interpretation of the health conditions that might be the subject of algorithms based on biometric data collection at work. These algorithms are based largely on studies done on young Caucasian men, and do not accurately represent women.[128] Women have higher rates of work-related stress, anxiety and depression than men.[129] Data suggesting anxiety in a man may be a more likely predictor of a condition such as fibroids in a woman.[130] Working moderately long hours is also likely to have a different health effect on men than on women. Women are also more likely to develop heart disease and cancer when they work more than forty hours a week, while men who work between forty-one and fifty hours a week are less likely to suffer from heart disease, chronic lung disease or depression.[131] There are also sex-related differences in the presentation and likely outcome of Parkinson's disease, stroke, brain ischemia as well as in the workings of the heart, lungs, and every human tissue and organ system.[132]

The wearables themselves could also exacerbate this potential gender data bias. Although most wearables are marketed as gender-neutral,

127. CAROLINE CRIADO-PEREZ, INVISIBLE WOMEN: DATA BIAS IN A WORLD DESIGNED FOR MEN 167 (2019) (noting the "well-documented and chronic gaps in medical data when it comes to women").

128. *Id.* at 116 (suggesting that "Caucasian men aged twenty-five to thirty who weigh 70kg" are "Reference Man" who is intended to "represent humanity as a whole").

129. *Id.* at 73; HEALTH AND SAFETY EXEC., WORK RELATED STRESS DEPRESSION OR ANXIETY STATISTICS IN GREAT BRITAIN 6 (2018), https://perma.cc/R76B-UPRL.

130. Tara Culp-Ressler, *When Gender Stereotypes Become a Serious Hazard to Women's Health*, THINKPROGRESS (May 11, 2015, 12:00 PM), https://perma.cc/W642-VFAX (describing the experience of a woman whose symptoms were repeatedly diagnosed as anxiety before she demanded an ultrasound revealing potentially fatal uterine fibroids requiring surgery).

131. Allard E. Dembe & Xiaoxi Yao, *Chronic Disease Risks from Exposure to Long-Hour Work Schedules Over a 32-Year Period*, 58 J. OCCUPATIONAL ENVTL. MED. 861 (2016).

132. CRIADO-PEREZ, *supra* note 127, at 198-99.

many of them are designed for men's bodies. These include sensor-enhanced jackets that fit men's torsos but are too large for most women,[133] smart glasses or virtual reality headsets whose lenses cannot accurately track the gaze of a person wearing mascara,[134] and smartwatches that are too big for women's wrists.[135] Similarly, facial recognition technology identifies men's faces well, but has trouble identifying women of color.[136]

Even the smart clothing modeled at CES 2019's Wearable Tech Summit designed to promote "intelligent wearable strength" was shown on a male model.[137] The only electronically enhanced clothing shown during that summit designed for women was by a company called CuteCircuit, which uses LEDS to make decorative but not functional patterns on dresses.[138]

C. Employers Tend to Misuse, but Employees Tend Not to Protest.

The interest, excitement, and willingness of employers to deploy new forms of data collection bear no apparent relation to the employers' self-reported ability to use that data responsibly or well. According to one study of global business leaders, most say they are not "very confident" in their ability to both collect and analyze data from employees responsibly.[139] Only 30% of leaders report feeling "very confident" that they can use workplace data in a responsible way.[140] As one reporter noted, "Just about half of business leaders say they will use workplace data as they

133. Adi Robertson, *Building for Virtual Reality? Don't Forget About Women*, VERGE (Jan. 11, 2016, 3:07 PM), https://perma.cc/6DBZ-WG67.

134. *Id.*

135. Kat Ely, *The World is Designed for Men*, MEDIUM (Sept. 8, 2015), https://perma.cc/SWS2-FHPD.

136. Tom Simonite, *Photo Algorithms ID White Men Fine—Black Women, Not So Much*, WIRED (Feb. 6, 2018, 6:21 PM), https://perma.cc/EW6W-TMZM.

137. Advertisement for the CES 2019 Wearable Tech Summit, SEISMIC, https://perma.cc/BFK7-29WL (last visited May 14, 2020).

138. WEARABLE TECHNOLOGY SUMMIT, https://perma.cc/QG26-YQYY (last visited June 28, 2020); *see, e.g.*, CUTECIRCUIT, https://perma.cc/4UXW-5W8J (last visited May 14, 2020).

139. Shook et al., *supra* note 66, at 6.

140. *Id.*

see fit, with no additional responsibility measures. Executives worry even more than employees that office data collection by intelligence machines will lead to the devaluation of human work."[141]

If employers misuse data as they predict, their misuse is unlikely to be curbed by worker resistance. Although more than half of large companies use some kind of remote monitoring of employees, employees do not generally object to such monitoring, although the survey was not limited to biometric monitoring.[142] In fact, the vast majority of workers surveyed (92%) said that they did not mind being monitored, as long as the data being collected will be used to help them become more successful at work.[143] Nearly four out of five workers said that they would welcome data-based feedback that might help them optimize their time, while more than three quarters of them approved of data monitoring that would "improve [their] relationships and communications with others."[144] An even greater percentage of workers approve, at least in principle, of using data to make decisions about how much they should be paid and who should be promoted. Approximately 82% of surveyed workers think "pay, promotions, and appraisal decisions" would be less biased and more accurate if they were based on hard data instead of subjective assessments."[145]

It is unclear whether the workers in this study were thinking of performance metrics rather than biometric data. When a study specifically refers to health monitoring, respondents are more likely to object. Most millennials object to employers taking health habits into account in evaluations, with 93% of employees surveyed saying that employers should

141. Eric Rosenbaum, *Companies Are Collecting More Data on Employees, and Not at All Confident They Are Doing It Responsibly*, CNBC (Jan. 23, 2019, 12:56 PM EST), https://perma.cc/K2S2-JCBP.

142. Anne Fisher, *Why Your Employer Is Spying on You—And Why That Might Be Okay*, FORTUNE (Jan. 24, 2019, 12:49 PM), https://perma.cc/JQ6C-Q6C2.

