UC Law Business Journal

Volume 20 | Number 1 Article 4

1-2024

Protecting Worker Health Data Privacy From The Inside Out

Elizabeth A. Brown

PROTECTING WORKER HEALTH DATA PRIVACY FROM THE INSIDE OUT

Elizabeth A. Brown[*]

This article investigates three new opportunities for complementary public, private, and design-centric protections of worker health data, an overlooked yet critical area of data privacy regulation. The expansion of biometric monitoring, of the $50 billion femtech industry, and the commercial value of health data also underscore the need for greater protection of worker health data. Now that states are developing more comprehensive data privacy laws, it is critical to consider innovative solutions that build on the best of these laws nationwide. Especially after the Supreme Court's Dobbs decision, the health data of women workers has become especially prone to misuse. This article proposes a three-part solution to protect worker health data more effectively. First, privacy by design requirements used for protecting children's data should be adapted to limit the unprotected health data that apps and websites store. Next, the U.S. should adopt a federal law comparable to the California Privacy Rights Act to limit the collection and use of worker health data. Finally, incentives should encourage employers to offer enhanced privacy protections to their workers as a perk, for competitive advantage, and as a novel form of corporate social responsibility.

[*] Professor of Law, Bentley University, Waltham, MA.

TABLE OF CONTENTS

INTRODUCTION

Sheryl works out four times a week, and tracks all of her steps on the smartwatch that her employer provided to her. Because she does not want to get pregnant, she also uses a period tracker to help her remember when her next period is likely to start. Her colleague, Tom, has been feeling tired at work, so he checks a program on his phone that helps him track how often he wakes up during the night. He runs searches for "sleep apnea causes" on his laptop. Tom also uses a popular meditation app to help him control his stress by doing breathing exercises during the workday, as well as guided meditations in the evenings.

Sheryl and Tom are both using their phones, laptops, and smartwatches to take care of their health. In doing so, they are generating health data that is not covered by HIPAA or any other federal privacy law and providing their employer with a wide range of data that it can use to make decisions about them, with no real legal ramifications. The health data of employees like Sheryl and Tom is not subject to the same kinds of privacy protection that consumer data is, in almost every part of the United States. It is increasingly risky for both employers and employees to leave that data unprotected.

How businesses protect the health data privacy of their workers has never been more critical. The increasing facility with which employers can access this data, whether through health data brokers, worker's voluntary disclosures online, or through their own collection via workplace wellness programs, and other methods underscores the need for health data security. For women and the people who care about them, reproductive health data privacy is becoming more critical as states move to criminalize abortion in the wake of Dobbs. Other factors, like the increasing prevalence of biometric monitoring and the emerging role of AI in workplace automation that may incorporate worker health data, all increase the urgency with which policymakers and employers must look for comprehensive solutions.

This article takes a comprehensive look at current options for the protection of worker health data privacy in the United States and suggests a three-part plan for reform. It uses an interdisciplinary approach by incorporating management and human resources concerns that must be considered when developing technological schema for the protection of worker health data, in order to maximize chances of successful adoption.

A threshold issue is what we mean when we talk about "health data." There is some debate as to whether the term "health data" is broad enough to encompass the full range of information that can support inferences about a person's health. People generate data every day that relates to their health, from their smart watches to online searches about health conditions to posts on social media about their aches, pains, and depression. According to one view, the traditional "term 'health data' has referred to information produced and stored by healthcare provider organizations," yet "vast amounts of health-relevant data are collected from individuals and entities elsewhere, both

passively and actively."[1] In this paper, I use the term "health data" broadly to refer to data that is relevant to a person's physical or mental health, as opposed to the narrower traditional definition.

While most regulatory discussions of data privacy in the United States focus on consumer data privacy, there has been comparatively little attention to the privacy needs of workers, whether or not they are classified as employees. Given the synthesis of trends such as the commodification of health data, the growth of biometric monitoring at work, the explosive growth of femtech as a major market and a component of wellness programs, and the criminalization of abortion in some states, protecting the health data privacy of workers has never been more important. The growth of hybrid and remote work in the post-COVID era also makes worker health data privacy an increasingly complex concern.

Fortunately, regulating the technological aspects of worker health data privacy in meaningful ways is a more realistic prospect now than it had been prior to the advent of online health records. Until recently, worker health data was primarily protected by HIPAA and some state privacy laws, all of which have significant shortcomings in this context. In 2023, however, some states began to fill these regulatory gaps. This article examines the benefits and shortcomings of these new approaches as a basis for improved federal statutory protection.

I propose three potential complementary reforms to improve the privacy of worker health data. First, this article proposes the adoption of privacy by design requirements for all apps and websites that collect health data. Regulations to protect the data privacy of children by requiring certain design principles exist in the U.K. and are beginning to emerge at the state level in the U.S. These privacy by design principles could be extended to sources of health data collection as well.

Secondly, this article proposes to expand the worker data protections provided by a new California law to the federal level, including the provision of new rights for workers regarding their health data and a private right of action to enforce them. Federal regulatory options, however, are complicated by a number of factors including preemption and a lack of clarity about which federal agencies might have primary responsibility for reform.

The third proposal is the development of stronger corporate health data privacy policies that employers might adopt as a recruitment tool. Well-accepted privacy protection principles could be used as the basis for such policies. The benefits of offering privacy as a perk, beyond a company's legal obligations, may outweigh the development and compliance costs. At the same time, that benefit risks exacerbating the existing socioeconomic divide between those who are more likely to be surveilled and those who are not. Enhancing

1. Deven McGraw & Kenneth Mandl, *Privacy Protections to Encourage Use of Health-Relevant Digital Data in a Learning Health System*, NPJ DIG. MED. (Jan. 04, 2021), https://www.nature.com/articles/s41746-020-00362-8#citeas.

privacy beyond legal requirements can also provide a competitive advantage and bolster an employer's corporate social responsibility program.

I. HEALTH DATA PRIVACY REQUIRES PROTECTION AT WORK

In the course of a normal day, like Sheryl and Tom, you might use your smartwatch or phone to keep track of many things you might not think of as "health data." You might keep track of your steps, or have an app take care of that for you. Another app might tell you how well you slept last night because that kind of thing is hard to figure out on your own. Your watch might alert you when your heart rate becomes elevated, perhaps during a meeting with your boss. You might post to one of your online communities that you have been feeling depressed, or that one of your kids is out of sorts. You might use a search engine to look up the nearest reproductive care clinic or where to get abortion pills online.

All of this information functions as personal health data. It can be used to draw conclusions about your physical and mental health and possibly that of your family members. Together, with your geolocation data and other kinds of information that can serve to identify you personally, it can tell a powerful story about who you are. That story can be embellished, shared, bought, sold, and traded in ways you may never understand or have an opportunity to witness. Although it is not generated by medical professionals and is not always subject to the same kinds of protections as medical records, which are, of course, also health data, these less formal kinds of personal health data can be used in innumerable ways.

Health data is one of the most sensitive and valuable kinds of personal information. As the Federal Trade Commission recognized in a recent statement, information about a person's health is "among the most sensitive categories of data collected by connected devices."[2] An increasing variety of devices can provide health data to entities that collect, process, interpret, and sell that data in almost unlimited ways. When that health data is combined with other common types of personal information, such as geographic location, there is an even wider range of commercially valuable applications.

Both workers and employers should be concerned about the potential misuse of health data. Focusing on the possible abuses of health data in the workplace is critical for at least three reasons. First, there are a myriad of ways in which employers can use the health data of their workforce. Many of these uses are beneficial,tending to increase productivity and/or improve workers' wellbeing. Many other uses are less clearly beneficial, or tend to benefit the

2. Kristin Cohen, *Location, Health, and Other Sensitive Information: FTC Committed to Fully Enforcing the Law Against Illegal Use and Sharing of Highly Sensitive Data*, FED. TRADE COMM'N. (July 11, 2022), https://www.ftc.gov/business-guidance/blog/2022/07/location-health-and-other-sensitive-information-ftc-committed-fully-enforcing-law-against-illegal [hereinafter Location, Health, and Other Sensitive Information].

employer at the worker's potential expense[3] Secondly, the marketplace for health data and other data with which it can be interpolated, including geolocation, is both vast and opaque.[4] Additionally, few laws in the United States effectively prevent misuse.

A. *Employers Increasingly Collect Health Data from Workers*

In the United States, the relationship between employment and health data is complex. Employers have a substantial interest in the health, often reflected by health data, of their work force. This is partly because there is a significant link between work and health insurance in this country. Companies employing more than 50 people are required to provide some form of health insurance under the employer mandate of the Affordable Care Act.[5] Indeed, nearly half of Americans get health insurance from their employer.[6] Although that percentage has been trending slightly down over the last 15 years, it remains significant.[7] The second most common source of health insurance is Medicaid, covering 21% of the population.[8]

When employers bear the costs of providing health insurance to their workers, they have a financial incentive to ensure that those workers are as healthy as possible. Workers who maintain their physical and mental health, employers have long believed, will be more productive and less expensive to insure. The most common practice associated with this belief is the provision of workplace wellness programs, examined in more detail below. The potential uses of this health data threaten workers' privacy, employment opportunities, and long-term wellbeing.[9]

There are two other factors enmeshing work and health data. One is that employers sometimes have a legal obligation to monitor the health or health-related data of their workers. The other is that it is easier than ever to keep track of workers' health-related data due to the expansion of biometric monitoring.

i. Wellness Programs and Brokers Facilitate Health Data Collection

Health data is relatively easy for employers to collect outside of HIPAA protections. The first point of collection is through apps and devices that employers issue as part of workplace wellness programs or in the ordinary

3. *See generally* Elizabeth A. Brown, *Workplace Wellness: Social Injustice*, 20 N.Y.U. J. LEGIS. & PUB. POL'Y 1 (2017).

4. Cohen, supra note 2.

5. *See generally* Patient Protection and Affordable Care Act, Pub. L. No. 111-148 (2010).

6. Vaughn Himber, *Employer-Sponsored Health Insurance Statistics: What the Data Tells Us*, E-HEALTH INS. (Oct. 20, 2022), https://www.ehealthinsurance.com/resources/small-business/how-many-americans-get-health-insurance-from-their-employer.

7. *Health Insurance Coverage of the Total Population*, KFF, https://www.kff.org/other/state-indicator/total-population (last visited Aug. 12, 2023).

8. *Id.*

9. Brown, *supra* note 3, at 9.

course of business. An increasing number of employers deploy workplace wellness programs in an effort to lower their health insurance costs, reduce absenteeism, improve productivity, and benefit the business in other ways associated with a healthier workforce. Although research has shown that workplace wellness programs may not actually result in long-term cost reductions[10], they remain popular.

As part of these workplace wellness programs, many employers provide their workers with access to health-related apps that workers may access either on their personal devices or on phones, tablets, and laptops that their employers provide. For example, a company may offer its workers free access to Calm, Headspace, or a similar meditation app that the worker and her entire family may use. Data from some health-related apps can be collected from both the mobile operating system and from the software development kits (SDKs) that collect location information and provide it to third parties.

A second point of collection is through data brokers. Health data is one of many kinds of information that some third-party companies aggregate and sell. Data brokers profit by building profiles of individual users that suggest certain tendencies about them, and inferences about what they are likely to do and buy based on what data shows about their past behaviors. This predictive information can then be sold onward to companies who plan to market to identifiable parties based on these predictions.

What employers do with the health data they receive from data brokers is largely unregulated. Many data analytics companies are in the business of helping employers interpret the data they collect, whether it is scraped internally or acquired. Even a well-meaning employer, concerned about the health of its employees, might find itself in possession of health data that has value in both positive and troubling ways. One health benefits analytics company, for example, describes the use case of an employer with a "hunch" that their workers "needed more help with behavioral or mental health conditions."[11] The analytics company could easily show them how a set of workers compares to the broader population using several markers that purportedly correlate with depression and anxiety, allowing the employer to identify the workers that struggle the most with those issues.[12] The employer might reach out to offer more support, or might instead use that data in combination with other factors to limit those workers' opportunities for advancement.[13]

---

10. Zirui Song & Katherine Baicker, *Effect of a Workplace Wellness Program on Employee Health and Economic Outcomes A Randomized Clinical Trial*, JAMA NETWORK (Apr. 26, 2019), https://jamanetwork.com/journals/jama/article-abstract/2730614.

11. *Big Data in Healthcare: How Employers, Providers, and Brokers Are Using Healthcare Analytics*, ARTEMIS HEALTH (Jan. 21, 2020), https://www.artemishealth.com/blog/big-data-in-healthcare-how-employers-providers-and-brokers-are-using-healthcare-analytics.