143. *Id.*

144. *Id.*

145. *Id.*

not take their smoking habits into account and 81% responding that employers had no right to consider alcohol use.[146]

Even when workers are aware of the risks that health data collection presents, they may be unable or unwilling to protest for practical reasons. Most people do not have an infinite choice of employment. The economic, practical and personal costs of changing jobs can be staggering, and most people try to keep their jobs as long as possible for these reasons. The fact that workers are ill equipped to protest against employers for practices that do not pose an immediate threat is also the reason why it is difficult to say whether workers can give informed consent to the use of their biometric and health data.[147] How voluntary can such consent truly be, given the significant difficulties of changing jobs for most people? As such data collection becomes more common, it may be practically impossible for people to "choose" to work for an employer that does not engage in such practices. And without pressure from current or potential employees, it is doubtful that employers will feel constrained to use biometric, health or any other data responsibly unless they are legally obligated to do so.

D. Employer Monitoring Also Invades Privacy and Risks Hacking Evaluations.

Another risk inherent in the more widespread collection of biometric data at work is the risk that such data will be hacked. Hackers are becoming more adept at getting unauthorized access to health data stored in connection with workplace wellness programs and increasingly focused on that data. According to the U.S. Department of Health and Human Services, there have been multiple large-scale data breaches involving

146. Daniel Singer, Note, *Differing Perspectives:* Doe v. Department of Justice*: Adverse Actions for Off-Duty Conduct: Why the Federal Circuit's Approach Infringes Employees' Privacy Rights*, 20 FED. CIR. B.J. 169, 189 n.131 (2010) (citing L. CAMILLE HEBERT, EMPLOYEE PRIVACY LAW § 13:3, at 13-9 (2009)).

147. For a more expansive critique of "choice" in privacy protection, see ARI EZRA WALDMAN, PRIVACY AS TRUST 83-85 (Cambridge Univ. Press 2018).

health plans, health care providers and health care clearing houses in recent years.[148] In the first few months of 2019 alone, over 100 additional breaches were reported, including a single breach at the University of Washington School of Medicine affecting nearly one million users.[149] Collectively, these breaches affected tens of millions of people.[150]

When hacking of private health information becomes commonplace, it undermines the basic premises both that (1) stored health information is ever really protected and (2) employers cannot easily link health data with specific individuals. While the federal Office of the National Coordinator for Health Information Technology has issued guidance on the best practices for managing the security of health information, which might in theory minimize the risk of similar breaches, these specific security processes are not required by federal law.[151]

IV. CURRENT LAWS DO LITTLE TO CURB EMPLOYER'S MISUSE OF BIOMETRIC DATA.

Although the risks of biometric and health data misuse are significant, few laws protect U.S. workers from their consequences. In order to understand why, let's use the example of an employer tracking sleep patterns. When an employer can track the amount and quality of sleep a worker gets, it can make qualitative inferences about that worker. An employer might infer that someone who gets eight solid hours of sleep is likely to be more productive than someone who only gets three or four hours a night. The employer might deem a worker who has more regular sleep patterns more reliable and responsible. These inferences might

148. *See Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information*, U.S. DEP'T OF HEALTH AND HUMAN SERVICES OFF. FOR CIVIL RIGHTS, https://perma.cc/P66W-ES4A (to locate, under "breach report results," sort by "individuals affected") (last visited Apr. 28, 2020).

149. *Id.*

150. Chuck Leddy, *Check-Up on Data Security: Protecting Employee Health Information*, ADP (Feb. 18, 2016), https://perma.cc/G8Y6-9Q76.

151. OFF. OF THE NAT'L COORDINATOR FOR HEALTH INFO. TECH., GUIDE TO PRIVACY AND SECURITY OF ELECTRONIC HEALTH INFO. 35, https://perma.cc/HL6H-WMT4.

work against a mother, for example, whose sleep is regularly interrupted because of her kids, or someone who simply doesn't need a lot of sleep in general. The relatively sleepless worker might be fired more quickly when the company needs to reduce its workforce. Would he or she have any legal remedy under federal law against the employer for its differential treatment? The following sections explain why the answer is probably no.

A. Anti-Discrimination Laws Do Not Protect Against Misuse of Health Data.

Discrimination is only illegal, of course, when it is prohibited by law. In order for our sleep-deprived worker to be protected by anti-discrimination laws, she would have to establish that she suffered an adverse employment action on the basis of some protected class defined by a specific anti-discrimination law. There are several federal and state laws that define classes into which she might fall, but no law will protect her from an adverse employment action on the basis of her sleep status even if she can prove that that was the basis for her employer's decision.

1. The Civil Rights Act of 1964

One of the most salient federal antidiscrimination laws is the Civil Rights Act of 1964.[152] Under Title VII of the Civil Rights Act, it is illegal for employers to "fail or refuse to hire or to discharge . . . or otherwise to discriminate against any individual with respect to his compensation, terms, conditions, or privileges of employment because of such individual's race, color, religion, sex, or national origin."[153] It also prohibits actions that would "deprive or tend to deprive any individual of employment opportunities or otherwise adversely affect his status as an

152. Civil Rights Act of 1964, 42 U.S.C. § 2000e
153. *Id.* § 2000e-2.

employee, because of such individual's race, color, religion, sex, or national origin."[154] Title VII does not protect people from adverse employment actions based on something other than membership in one of those five protected classes, such as where an applicant went to college or what kind of shoes she wore at her performance review.

Title VII does not bar an adverse employment action against the sleep-deprived workers above. "Sleeping less than eight hours a night" does not correlate with any of the protected classes enumerated by that statute.[155] An employer could fire or refuse to promote an employee who sleeps less than others on that basis without violating Title VII, just as it might fire or refuse to promote someone based on her alma mater or footwear. The fact that she is a mother, without more, will not violate Title VII either, as Title VII does not provide protection based on family status alone.[156] If the employer takes more adverse action against sleepless women than against sleepless men, however, the female workers may be able to argue that they are subject to disparate treatment discrimination.