12. *Id.*

13. While employment discrimination on the basis of a disability like clinical depression or diagnosed anxiety would likely violate the ADA, it is often difficult for potential claimants to prove the kind of causal link between their disabilities and an adverse employment action that a successful ADA claim

ii. Worker Surveillance Expands While Data Protections Weaken

The Covid-19 pandemic helped to expand the ways in which employers track workers' health. When remote work became ubiquitous, workers became acclimated to certain kinds of digital surveillance. For example, some employers began monitoring their employees remotely for early signs of Covid-19, using small skin patches that can help detect a fever.[14] Employers also began using surveillance technology to determine whether employees were actually working while they were at home. PwC used a facial recognition tool to determine when their workers were away from their computer screens, including taking bathroom breaks.[15] The company justified their remote monitoring as necessary to help it meet compliance obligations.[16]

Employer monitoring is not the only source of health data about workers. Health data generated from personal devices also can be used as a basis for discrimination.[17] To the extent that health insurers require its collection, it can also lead to invasions of privacy through unauthorized data sharing by the insurer and the app developers.[18]

The trend of increasing the use of AI and algorithms in employment dovetails with the increasing collection and monitoring of health data in the workplace. From the moment candidates apply for a position, chatbots and other forms of AI, including video interviews scored by algorithms[19] and game-based and image-based assessments, are increasingly likely to evaluate them.[20] These automated evaluations may capture health data about the candidates that would be hard for the subjects to access or evaluate under current laws. Both New York City and Illinois have passed legislation limiting the use of automated candidate evaluations, but these systems are still likely to become more common across the country. Automated tools can also help write reports

---

requires.

14. David Cox, *The Rise of Employee Tracking*, BBC (Nov. 10, 2020), https://www.bbc.com/worklife/article/20201110-the-rise-of-employee-health-tracking.

15. Lucy McNulty & Trista Kelley, *PwC under Fire for Tech That Tracks Traders' Loo Breaks*, FNLONDON (June 15, 2020), https://www.fnlondon.com/articles/pwc-under-fire-for-tech-that-tracks-traders-loo-breaks-20200615.

16. *PwC Statement on Technology Compliance Tool*, PWC (June 16, 2020), https://www.pwc.co.uk/press-room/press-releases/tech-trader-tool.html.

17. Elizabeth Davidson et al., *Challenges and Opportunities with Governance of Personally Generated Health Data*, SCHOLARSPACE (2019), http://hdl.handle.net/10125/63535.

18. *See generally* Alexandra Troiano, *Wearables and Personal Health Data: Putting a Premium on Your Privacy*, 82 BROOK. L. REV. (2017).

19. Airlie Hilliard, Emre Kazim, Theodoros Bitsakis & Franziska Leutner, *Measuring Personality Through Images: Validating a Forced-Choice Image-Based Assessment of the Big Five Personality Traits*, 10 J. INTELLIGENCE 1, 12 (Feb. 7, 2022).

20. Dandara B. Palhano et al., *Identifying Player Personality Via a Serious Game A Pilot Study Using Item Response Theory*, PROC. OF SBGAMES 575, 575 (2019).

and monitor worker performance.[21] Legal and management scholars are calling for more and better governance of these tools as a general matter.[22]

The trend toward using more data in the workplace to monitor the actions and behaviors of workers, taken together with the increases in health data that employers can collect and use to evaluate workers, is a cause for concern. These two changes suggest that at least some employers in the United States may be moving toward a fully automated surveillance culture. In that light, the consequences of an unchecked worker health data market should spur the creation of more stringent protections in both the public and private spheres.

iii. Femtech Apps Create Monitoring Risks and Obligations

Femtech is a relatively new term that refers to the technology, including products, software, and services, that support women's health.[23] The market for femtech is growing at an explosive pace. According to one projection, the femtech market is expected to grow to 75 billion dollars worldwide by 2025- from a 2020 valuation of 40.2 billion dollars.[24] By the end of 2022, the global femtech market was estimated at 51.6 billion dollars, more than a third of the total valuation of digital health.[25] Women may get access to femtech through a workplace wellness program, offered by either their employer or their partner's employer, or through an app or website on a device that the employer monitors.

Although femtech apps are becoming ubiquitous, some have a questionable track record regarding data privacy.[26] In May 2022, a survey of digital privacy protections in period tracker apps found flaws in the privacy provisions of all five of the surveyed apps.[27] In January 2021, the developer of Flo, a period and fertility-tracking app, settled federal charges that it had misled users about its data security practices after sharing users' intimate health

---

21. *See* Andreas Schumacher & Wilfried Sihn, *Development of a Monitoring System for Implementation of Industrial Digitalization and Automation Using 143 Key Performance Indicators*, 93 PROCEDIA CIRP 1310 (2020).

22. *See, e.g.*, Emre Kazim & Adriano Soares Koshiyama, *A High-Level Overview of AI Ethics*, 2 PATTERNS, no. 9, Sept. 10, 2021, at 1.

23. Amy Olivero, *Privacy and Digital Health Data: The Femtech Challenge*, IAPP (Oct. 25, 2022), https://iapp.org/news/a/privacy-and-digital-health-data-the-femtech-challenge/.

24. Conor Stewart, *Global Femtech Market Revenue Between 2020 and 2025*, STATISTA (Sept. 14, 2023), https://www.statista.com/statistics/1125599/femtech-market-size-worldwide/.

25. *Digital Health – Worldwide*, STATISTA, https://www.statista.com/outlook/dmo/digital-health/worldwide (last visited Aug. 16, 2023).

26. *See* Elizabeth A. Brown, *The Femtech Paradox: How Workplace Monitoring Threatens Women's Equity*, 61 JURIMETRICS 289 (2021) for a broader discussion of the threats of Femtech to women at work.

27. Catherine Roberts, *These Period Tracker Apps Say They Put Privacy First. Here's What We Found.*, CONSUMER REPORTS (Aug. 30, 2022), https://www.consumerreports.org/health-privacy/period-tracker-apps-privacy-a2278134145/.

details with Facebook and Google.[28] In 2020, the California Attorney General reached a $250,000 settlement with Glow, Inc. after alleging that the femtech app's "serious privacy and basic security failures" put users' "sensitive personal and medical information at risk."[29]

When the U.S. Supreme Court removed the federal constitutional right to abortion in *Dobbs v. Jackson Women's Health Organization*,[30] the risks for both women workers of childbearing age and their employers increased. As some states began to criminalize abortion, many employers announced that they would support their workers by helping them finance travel to states where they could still get abortions legally. At this writing, over one hundred employers offer substantial abortion care benefits.[31]

Post-*Dobbs* abortion laws have created new risks for employers who want to help their workers get abortions at both the state and federal levels. In July 2022, for example, a faction of conservative Texas legislators informed Lyft and Sidley Austin, a law firm, that it was illegal to provide certain benefits to their workers in relation to abortion access.[32] In that letter, the legislators warned that Texas was likely to pass more laws criminalizing the provision of abortion access benefits to workers. The federal government is concerned as well. In November 2022, the Commissioner of the EEOC began to target companies providing abortion benefits, alleging that those employers might be discriminating against pregnant and disabled workers by not offering equivalent benefits for their medical needs.[33]

Employers also face compliance risks relating to their insurance plans if they provide abortion care. Whether they may do so without violating the federal Employee Retirement Income Security Act (ERISA) depends in part on whether they are fully insured or self-insured. It also depends on how federal courts interpret the provision of the Affordable Care Act (ACA) which requires certain fully insured health plans to cover essential health benefits. If states determine that abortion is an essential health benefit, that would facilitate insurance coverage.[34]

---

28. Natasha Singer, *Flo Settles F.T.C. Charges of Misleading Users on Privacy*, N.Y. TIMES (Jan. 13, 2021), https://www.nytimes.com/2021/01/13/business/flo-privacy.html.

29. Jerry Beilinson, *Glow Pregnancy App Exposed Women to Privacy Threats, Consumer Reports Finds*, CONSUMER REPORTS (Sept. 17, 2020), https://www.consumerreports.org/mobile-security-software/glow-pregnancy-app-exposed-women-to-privacy-threats-a1100919965/.

30. Dobbs v. Jackson Women's Health Org., 597 U.S. 2240, 2284 (2022).

31. *#WhatAreYourReproBenefits*, RHIA VENTURES (Aug. 16, 2023), https://rhiaventures.org/corporate-Engagement/whatareyourreprobenefits/.

32. Poppy Noor, *Texas Lawmakers Test How Far Their Threats Against Abortions Can Reach*, THE GUARDIAN (July 24, 2022), https://www.theguardian.com/us-news/2022/jul/23/texas-republican-lawmakers-legal-threats-abortions.

33. J. Edward Moreno, *EEOC Official Quietly Targets Companies Over Abortion Travel*, BLOOMBERG LAW (Nov. 14, 2022), https://news.bloomberglaw.com/daily-labor-report/eeoc-official-quietly-targets-companies-over-abortion-travel-20.

34. Stephen Miller, *Employers Providing Abortion Benefits Should Address Compliance Questions*, SHRM (June 29, 2022), https://www.shrm.org/resourcesandtools/hr-topics/benefits/pages/employers-providing-abortion-benefits-should-address-compliance-questions.aspx. Although it is possible that states

In fact, restrictive state abortion laws may require employers to monitor their workers more closely with regard to their reproductive care. In the states with laws restricting or limiting abortion, including Alabama, Kentucky, Louisiana, Mississippi, North Dakota, Oklahoma, Texas, and South Carolina, people or entities may face "aiding and abetting" liability for assisting women in obtaining an abortion.[35] The extent to which employers might be liable in these states for "assisting" employees who wish to obtain an abortion by, for example, providing laptops or travel coverage is not yet clear. At the same time, the federal government is trying to prevent health care providers and insurers from turning over information that might help state officials prosecute women for seeking or providing a legal abortion.[36] All of these developments underscore the importance of ensuring that data related to reproductive health is treated with particular care.

Data brokers can be particularly threatening in the context of reproductive health data. Workers can be tracked and targeted when they look up certain information online or when they visit reproductive health clinics, although this practice may violate state laws. For example, in 2017, the Massachusetts Attorney General reached a settlement with Copley Advertising based on allegations that Copley had used geofencing to identify people who had come within a certain range of reproductive health facilities in five large urban areas.[37] "Geofencing" is the practice of using geographic location as a kind of trip wire to send specific kinds of advertisements through browsers and apps. According to the Attorney General's office, Copley had then pushed a series of targeted advertisements to those people, including texts saying "Pregnancy Help" and "You Are Not Alone."[38] When a user clicked on these text advertisements, they were connected to a live web chat with a "pregnancy support specialist" and provided with information about alternatives to abortion.[39] This practice, the Attorney General alleged, violated Massachusetts laws that bar tracking individuals' physical location near or within medical facilities.[40]

While Massachusetts law may have barred that practice, federal law does not. A 2022 investigation by the Washington Post revealed that many popular

---

could also deem abortion-related travel to be an essential health benefit, further facilitating the provision of such benefits, this seems less likely in states that have criminalized abortion in the first place.

35. Mary Cassidy et al., *Issues for Employers After Dobbs v. Jackson Women's Health Organization*, ARNOLD & PORTER, (July 18, 2022), https://www.arnoldporter.com/en/perspectives/advisories/2022/07/issues-for-employers-after-dobbs-v-jackson.

36. HIPAA Privacy Rule to Support Reproductive Health Care Privacy, 88 Fed. Reg. 23506 (proposed Apr. 17, 2023) (to be codified at 45 C.F.R. pts. 160, 164).

37. Press Release, Office of the Attorney General, AG Reaches Settlement with Advertising Company Prohibiting 'Geofencing' Around Massachusetts Healthcare Facilities, Massachusetts (Apr. 4, 2017), https://www.mass.gov/news/ag-reaches-settlement-with-advertising-company-prohibiting-geofencing-around-massachusetts-healthcare-facilities.

38. *Id.*

39. *Id.*

40. *Id.*

health apps shared user identifier information with dozens of advertising companies.[41] For example, The Post found that Drugs.com's app for Android users was sending data to more than 100 outside entities including terms such as "diabetes," "herpes," and "adderall" in conjunction with data that identified the specific devices used for the search. As the investigation noted, and as I discuss in more detail below, HIPAA does not prohibit these data transfers.

When users first sign up for these apps, they click a box indicating that they agree to the terms and conditions of the apps' use. As anyone who has ever clicked on such a box knows, it is practically impossible to review these terms and conditions in a meaningful way if you want to use the app. It is also difficult for most people who are not lawyers to review privacy policies.[42] Yet agreeing to the app's terms and conditions generally precludes the user from complaining that they have not consented to the disclosure of their information if the policy allows for such disclosure.