2. *The Pregnancy Discrimination Act of 1978*

Let's say that a worker is losing sleep because she is seven months pregnant and finds it hard to sleep, or because she is a new mother, and her newborn keeps her awake. If Title VII does not apply to protect the worker, can she establish that she is the victim of pregnancy discrimination and therefore protected by the Pregnancy Discrimination Act (PDA)?[157] This law amended the Civil Rights Act to specify that "sex" as a protected classification encompasses "pregnancy, childbirth, or related

154. *Id*.

155. *See id.*

156. Adamson v. Multi Cmty. Diversified Servs., 514 F.3d 1136, 1148 (10th Cir. 2008) (holding that Title VII does not protect based on "family" or "familial status" alone); Akin-Taylor v. Kaiser Found. Health Plan, Inc., No. 13-00039 JCS, 2013 U.S. Dist. LEXIS 116571, at *9-10 (N.D. Cal. Aug. 16, 2013) (noting that "Title VII does not create a stand-alone cause of action for discrimination based on family responsibility").

157. Pregnancy Discrimination Act of 1978, Pub. L. No. 95–555, 92 Stat. 2076 (amending 42 U.S.C. § 2000e (1964)).

medical conditions," and employees cannot be subject to adverse employment actions on those bases.[158] While the worker might claim that she was subject to discrimination in violation of the PDA, she is likely to lose her claim if the employer can show that its action was not based on a "related medical condition," but on her sleeping patterns, if it can demonstrate that those are unrelated to her childbirth. Even if the worker can show that she was losing sleep because of her childbirth, she is unlikely to succeed if the employer applies a general preference for workers who get more sleep, rather than applying its preference selectively to those with newborns.

3. The Americans With Disabilities Act

For similar reasons, the ADA would also provide no protection to the sleep-deprived worker in our example. The ADA, as amended by the ADA Amendments Act in 2008, makes it unlawful for an employer to "discriminate against a qualified individual on the basis of disability in regard to job application procedure, the hiring, advancement, or discharge of employees, employee compensation . . . . and other terms, conditions, and privileges of employment."[159] A "disability" can be "a physical or mental impairment that substantially limits one or more major life activities," "a record of such an impairment," or "being regarded as having such an impairment."[160] The statute provides an illustrative but not exhaustive list of major life activities.[161]

The critical question in this context is whether the monitored condition or activity qualifies as a "disability." In order to answer this question, we would ask whether the monitored individual's practice of sleeping less than others "substantially limits" one or more major life activities (or whether she is regarded as being disabled as statutorily defined). Assuming that the answer is no, the ADA does not apply. Sleeping less than

158. *Id.*
159. 42 U.S.C. § 12112 (2018).
160. *Id.*; *see also* 42 U.S.C. § 12102 (1)(A)-(C) (2018).
161. § 12112; *see also* § 12102 (2)(A).

other people does not meet the definition of an actual or perceived disability under that law.[162]

This example illustrates the fact that not all health-related conditions qualify as disabilities at law, leaving open the possibility that employers may treat workers with certain habits, such as smoking or higher body mass indexes (BMIs), differently from other workers without creating liability under the ADA.[163] Prejudice against certain groups of people based on their health conditions that fall outside of the ADA's definition of "disability" and otherwise do not correlate with protected classes, has been referred to as "healthism," a term coined by Jessica Roberts.[164] Roberts argues that singling people out because of their health status is "healthist" and offends health equality.[165]

Healthism is pernicious in part because it rests on the false assumption that everyone is equally capable of improving their own health. Roberts offers the example of a single mother who is the sole breadwinner for several children, who may have to work two jobs, live in a low-income area with few safe green spaces or other opportunities for exercise and with many fast-food restaurants but few stores selling fresh produce.[166] It will be significantly harder for that woman to make healthier "choices" than it would be for someone in a dual-income family living in a suburban area with more recreational options and a Whole Foods nearby.[167] Preferring healthier employees, through imposing employment-related

162. If she suffered from sleep apnea, however, this might qualify as a disability under the ADA. *See* Russo v. Jefferson Parish Water Dep't, CIVIL ACTION NO. 96-2134 SECTION "N", 1997 U.S. Dist. LEXIS 17951, at *7 (E.D. La. Nov. 7, 1997) (holding that whether sleep apnea constitutes a disability under the ADA presents a material issue of fact). It is also possible that employees who have higher heart rates or other biometric data suggesting higher stress levels may qualify for ADA protection if they are "regarded as" having a disability.

163. Jessica L. Roberts, *Healthism and the Law of Employment Discrimination*, 99 IOWA L. REV. 571, 615 (2014).

164. Jessica L. Roberts, "*Healthism": A Critique of the Antidiscrimination Approach to Health Insurance and Health-Care Reform*, 2012 U. ILL. L. REV 1159, 1171.

165. ROBERTS & WEEKS, *supra* note 115, at 37.

166. *Id.* at 36.

167. *Id.*

penalties on those who are measured as less healthy, may tend to perpetuate socioeconomic conditions we might prefer to remedy.[168]

4. State and Local Anti-Discrimination Laws

No states prohibit discrimination on the basis of biometric data, although several expand federal coverage for protection against discrimination on the basis of genetic information.[169] It is possible that some workers who suffer from discrimination based on their biometric or health data could be protected under a few state antidiscrimination laws, but they would have to make an indirect argument for that coverage. For example, the District of Columbia and Minnesota both prohibit discrimination on the basis of "family responsibilities" and "familial responsibilities," respectively.[170] The sleepless mother in our example may claim that she suffered discrimination based on her family responsibilities, in violation of those laws. The employer may escape liability if it can prove that she was not fired because she needed to take care of her family but rather because of her sleep levels per se, which likely would not constitute an adverse employment decision on the basis of her family responsibilities.

B. HIPAA Does Not Protect Against Biometric and Health Data Collection.

While many people believe that their health-related data must be protected by privacy laws such as the Health Insurance Portability and Accountability Act (HIPAA), there is no such protection in place given the way data is collected in workplace wellness programs. Data collection and monitoring companies such as Fitbit, Castlight, LexisNexis and Milliman are not the kinds of intermediaries that Congress presumably envisioned when HIPAA was signed into law on August 21, 1996. To understand why, it is important to understand the structure of HIPAA.