Moreover, there is no guarantee that the health apps are actually abiding by their own policies, although it would be difficult for an individual user to prove otherwise. The Washington Post's investigation, for example, uncovered at least one striking example of disregard. In one case, Drugs.com was found to be transferring the first and last name of a user (a fake profile used for testing) to an outside company.[43] When the Post pointed out that this appeared to contradict Drugs.com's ."

iv. Employers May Misunderstand Regulatory Obligations

Another challenge for protecting worker health data is that employers themselves may have a poor grasp of the data they control relating to their own workforce. Employers are often in a precarious position when it comes to monitoring the health data of their workers, whether that is their workers' Covid-19 vaccination status or any other kinds of information. They may struggle to understand their compliance obligations, including the differences between guidelines and regulation. With regard to data collection, they may not fully understand what data they have and how that data is being stored or processed.

In some cases, they may not even want to collect certain kinds of health information that they are required by law to keep. For example, during the Covid-19 pandemic, OSHA required some employers to conduct health checks and contact tracing. At the time, the president of one health data technology firm noted that employees were nervous about this data collection

41. Tatum Hunter & Jeremy Merrill, *Health Apps Share Your Concerns with Advertisers. HIPAA Can't Stop It*, WASH. POST (Sept. 22, 2022, 7:00 AM), https://www.washingtonpost.com/technology/2022/09/22/health-apps-privacy.

42. Geoffrey Fowler, *I Tried to Read All My App Privacy Policies. It Was 1 Million Words*, WASH. POST (May 31, 2022), https://www.washingtonpost.com/technology/2022/05/31/abolish-privacy-policies/.

43. Hunter & Merrill, *supra* note 41.

and "[c]ompanies[44] He added that "it sets them up for more legal repercussions if handled incorrectly."[45]

Many employers use an automated platform to ensure compliance with the European Parliament's General Data Protection Regulation (GDPR), the California Privacy Rights Act of 2020 (CPRA) and other regulatory obligations. Truyo is one such platform, funded in part by Intel. Truyo claims to offer businesses the ability to manage all of their employment data with a product that combines "AI connectors" with a data scanner to "locate, tag, and automate your employment data responses – all within scope of upcoming legislation."[46] By "upcoming legislation," they presumably mean CPRA, which took effect on January 1, 2023.

But companies may also turn to outside analytics companies to help them interpret health data in more troubling ways as well. In 2016, for example, Wal-Mart was reported to have engaged Castlight Healthcare Inc. to collect and analyze employee data to predict which workers were more likely to get sick and to direct those workers toward health management services.[47] Castlight was reported to be helping other employers to track their workers' pregnancies.[48]

Health data mapping is easily outsourced. It may be done through human resources management software (HRMS) or to virtually any extent by outside providers such as Truyo. At the 2023 Global Privacy Summit of the International Association of Privacy Professionals (IAPP), one of the world's largest privacy professional associations, more than one hundred vendors of privacy management software marketed their wares to the privacy officers and other professionals tasked with maintaining data privacy who attended from around the world.[49] The widespread distribution of privacy management functionality tends to increase the distance between upperlevel corporate management and the day-to-day control of an entity's data privacy. As a result, senior leadership may have little idea of the worker health data their entities are collecting in the first place.

---

44. Leila Hawkins, *Truyo: Checking Employee Health Without Violating Privacy*, HEALTHCARE (Feb. 28, 2021), https://healthcare-digital.com/digital-healthcare/truyo-checking-employee-health-without-violating-privacy.

45. *Id.*

46. *Employment-Related Data Management*, TRUYO, https://truyo.com/solutions/employment-related-data-management (last visited Mar. 29, 2023).

47. Rachel Emma Silverman, *Bosses Tap Outside Firms to Predict Which Workers Might Get Sick*, WALL ST. J. (Feb. 17, 2016, 7:58 PM ET), https://www.wsj.com/articles/bosses-harness-big-data-to-predict-which-workers-might-get-sick-1455664940.

48. Valentina Zarya, *Employers Are Quietly Using Big Data to Track Employee Pregnancies*, FORTUNE (Feb. 17, 2016, 5:36 pm), https://fortune.com/2016/02/17/castlight-pregnancy-data/.

49. *IAPP Global Privacy Summit 2023*, IAPP, https://iapp.org/conference/global-privacy-summit/ (last visited Apr. 19, 2023).

B. *Few Laws Protect the Privacy of Health Data Employers Collect*

Scholars have been cautioning about the potential misuse of health data collected from wearable devices for years.[50] Federal law, however, has not changed significantly to protect workers or anyone else from such consequences.

i. HIPAA Offers Insufficient Coverage in the Workplace

A common misconception is that the Health Insurance Portability and Accountability Act (HIPAA) protects against the disclosure and misuse of health data in general. In fact, HIPAA's scope leaves a great deal of health data unprotected.[51] Adopted in 1996, HIPAA focuses on maintaining the privacy of electronic health data that is generated by and for a defined range of "covered entities."[52] These covered entities include health care providers and health plans, [53] Even when HIPAA has been updated, these gaps have remained. In 2009, for example, when the Health Information Technology for Economic and Clinical Health Act (HI-TECH) came into effect and updated certain HIPAA provisions, the statutory focus remained on protecting only clinical health data and only in limited contexts.[54]

According to guidance issued by the U.S. Department of Health and Human Services (HHS), HIPAA does not generally protect the privacy of health data stored on mobile phones or tablets, nor does it protect the privacy of internet searches related to health issues.[55] While HIPAA initially may protect the confidentiality of health data that a doctor records, such as a blood pressure reading or a cholesterol level recording, that protection is lost once a

---

50. *See, e.g.*, Elizabeth A. Brown, *The Fitbit Fault Line: Two Proposals to Protect Health and Fitness Data at Work*, 16 YALE J. HEALTH POL'Y L. & ETHICS 1 (2016); Nayanika Challa et al., *Wary About Wearables: Potential for the Exploitation of Wearable Health Technology Through Employee Discrimination and Sales to Third Parties*, 10 Intersect, July 7, 2017, at 1.

51. *See* Health Insurance Portability and Accountability Act (HIPAA) of 1996, Pub. L. No. 104- 191, 110 Stat. 1936 (codified as amended in scattered titles of the U.S Code), amended by Health Information Technology for Economic and Clinical Health Act (HITECH), Pub. L. No. 111-5, 123 Stat. 226 (2009) (codified as amended in various sections of 42 U.S.C.); HHS's privacy regulations, which implement section 264© of HIPAA, are codified at 45 C.F.R. §§ 164.500–.534; Kim Theodos & Scott Sittig, *Health Information Privacy Laws in the Digital Age: HIPPA Doesn't Apply*, 18 PERSP. IN HEALTH INFO. MGMT. Dec. 7, 2020, at 1.