---

168. Brown, *supra* note 26.

169. *Discrimination—Employment Laws*, NAT'L CONF. OF ST. LEGISLATURES, https://perma.cc/END3-EAJX (last visited May 10, 2019).

170. *Id.*

A main purpose of HIPAA was, as its name suggests, to "improve [the] portability and continuity of health insurance coverage," and to "combat waste, fraud, and abuse in health insurance and health care delivery."[171] HIPAA was also meant to help protect the confidentiality of certain personal health information that workers may disclose.[172] It mandated that the U.S. Department of Health and Human Services (HHS) develop national standards for that protection.[173] The HHS created the Privacy Rule in order to guide the "use and disclosure" of "protected health information" and to determine how this information may be used by organizations subject to the Privacy Rule.[174] These organizations, referred to as "covered entities," include health plans, health maintenance organizations (HMOs), health insurers and health care providers.[175] Billing services, repricing companies, and other entities that process and standardize information, are also covered entities.[176] The Privacy Rule protects "individually identifiable health information" held or transmitted by a covered entity or its business associate.[177] Wearable technology manufacturers are not "covered entities" under HIPAA,[178] nor are they "business associates" because they have a more active role than the data-transformative nature of the entity types used to illustrate the meaning of that term.

Even if HIPAA did protect the privacy of health-related data collected through workplace wellness programs, it would do little good to individual workers who had suffered as a result of employer misuse facilitated by that data collection. There is no private right of action under

171. JOHN HASTERT, CONFERENCE REPORT, H.R. REP. NO. 104-736 at 1 (1996).

172. *See generally* 45 C.F.R. §§ 164.500-534 (2015).

173. *Id.*

174. U.S. DEP'T OF HEALTH & HUM. SERV., SUMMARY OF THE HIPAA PRIVACY RULE 1 (2003), https://perma.cc/L38L-TDF6.

175. *Id.*

176. *See generally* 45 C.F.R. §§ 160.102-160.103 (2013).

177. *Id.* § 160.103.

178. Matthew R. Langley, *Hide Your Health: Addressing the New Privacy Problem of Consumer Wearables*, 103 GEO. L.J. 1641, 1647 (2015) (arguing HIPAA is ineffective when protecting consumers' personal data in a commercial setting).

HIPAA.[179] No individual can sue for a violation of HIPAA itself. It is possible, however, that individuals could sue under a state law of negligence per se based on a likely violation of HIPAA.

Health-related apps may violate users' privacy in any number of ways without violating HIPAA. For example, MDLive, a telehealth app, was sued in April 2017 for allegedly sharing users' health information with an Israeli tech company, TestFairy, without the users' consent.[180] The class action lawsuit alleged that MDLive took an average of sixty screenshots during the first fifteen minutes of use, in which users filled out questionnaires asking for information including health conditions, behavioral health history and medications, and then transmitted those images to TestFairy, which is not a health care provider.[181]

HIPAA offers no protection in such cases. The complaint did not allege, and could not have truthfully alleged, that MDLive was subject to HIPAA as either a covered entity or a business associate.[182] As lawyers observed when the complaint was filed, the MDLive app is likely not subject to HIPAA restrictions because it is downloaded directly by consumers rather than being an interface between consumers and covered entities.[183] Even if MDLive were covered by HIPAA, nothing in the HIPAA regulations would require MDLive to inform users that their health-related information was being transferred to a business associate such as TestFairy.[184]

This was not an isolated case. In a 2016 article, researchers studied the privacy protections of diabetes apps available through the Google

179. Lee-Thomas v. Labcorp, 316 F. Supp. 3d 471 (D.D.C. 2018) (holding that there is no private right of action under HIPAA).

180. Maria Castellucci, *MDLive Sued Over Patient Privacy Concerns*, MODERN HEALTHCARE (Apr. 19, 2017, 1:00 AM), https://perma.cc/7W3W-L4CA.

181. Marianne Kolbasuk McGee, *Telehealth App Lawsuit Spotlights Privacy Questions*, GOV INFO SECURITY (Apr. 21, 2017), https://perma.cc/Q73H-VB6H.

182. *Id.*

183. *Id.*; *see also* Grant Arnow, Note, *Apple Watching You: Why Wearable Technology Should Be Federally Regulated,* 49 LOY. L.A. L. REV. 607, 629 (2016) (explaining that wearable device manufacturers are not "business associates" within the meaning of HIPAA).

184. McGee, *supra* note 181.

Play portal and found that between 76% and 86% of these apps routinely shared sensitive health information including insulin and blood glucose levels with third parties.[185] As the authors noted, "the sharing of sensitive health information by apps is generally not prohibited by [HIPAA]."[186] Even if HIPAA protected user privacy in these apps, it is hard to imagine the HHS or any other regulatory body effectively prosecuting illegal disclosures in what appear to be the majority of health-related apps, at least in the diabetes management sector.

C. General Data Privacy Laws Offer Inadequate Protection.

Existing data privacy laws that are not, like HIPAA, restricted to protecting health information are similarly unhelpful. Although users might claim that the unauthorized disclosure of their health information to an unknown third party in cases like the MDLive transfer violates their privacy, there are few privacy statutes that would provide an effective remedy in such situations.

Most privacy protection statutes require the plaintiff to demonstrate an injury, usually one that is objectively measurable, such as economic loss. For that reason, privacy advocates praised the Illinois Supreme Court's January 2019 ruling that a plaintiff can state a claim under Illinois' Biometric Privacy Act (BIPA) without a showing of actual damage.[187] The court's ruling specifically noted the damage biometric monitoring can cause, finding that the expenses of complying with BIPA "are likely to be insignificant compared to the substantial and irreversible harm that could result if biometric identifiers and information are not properly safeguarded."[188]

185. Sarah R. Blenner, et al., *Privacy Policies of Android Diabetes Apps and Sharing of Health Information*, 315 JAMA 1051, 1051 (2016), https://perma.cc/X6VQ-8ZBN.

186. *Id.* at 1052.

187. Russell Brandom, *Crucial Biometric Privacy Law Survives Illinois Court Fight*, VERGE (Jan. 26, 2019, 1:00 PM), https://perma.cc/SD5M-LUEF.

188. Rosenbach v. Six Flags Entm't Corp., 129 N.E.3d 1197, 1207 (Ill. 2019).

Data privacy laws have particularly limited application in the employment context. Because employers offer financial incentives for compliance with wellness programs, workers with less disposable income are more likely to feel compelled to participate in such programs.[189]

Another legal loophole through which workers' health data might fall is the eventual sale or bankruptcy of either a wearables company like Fitbit or the employer itself. As Syagnik Banerjee has pointed out, the end user license agreements (EULAs) of wearable devices regularly require users to acknowledge that the device company reserves the right to sell the collected data.[190] These sales could disperse employee health data even more broadly. When Radio Shack entered bankruptcy, it auctioned off customer email data along with its other intellectual property.[191] It is easy to imagine that another company might auction off employee data as well.

V. THREE SOLUTIONS COULD CURB EMPLOYER MISUSE OF BIOMETRIC DATA.

The increasing likelihood that employers will take adverse action against workers based on the biometric and health data that is becoming easier to monitor, together with the lack of existing regulatory protections, suggests the need for creative and effective solutions. I propose three possible solutions here. The most comprehensive solution would be to decouple health insurance from employment altogether. A second, more focused option would be to amend HIPAA and the Affordable Care Act (ACA) to clarify that neither employers nor their business associates can collect biometric and health-related data as part of even "voluntary"

189. Moritz Becker, *Understanding Users' Health Information Privacy Concerns for Health Wearables*, 51st HAW. INT'L CONF. ON SYS. SCI. 3261, 3266 (2018).

190. Syagnik Banerjee et al., *Wearable Devices and Healthcare: Data Sharing and Privacy*, 34 INFO. SOC'Y 1, 5 (2017), https://perma.cc/7ZF3-XKH6.

191. ACQUISITION OPPORTUNITY: INTELLECTUAL PROPERTY ASSETS – RADIOSHACK CORPORATION, HILCO STREAMBANK, https://perma.cc/8HLF-GPW7 (last visited May 10, 2019).

workplace wellness programs. The most direct way to limit the harm caused by misuse of biometric and health data is to broaden the scope of planned federal consumer data privacy legislation to encompass employee data privacy protection as well. Such legislation could be informed by comparison to employee data protection in other countries. Whether we choose a broad or narrow solution, involving one or more of these options, we should make an informed decision based on full knowledge of the risks involved rather than letting the biometric monitoring market chart the course. A final remedy would be to ensure that the development of a comprehensive federal data privacy law would address the needs of employees and not just consumers, the current focus of such legislative development efforts. Any one and any combination of these remedies would reduce the potential for the harms described in Part III. The choice of which to pursue will depend on a collective assessment of societal values, priorities, and political will.

A. Option 1: Decouple Health Insurance Coverage from Employment.

The single most important driver of workplace monitoring is the financial imperative to reduce the burgeoning costs of health insurance that employers bear. In 2018, employers paid an average of $19,616 for family coverage and $6,896 for individual coverage. That average for family coverage has increased 55% since 2008.[192] The rising cost of insuring employees has been described as one of the reasons why employers would prefer to categorize their workers as independent contractors rather than employees.[193] The rise of the gig economy, in which workers are generally classified as independent and therefore less expensive than employees, has made this distinction critical for millions of workers.[194]

192. KAISER FAMILY FOUND., 2018 EMPLOYER HEALTH BENEFITS SURVEY: SUMMARY OF FINDINGS (Oct. 3, 2018), https://perma.cc/G2A7-GGEF.

193. Conrad de Aenlle, *Employee or Contractor? Health Care Law Raises Stakes*, N.Y. TIMES (Feb. 4, 2015), https://perma.cc/4H6T-CKFL.

194. It is hard to gauge exactly how many workers there are in the gig economy

Decoupling health insurance from employment would make employers less compelled to drive down insurance costs through workplace wellness programs, while making health insurance easier to obtain for gig workers and others who do not qualify for benefits. Biometric and health data surveillance is largely driven by the belief that healthier workers lower health insurance costs for a firm over time. If employers were no longer responsible for subsidizing health insurance for their employees, they would have less incentive to collect biometric and health data, greatly reducing the chances that such data will be used for adverse employment actions.

Some have suggested that it makes no sense for employers to bear the administrative burden and financial cost of subsidizing health insurance.[195] If people are individually responsible for securing their own car insurance and homeowner's insurance, should health insurance be secured any differently? If workers had to secure their own health insurance, just as most people secure their own car insurance, there would still be financial incentives to be healthier because premiums presumably would still vary with the insurer's perception of risk. There may still be

because the federal government does not measure this uniformly. The Bureau of Labor Statistics found that as of May 2017, there were nearly six million "contingent workers" in the United States, defined as people who do not expect their jobs to last, or whose jobs are temporary. Karen Kosanovich, *Spotlight on Statistics: A Look at Contingent Workers*, BUREAU OF LAB. STAT. (Sept. 2018), https://perma.cc/F2QG-2DHW. This definition would appear to omit people who work as independent contractors on a regular basis, such as Uber drivers. While Uber has not directly disclosed how many people drive for it, current estimates based on Uber executive presentations and other reports suggest that there are at between 1 and 1.5 million Uber drivers in the United States alone. JC, *How Many Uber Drivers Are There?*, RIDESTER (Jan. 29, 2019), https://perma.cc/YA6X-ZLHR. The Federal Reserve reports that 31% of adults engaged in some form of gig work in 2017, but this includes people who had more traditional employment arrangements as well as gig work. FED. RESERVE, REPORT ON THE ECONOMIC WELL-BEING OF U.S. HOUSEHOLDS IN 2017, (June 19, 2018), https://perma.cc/JMP5-MYA4.