52. *See* 45 C.F.R. § 160.103 (2018); 45 C.F.R. § 160.102(a)-(b) (2018) (applying HIPAA rules to covered entities and their business associates).

53. Theodos & Sittig, *supra* note 51.

54. *Special Topics: HITECH Act Enforcement Interim Final Rule*, U.S. DEP'T. OF HEALTH & HUM. SERVS. (June 16, 2017), https://www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html.

55. *Protecting the Privacy and Security of Your Health Information When Using Your Personal Cell Phone or Tablet*, U.S. DEP'T. OF HEALTH & HUM. SERVS. (June 29, 2022), https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/cell-phone-hipaa/index.html.

person downloads that information onto a phone or other personal device.[56] Combinations of data, including email or IP addresses and search terms, are also unprotected by HIPAA, a concern expressed by the director of the HHS' Office for Civil Rights in April 2023. She noted that her office was "seeing people go in and type symptoms, put in information, and that information is being disclosed in a way that's inconsistent with HIPAA and being used to potentially track people, and that is a problem."[57]

Another limitation of HIPAA in this context is that it does not apply to small employers. With regard to workplace wellness plans, an employee welfare benefit plan that has fewer than 50 participants is not considered a "group health plan" within the scope of the HIPAA Rules.[58] People who work for smaller employers therefore may not be protected by HIPAA at work.

In addition, HIPAA may not protect health data that has been de-identified, or unlinked from a particular individual, even when that data can be re-identified after its sale to another entity to recreate a personal association. The definition of individually identifiable health information, however, does encompass data that either identifies the individual directly or for "which there is a reasonable basis to believe the information can be used to identify the individual."[59]

ii. Federal Responsibility For Worker Health Data Privacy Is Diffuse

If worker health data is so sensitive and prone to misuse, why does it receive so little legal protection? Several factors are relevant here. The first is a comparative lack of public concern. Worker data privacy in general receives less attention from lawmakers in the United States than customer or consumer privacy. Although there is no comprehensive federal data privacy law at this writing, the data privacy bills that have been introduced into Congress have largely focused on the privacy concerns of people who use online services such as Facebook and Amazon as consumers. This is in part because concerns about data privacy have been fueled in the United States by outrage over the data leaks at Facebook and by concerns about the algorithms used to determine things like mortgage rates and other issues that affect people in all aspects of their lives, not just their working lives. While some health data privacy protection measures have been introduced, they have failed to gain traction in Congress. It is also in part because the agency charged with

56. *The Access Right, Health Apps, & APIs*, U.S. DEP'T. OF HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access-right-health-apps-apis/index.html (last visited Mar. 29, 2023).

57. Ruth Reader, *'Shut It Off Immediately': The Health Industry Responds to Data Privacy Crackdown*, POLITICO (Apr. 17, 2023), https://www.politico.com/news/2023/04/17/health-industry-data-privacy-00092447.

58. 45 C.F.R § 160.103; *see also Privacy and Security and Workplace Wellness Programs*, U.S. DEP'T. OF HEALTH & HUM. SERVS., n. 2, https://www.hhs.gov/hipaa/for-professionals/privacy/workplace-wellness/index.html (last visited Aug. 19, 2023).

59. 45 C.F.R. § 160.103.

enforcing the privacy regulations that do exist in certain sectors has been the Federal Trade Commission (FTC),whose remit primarily concerns consumers and not workers.

This suggests a larger and more intractable problem. There is a structural obstacle to the development and enforcement of sound federal worker health data privacy laws in the United States: the lack of clear regulatory authority. The IAPP maintains an overview of the dozens of federal government agencies and offices that have some role in regulating privacy in the United States.[60] None is specifically tasked with developing or enforcing worker health data privacy laws. Several, however, may play a role in their creation. The scope of the public entities that might have some role in privacy regulation in the United States is breathtaking.

There is a Federal Privacy Council (FPC), established in 2016, but it does not make rules.[61] Its official purpose is to serve as "the principal interagency forum to improve the Government privacy practices of agencies and entities acting on their behalf."[62] The FPC is composed of the Senior Agency Officials for Privacy at more than a dozen federal agencies.[63] While the FPC is supposed to "inform government-wide priorities on privacy policy and monitor their implementation," among other roles, it does not appear to have any rulemaking authority itself.[64] The House of Representatives also has a subcommittee tasked with the oversight of consumer privacy bills known as the Subcommittee on Innovation, Data and Commerce (a rebranding from its previous name, the Consumer Protection and Commerce subcommittee).[65]

Within the executive branch, there are at least six entities that report to the Cabinet which could have some role in developing worker health data regulation. These include: (1) the Bureau of Cyberspace and Digital Policy, which is part of the State Department; (2) the Office of Privacy and Civil Liberties, within the Department of Justice; and (3) the Office of Civil Liberties, Privacy & Transparency, part of the Office of the Director of National Intelligence.[66]

---

60. Cobun Zweifel-Keegan, *US Institutions Privacy Stakeholder Map*, https://iapp.org/resources/article/us-institutions-privacy-stakeholder-map/ (last visited Apr. 27, 2023). This map, while nearly comprehensive, omits an agency that has relevance in the context of worker health data privacy: the U.S. Occupational Safety and Health Administration (OSHA), which issues recommendations about how employers should collect and store health data.

61. Exec. Order No. 13,719, 81 Fed Reg. 7961 (Feb. 12, 2016).

62. *Id.* § 4(a).

63. *Id.* § 4(b).

64. *Vision and Purpose*, FED. PRIVACY COUNCIL, https://www.fpc.gov/vision-and-purpose/ (last visited Aug. 11, 2023).

65. Cobun Zweifel-Keegan, *A View from DC: From Consumer Protection to Innovation and Data*, IAPP (Jan. 27, 2023), https://iapp.org/news/a/a-view-from-dc-from-consumer-protection-to-innovation-and-data/.

66. Within the Department of Commerce, there are three additional offices that have some role in privacy regulation and policy development: (4) the NTIA, which is tasked with working with stakeholders to create recommendations about technology policy, including privacy, for the executive branch; (5) the ITA, which may be relevant to developing privacy policies for multinational employers, and (6) the NIST, which also works with stakeholders to develop privacy guidance, tools and standards.