195. *See, e.g.*, Alain C. Enthoven & Victor R. Fuchs, *Employment-Based Health Insurance: Past, Present, and Future*, 25 HEALTH AFF. 1538 (2006), https://perma.cc/2YTN-3FZY; Brian Honermann, *Employer-Based Health Care – All Cons, No Pros*, O'NEILL INST.: GEO. L. (Apr. 17, 2014), https://perma.cc/L8SZ-HKXA.

some degree of data monitoring by life insurance companies, but the danger of adverse employment decisions based on this data would all but disappear.

Political resistance to such a change would probably be enormous. Many are already concerned about the relatively high costs of health care in the United States, even for those who have insurance. Decoupling health insurance from employment could be perceived as a further impediment to broader health care access. As one observer noted, health insurance coverage provided by employers "has been the only safe harbor in the American health care system for so long that people are understandably terrified of losing it."[196] Another source of resistance could be the longstanding opposition to universal health coverage, which flared most recently in response to Bernie Sanders' Medicare for All proposal.[197] Recent polls show that approximately half of Americans support both Medicare for All and a "public option," which is a government-run health plan.[198] While the coronavirus pandemic may have increased public support for universal health coverage in some quarters, the fact that some countries with the highest death rates per capita (including Spain, Italy and France) had such coverage may mitigate that support.[199]

While portable health care that travels with the worker from job to job may be difficult to achieve, examples suggest that it can be done. The National Domestic Workers Alliance created a portable benefits platform for its members, beginning with house cleaners and planning expansion to other groups.[200] Similarly, the Black Car Fund and the Independent Drivers Guild in New York are collaborating to provide health benefits

196. Jeff Spross, *Why Americans Need to Stop Getting Health Care Through Their Employers*, WEEK (Apr. 8, 2015), https://perma.cc/3HVN-4F5P.

197. KAISER FAMILY FOUND., PUBLIC OPINION ON SINGLE-PAYER, NATIONAL HEALTH PLANS, AND EXPANDING ACCESS TO MEDICARE COVERAGE (Apr. 3, 2020), https://perma.cc/3G9J-V85Y.

198. *Id*. at fig.17.

199. Editorial Bd., *Has the Coronavirus Provided Urgency for Universal Health Coverage? Yes and No*, WASH. POST (Apr. 11, 2020, 7:30 AM), https://perma.cc/NL26-S974.

200. Carolyn Said, *Gig Work Update: Portable Benefits for Domestic Workers*, S.F. CHRON. (Dec. 11, 2018), https://perma.cc/XU6H-V9N7.

for app-based drivers, funded by a 2.5% rider surcharge.[201] These models suggest that decoupling health insurance from employment can be done more broadly as well.

B. Option 2: Strengthen Existing Health Privacy Protections.

A second option would be to strengthen both HIPAA and the ACA to improve the protection of biometric and health data that can be collected in the workplace. One specific way to do this would be to amend HIPAA to ensure that the current and developing field of biometric monitoring devices are properly regulated, as scholars have recently suggested.[202] Grant Arnow has made a similar suggestion with regard to wearable technology in particular, arguing that HIPAA should be amended so that wearable technology is considered a "regulated medical device" instead of a "consumer electronics device."[203] In light of the expanded data collection capacities wearables now have, he also argues that HIPAA should explicitly acknowledge that wearables collect "protected health information" on behalf of "covered entities" because of the frequency with which users share this information with physicians.[204]

HIPAA might also be amended to recognize that all health information is "personally identifiable," regardless of its source, and therefore all health data should be protected. As tracking and identifying technology in phones, laptops and smartwatches becomes more ubiquitous, creating more points of identification that can be combined, it is hard to say

201. *Id.*

202. *See, e.g.*, Charlotte A. Tschider, *Enhancing Cybersecurity for the Digital Health Marketplace,* 26 ANN. HEALTH L. 1, 29 (2017) (critiquing the effectiveness of HIPAA in enhancing cybersecurity because of gaps in coverage); Latena Hazard, *Is Your Health Data Really Private? The Need to Update HIPAA Regulations to Incorporate Third-Party and Non-Covered Entities*, 25 CATH. U. J. L. & TECH., 447, 468 (2017) (noting gaps in HIPAA coverage for health data at various transmission points); Cristina M. Mares, *To Cover or Not to Cover? The Relationship Between the Apple Watch and the Health Insurance Portability and Accountability Act*, 18 DEPAUL J. HEALTH CARE L. 159, 176–77 (2016) (suggesting that the definition of PHI be expanded to better encompass data collected from wearables).

203. Arnow, *supra* note 183, at 631–32.

204. *Id.* at 632.

accurately that any health data is not personally identifiable. As Barbara J. Evans points out "data from mobile and wearable health devices . . . are inherently identifiable" because of the access to identifiers necessary during database creation to ensure that the data are properly matched to the right individual.[205] Amending HIPAA to broaden the protection of all such "inherently identifiable" health information would strengthen its protective power.

The definition of "business associates" in HIPAA is also too narrow in light of advances in biometric monitoring. Arnow suggests that wearable manufacturers themselves be categorized as "business associates" to acknowledge their role in storing and maintaining health data.[206] Because users are also sharing this biometric data with employers through data collectors and clearinghouses like Castlight to an unprecedented extent, those intermediaries also should be categorized as "business associates" as defined by HIPAA.

Alternatively, or in addition, the ACA's provisions for "voluntary" workplace wellness programs could be revised to ensure that they are truly voluntary. Removing any kind of individual incentives for compliance with such programs might affect a more comprehensive and effective wellness program that benefits the collective workforce rather than singling anyone out. Stefanie Brody makes a compelling argument for a return to a "zero-incentive" rule for workplace wellness programs, noting that a rule preventing employers from using financial incentives or penalties to encourage participation in wellness programs would help to shield employees from discrimination.[207] Removing individual incentives would also reduce the disparate impact of these incentives on

205. Barbara J. Evans, *Barbarians at the Gate: Consumer-Driven Health Data Commons and the Transformation of Citizen Science*, 42 AM. J.L. MED. 651, 655–56 (2016).

206. Arnow, *supra* note 183, at 632–33.

207. Stefanie Brody, Comment, *Working Well(ness): The Impact of the ADA Final Rule on Wellness Program Regulation and a Proposal for a Zero-Incentive Rule*, 11 ST. LOUIS U. J. HEALTH L. & POL'Y 209, 223 (2017) (arguing that a zero-incentive rule would be consistent with "the ADA's goal of protecting individuals from discrimination on the basis of disability").

lower-income workers who may be less able to forgo financial incentives due to their socioeconomic status, regardless of the impact on their privacy.[208]

Revising the ACA's guidelines to remove individual incentives would not prevent employers from helping to improve their employees' health. Employers could still offer discounted health club memberships, access to smoking cessation and weight loss programs, free healthy food in the office,[209] and many other benefits without collecting health data or compelling participation through the kinds of incentives commonly offered in workplace wellness programs. Companies might choose to offer these benefits because they align with corporate principles about how they treat their stakeholders, because they believe that healthier workers will be more productive or loyal, or because they believe it is the right thing to do.

C. Option 3: Write and Amend Data Privacy Laws to Protect Employees.

There is no comprehensive federal privacy law that applies to personal information in every sector.[210] In the United States, many of the biggest technol*ogy companies, including Facebook, Apple, and Google, support the develop*ment of new federal legislation designed to protect consumer data privacy,[211] although some have suggested that their support is designed to preempt even stronger state laws.[212] This article stresses the importance of federal privacy protections in the workplace, and the sudden

208. *See* Brown, *supra* note 26, at 212.

209. Anecdotal evidence suggests that when companies offer free food, limiting the options to healthier food may annoy employees. *See, e.g.*, Kathy Gurchiek, *Free Food Is a Tasty Benefit at Some Companies*, HR NEWS (Mar. 29, 2019), https://perma.cc/P3MD-2X4C (noting that one office manager who replaced custom food orders with a "curated healthy snack-box delivery service" faced an "officewide revolt").

210. Nuala O'Connor, *Reforming the U.S. Approach to Data Protection and Privacy*, COUNCIL ON FOREIGN REL. (Jan. 30, 2018), https://perma.cc/E24Y-QBTX.

211. Russell Brandom, *Tim Cook Wants a Federal Privacy Law — but So Do Facebook and Google*, VERGE (Oct. 24, 2018), https://perma.cc/RTT2-B4HM.

212. Bennett Cyphers, *Big Tech's Disingenuous Push for a Federal Privacy Law*,

prevalence of COVID-19 highlights its relevance.[213] As this new legislation is developed, there is every reason to expand its scope to encompass the protection of employee data from unauthorized employer surveillance. This protection should extend to biometric and health data collected through the kinds of evolving technologies described in Part II.

One potential model for the United States as it considers employee data protection laws is the European Union's data privacy law. In the EU, it is legal for employers to collect data about their workers subject to a series of conditions. Under the General Data Protection Regulation (GDPR), which went into effect on May 25, 2018, data cannot be collected from workers without their valid consent.[214] Because worker monitoring will likely be considered "high risk" processing, the employers must first conduct and document a detailed privacy impact assessment (PIA).[215] In addition, various countries within the EU have heightened protection policies above and beyond the GDPR. For example, Germany has more restrictive laws, including the Secrecy of Telecommunications Act, which make it a criminal offense to review the personal emails of employees.[216] In any event, employers in the EU are well advised to warn workers explicitly about any intention to monitor data whether or not that data relates strictly to employment-related communications.[217]

ELECTRONIC FRONTIER FDN. (Sept. 18, 2019), https://perma.cc/6ZT7-5EEU; *see also* Michael Beckerman, Opinion, *Americans Will Pay a Price for State Privacy Laws*, N.Y. TIMES (Oct. 14, 2019), https://perma.cc/VU69-MMTV (Beckerman is President and CEO of the Internet Association, which "represents social media companies, sharing economy platforms, e-commerce businesses and commercial cloud providers").

213. Allison Grande, *How COVID-19 Is Set to Reshape Federal Privacy Law Debate*, LAW360 (Apr. 27, 2020), https://perma.cc/C2BE-K43E.

214. *See* Commission Regulation 2016/679 of Apr. 27, 2016, Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC, 2016 O.J. (L 119/1) ¶ 40.

215. *See e.g.*, *Employee Monitoring Update*, TAYLOR WESSING: GLOBAL DATA HUB (Mar. 2017), https://perma.cc/PL45-8L2S.

216. *Id.*

217. *See, e.g.*, Bărbulescu v. Romania, No. 61496/08, Eur. Ct. H.R. (2016), https://perma.cc/5K6Z-MC9M (finding that an employee had a reasonable expectation of privacy in personal calls, emails, and internet usage absent a specific warning from his employer that his "private life and correspondence" would be monitored, which the employer provided).

Some U.S. legislators have already suggested that the United States follow the EU's lead in a more limited regard.[218] In November 2018, Oregon Senator Ron Wyden introduced a bill that was modeled after some provisions of the GDPR, but its name conveyed a more limited scope of protection: the Consumer Data Privacy Act.[219] The focus of this proposed law was squarely on consumer data rather than employee data. Its provisions included a requirement that the biggest companies (defined by having more than $1 billion in revenues or storing data on more than fifty million consumers) submit annual reports describing their data protection practices to the Federal Trade Commission, as well as a requirement to comply with "do not track" policies.[220] Although that bill did not pass, Wyden introduced a second bill known as the "Mind Your Own Business Act" in October 2019.[221] This was also modeled on the GDPR and also focused on consumer rather than employee data privacy.[222]

Similarly, the collection of biometric and health data in Canadian workplaces is limited by both the Personal Information Protection and Electronic Documents Act (PIPEDA), which applies to private sector organizations, and the Privacy Act, which applies to the public sector.[223] The Canadian government identifies "providing benefits to employees" as a purpose that private organizations must identify specifically before getting valid, informed consent from employees in order to comply with PIPEDA.[224] Ontario, New Brunswick, and Newfoundland and Labrador

218. Danielle Abril, *This Is What Tech Companies Want in Any Federal Data Privacy Legislation*, FORTUNE (Feb. 21, 2019), https://perma.cc/QM5V-5RY3.