There are more privacy-related entities outside of the executive branch. Some of these are independent agencies that operate autonomously from the rest of the executive branch. Among the independent federal agencies, the most visible in the privacy sphere may be the FTC. Congress has conferred rulemaking power to the FTC under certain sectoral privacy laws, including the Children's Online Privacy Protection Rule and the Fair Credit Reporting Act. Because consumer privacy differs from worker privacy in critical ways, the FTC may not be the most appropriate rulemaking entity for worker health data privacy regulation.

Other independent agencies with potentially relevant remits include the Securities & Exchange Commission (SEC); the Federal Communications Commission (FCC); the Consumer Financial Protection Bureau (CFPB), which is part of the Federal Reserve, and the Privacy & Civil Liberties Oversight Board. Although the SEC focuses on the regulation of financial markets, which is only one sector of employers, it also brings enforcement actions relating to data protection and cybersecurity that may affect a broader scope of workers.

The FCC focuses on telecommunications including both traditional broadcast and social media communications. Among other rules, it enforces the privacy and data protection aspects of the Communications Act. Employer monitoring of worker communications relating to health, including searches for health-related keywords such as "depression" or "cancer," arguably could be overseen by the FCC.

The CFPB, as its name suggests, focuses on consumer protection.[67] In the context of health-related apps and websites, however, workers are a subset of the consumers whose privacy may be at stake. Indeed, the CFPB indicated its intentions to investigate data brokers, presumably including those who trade in health data, in March 2023 when it issued a Request for Information from the public about data brokers.[68] In that request, the CFPB noted that data brokers collect "sensitive and intimate personal information such as genetic and health information...nd geolocation data."[69] The potential harms of data broker operations, it observed, include "significant privacy and security risks..."[70]

Trying to create a Venn diagram of the federal entities that might have responsibility for rulemaking about worker health data privacy would be a frustrating exercise. None of these federal government entities is specifically

67. As of this writing, the legitimacy of the CFPB is in question because the Supreme Court has agreed to review a Fifth Circuit decision that the agency's funding mechanism is unconstitutional (Comm. Fin. Servs. Assn. of America v. CFPB, 51 F.4th 616 (5th Cir. 2022), *cert. granted*, 143 S. Ct. 978 (2023). If affirmed, this would likely mean that the CFPB would have to be disbanded at least temporarily because it would have no constitutional funding source.

68. Request for Information Regarding Data Brokers and Other Business Practices Involving the Collection and Sale of Consumer Information, 88 Fed. Reg. 16951 (Mar. 21, 2023).

69. *Id.*

70. *Id.*

responsible for regulating worker health data or developing relevant policies, but the scope of each one's authority arguably extends to this sphere.

iii. U.S. Federal Laws Cannot Compare with the GDPRs

The failure of federal data privacy laws is particularly striking in comparison with the laws of the European Union and the United Kingdom. The European Parliament's General Data Protection Regulation[71] (GDPR) provides workers in the EU with more privacy protection than United States federal law. Collecting health data through fitness trackers and other devices provided by employers without a narrowly defined, permissible justification is likely to violate the GDPR.[72] Health-related data, along with genetic data and biometric data used to identify a unique subject, is considered "sensitive" and its processing is subject to a higher level of protection than other data.[73] It may only be processed under relatively limited conditions in which the public interest outweighs the subject's right to privacy.[74]

In the UK, the Information Commissioner's Office (ICO) is also strengthening protections for workers by updating its employment practice code.[75] Among other initiatives, it recently sought public input on its Monitoring at Work Guidance, which aims to provide guidance on the best practices relating to worker monitoring in accordance with the UK's data protection laws. The provisions of this draft guidance include a recognition that while monitoring is part of the employment relationship, employers should justify their monitoring based on at least one of several discrete lawful bases.[76] Employers monitoring "special category data," which includes personal data revealing or concerning information about health, disability, genetic data, or biometric data, have to meet a higher standard to justify such monitoring.[77] In addition, UK employers have to carry out a data protection impact assessment (DPIA) to ensure that the value of the purpose for monitoring outweighs the risk of inadvertently capturing this sensitive information.[78]

---

71. *See* General Data Protection Regulation, 2016 O.J. (L 119) 1 (EU).

72. Philippa Collins & Stefania Marassi, *Is That Lawful? Data Privacy and Fitness Trackers in the Workplace*, 37, 1-4 INTL. J. COMP. LABOUR L. INDUS. RELATIONS 65 (2021).

73. *What Personal Data Is Considered Sensitive?*, EUR. COMM'N, https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/what-personal-data-considered-sensitive_en (last accessed Apr. 15, 2023).

74. *See, e.g.*, GDPR Recital 51 of Apr., 26, 2016, O.J. (L 119) 1 (EU); *see e.g.*, GDPR Recital 53 of Apr., 26, 2016, O.J. (L 119) 1 (EU); *see, e.g.*, General Data Protection Regulation, *supra* note 71.

75. Dan Cooper et al., *UK Information Commissioner's Office released a New Draft Employment Guidance for Monitoring at Work*, COVINGTON (Nov. 28, 2022), https://www.insideprivacy.com/united-kingdom-2/uk-information-commissioners-office-released-a-new-draft-employment-guidance-for-monitoring-at-work/.

76. *Employment Practices: Monitoring at Work Draft Guidance*, U.K. INFO. COMM'N'S OFFICE (Oct. 12, 2022) at 9.

77. *Id.* at 12-13.

78. *Id.* at 13.

The GDPR has been successful in many regards, but it is neither ideal nor an entirely public initiative, having been developed in large part through consultations with industry stakeholders. Although it may be tempting to model federal worker health data privacy laws on the GDPR and the UK GDPR, it is important to consider the lessons learned in Europe and the UK since those laws took effect. The GDPR is being subject to reform, both in Europe and in the UK. It is also worth noting that as technology expands in its capacity to capture and use data in the employment sphere, the regulation of monitoring has to evolve alongside it.

Whether rooting worker health data privacy protection in a model based on the GDPR is likely to be effective in the U.S. is also questionable in part because privacy is considered to be a fundamental right in the E.U., but not in the U.S. There is no federal constitutional recognition of privacy as a fundamental right in any way that is comparable to the acceptance of privacy rights in Europe. To the contrary, the First Amendment rights of freedom of speech may handicap the ability of U.S. lawmakers to require app and website developers to build privacy protections into their products. There are also different assumptions about the efficacy of notice and choice in the employment context between the U.S. and the E.U. Because many U.S. employers have international workforces, however, the impact of the GDPR, and the potential roles of the ILO and OECD in developing future paradigms for protecting worker privacy, should be examined.