219. Robert Hackett, *Sen. Wyden Proposed a CEO-Felling Data Privacy Law. Is Big Tech Ready for It?*, FORTUNE (Nov. 3, 2018), https://perma.cc/E4DH-JFP3.

220. *Id.*

221. *See* Teri Robinson, *Mind Your Own Business Act Beefs Up Privacy Protections, Gives Consumers Dominion Over Data, Punishes Execs*, SC MEDIA (Oct. 19, 2019), https://perma.cc/NSW3-G67H.

222. *Id.*

223. Personal Information Protection and Electronic Documents Act, S.C. 2000, c 5 (Can.); Privacy Act, R.S.C. 1985, c P-21, amended by S.A. 2018 (Can.).

224. OFF. OF THE PRIVACY COMMISSIONER OF CAN., PRIVACY TOOLKIT (Dec. 2015), https://perma.cc/DE39-M4RQ.

have provincial laws that provide similar protections but are more specifically focused on personal health information.[225] In sum, there are several models the United States might follow in developing federal privacy legislation that protects both consumers and workers from data misuse.

VI. ADDITIONAL ISSUES AND CONCLUSION

The coronavirus pandemic that began in early 2020 underscores the urgency of the health data privacy and potential discrimination issues raised in this article. As offices reopen across the United States, an increasing number of workplaces are likely to institute health screening measures.[226] They may be compelled to do so in order to protect their employees from infection and to protect themselves from lawsuits brought by employees who get infected nonetheless.[227] The EEOC issued new guidance in March 2020 permitting mandatory testing of employees for COVID-19 before allowing them to return to the workplace and permitting testing of job applicants for COVID-19 symptoms.[228] As a result, workplace monitoring of biometric and health data may expand exponentially in the coming years, making the protection of such data a critical issue.

Existing legal frameworks do too little to curb potential misuse of biometric and health monitoring, threatening the trust relationship between employers and workers and raising the risk of adverse employment actions tainted by bias and error. As the sensor-laden workplace expands, and employers use technology that makes it easy for them to

225. *Id.* at 2.

226. Konrad Putzier & Chip Cutter, *Welcome Back to the Office. Your Every Move Will Be Watched.*, WALL ST. J. (May 5, 2020, 10:48 AM), https://perma.cc/K78Z-ESBN.

227. Amanda Robert, *Can Companies Be Held Liable When Their Employees Fall Ill with the Coronavirus?*, ABA J. (Mar. 19, 2020), https://perma.cc/RG4L-WD9E; *see also* Debra Cassens Weiss, *Nearly 800 COVID-19 Lawsuits Have Been Filed, According to Law Firm's Tracker*, ABA J. (May 4, 2020), https://perma.cc/N6N6-ZGL4 (noting that employment cases relating to COVID-19 are among those "[o]n the upswing").

228. U.S. EQUAL EMP'T OPPORTUNITY COMM'N, PANDEMIC PREPAREDNESS IN THE WORKPLACE AND THE AMERICANS WITH DISABILITIES ACT (Mar. 21, 2020), https://perma.cc/6UDD-UUEP.

gather an expanding range of biometric data about their workforce and combine it with other sources of health data, the potential for damage to both companies and workers is likely to increase unless we opt for new solutions. Which solution or solutions we choose may be influenced by a number of factors.

Limiting the advancement of monitoring technology would be unwise and impossible. The market is expanding and will respond to continued consumer, employer and medical demand. The science behind wearables promises to offer new ways to detect disease earlier than ever before, improving doctors' ability to flag and treat a wide variety of health problems.[229] In April 2020, Stanford Medicine, Fitbit, and Scripps Research announced a new effort to use wearables to detect early signs of infection which could curb the spread of diseases including COVID-19.[230]

In coming years, it is possible that health monitors may become less susceptible to workplace misuse. Manufacturers may become better equipped and more motivated to manage user data safely and protect it from downstream misuse even if they are not legally compelled to do so. They may choose to enhance security, for example, to gain a competitive advantage by increasing users' trust and confidence. Similarly, users may demand greater access to their collected data and the algorithms used to draw conclusions about them, possibly lowering the rate of error and providing a platform for employers and employees to have more open discussions about evaluative processes. Increased disclosure about the nature and use of data collected is likely to benefit employers in a number of ways, increasing their likely compliance with privacy laws (which often require notice of use) and the Fair Labor Standards Act (which limits the hours of "work" that monitoring may blur).[231]

---

229. Hanae Armitage, *Stanford Medicine Scientists Hope to Use Data from Wearable Devices to Predict Illness, Including COVID-19*, STAN. MED. (Apr. 14, 2020), https://perma.cc/AQ6N-8VCF.

230. *Id.*

231. Allen Smith, *How to Limit Wearable Technology's Legal Risks*, SOC'Y FOR HUM. RESOURCE MGMT. (May 29, 2018), https://perma.cc/5RU7-6R3M.

Even if worker awareness grows alongside the reach of monitoring technology, it is critical that we develop a comprehensive approach to keeping potential data misuse in check. Sensibly regulating biometric data surveillance in the workplace will have a significant impact on the workplace. If done correctly, it will improve the accuracy of predictive analytics, protect employees from both data-based discrimination and privacy violations, and provide an understandable framework for evolving technological advances in this field.

The long-term costs of failing to regulate these innovations in data collection will be far greater to both employers and employees than the short-term ease of avoidance. In order to maintain the trust inherent in the employer-employee relationship, we must determine how best to minimize the potential harms of biometric and health monitoring in the workplace. This article offers specific options for lawmakers, scholars, employers and workers to consider as they develop an intentional strategy rather than passively being led by technological advances.