II. NEW STATE DATA PRIVACY LAWS OFFER MODELS AND FORESHADOW CHALLENGES

While there is no uniform federal statute protecting data privacy, state level legislation is moving fast. Over the past few years, states have begun to fill some of the gaps created by the federal patchwork of health data privacy laws. Although these laws differ from each other in some ways, they all share some features. First, they all have an exemption for data that HIPAA already protects. They all also define the sensitive data that is subject to their state law protections, including certain kinds of health data.

Six states have substantial general data privacy laws as of April 2023: California, Colorado, Connecticut, Iowa, Utah and Virginia.[79] The California Privacy Rights Act and the Virginia Consumer Data Protection Act took effect on January 1, 2023, while comparable laws in Colorado and Connecticut take effect on July 1, 2023. Utah's Consumer Privacy Act goes into effect on the last day of 2023. Eighteen other states have active data protection bills with varying scopes.

These state law's definitions of sensitive data encompass at least two kinds of health data: (1) information revealing physical or mental health conditions

79. Anokhy Desai, *US State Privacy Legislation Tracker*, IAAP https://iapp.org/resources/article/us-state-privacy-legislation-tracker/ (last visited Aug. 20, 2023).

and (2) genetic information and/or biometric data.[80] The state laws differ, however, with regard to protecting information such as geolocation and information about individuals' sex lives or sexual orientation.

Perhaps the most important feature of a privacy law is the ability to enforce it. Of the five state laws currently in effect, only California's laws have private rights of action.[81] Even in those laws, the private enforcement rights are limited to certain types of statutory violations.[82] There is also a proposed private right of action in the current data privacy bills in Maryland, Massachusetts, Minnesota, New Jersey, New York, Oregon, Rhode Island and Washington.[83] For all other violations, and in every other state, enforcement of the state privacy laws depends on the discretion and resources of the state attorneys general.

A. *California*

As one of the largest global economies, California can create an outsized impact through its laws. California passed the California Consumer Privacy Act (CCPA) in 2019, just a year after the GDPR went into effect. The CCPA has been creating data privacy obligations for companies with a California presence, which is effectively all companies with an internet presence, since then.

In the context of data privacy regulation in employment, however, the CCPA has had little impact. The CCPA offered an exemption for employers regarding data collected in the context of employment, but that exemption has now expired, and a new set of obligations has come into effect through the CPRA. Another state law, the California Age-Appropriate Design Code Act, may also play a significant role in discussions of health privacy regulation.

i. California Privacy Rights Act

The CPRA, which took effect on January 1, 2023[84], is the most comprehensive regulatory framework for worker data privacy rights in the United States. It largely draws on the European Union's General Data Protection Regulation (GDPR). Unlike the CCPA, the CPRA explicitly addresses the employment context and provides rights and obligations regarding health and other data privacy in the workplace. The CCPA had an explicit exemption for job applicants and workers with regard to personal information "collected and used solely within the context of the natural

80. Amy Olivero, *Privacy and Digital Health Data: The Femtech Challenge*, IAPP (Oct. 25, 2022), https://iapp.org/news/a/privacy-and-digital-health-data-the-femtech-challenge/.

81. As of this writing, Iowa also has a state privacy law that has been passed but not yet signed, making it the closest of any other state bill to becoming law, but that bill also lacks a private right of action. Desai, *supra* n. 79

82. *Id.*

83. *Id.*

84. Cal. Civ. Code § 1798.100.

person's role or former role as a job applicant to, an employee of...or an independent contractor of that business."[85]

The CPRA's scope in the employment context is limited. Critically, the CPRA, like the CCPA, restricts large businesses that focus on collecting consumer data. The definition of "business" under both laws is a for-profit entity doing business in California that collects or controls the processing of consumer information and meets one or more of the following conditions: (1) had annual gross revenues of $25,000,000 in the preceding calendar year; (2) buys, sells, or shares the personal information of at least 100,000 consumers or households, or (3) derives at least 50 percent of its annual revenue from selling or sharing personal information.[86]

Under the CPRA, Californians who work for covered employers have several new rights regarding their personal data, including health data. They have the right to know what kinds of data their employers collect, share, sell, and disclose about them, as well as the right to know what kind of data the employer has collected about them individually.[87]

The disclosure requirements are somewhat detailed, but possibly easy to evade. CPRA also requires that employers disclose every category of "sensitive personal information" collected from its workers in a formal notice.[88] "Sensitive personal information" includes personal information that reveals a worker's geolocation, among other things. It also includes information "collected and analyzed" about a worker's health, sex life, or sexual orientation.[89]

What does "collected and analyzed" mean in this context? Does the employer need to do both the collection and the analysis for this notice requirement to kick in? In many workplaces, the employer offers femtech apps as a benefit to some workers. If the femtech app collects and analyzes data from the workers and then sells or even offers it to the employer, does that count?

There are also ways in which even health-related data collection might not be apparent at first and might not trigger the notice requirement. Imagine, for example, that an employer collects information both about where its workers go (geolocation data) and whether its workers are looking for search terms like "abortion" or "pregnancy termination." If the geolocation data collection is not limited to, say, the building where the employee works, it may reveal that the worker has visited a reproductive health clinic. Triangulating this data may suggest that a particular member of the workforce is likely to have had an abortion. However, it may alternatively suggest that the worker accompanied someone else to a clinic. In this scenario, the employer need only disclose that it collects geolocation data. The worker might never know

85. Cal. Civ. Code § 1798.145(m)(1)(A).
86. Cal. Civ. Code § 1798.140(d)(1).
87. Cal. Civ. Code § 1798.110(a)(1)-(5).
88. Cal. Civ. Code § 1798.140(ae).
89. Cal. Civ. Code § 1798.140(ae)(2).

that the employer can also make inferences about her health from combining geolocation data and search terms. It is possible that a court might interpret the triangulation itself as collection and/or analysis, but that is not clear.

Under the CPRA, workers also have the right to correct, rectify, and delete certain types of personal information that the employer has collected about them.[90] But lawyers advising companies about the CPRA note that there are simple ways to avoid notifying workers that certain kinds of data are being collected, the CPRA guidelines notwithstanding. In one client advisory, a law firm observed that a company would not necessarily have to disclose that it was collecting specific information about a worker's "health, sexual orientation or religious beliefs." Having to alert workers that a company collected such information through the notices that the CPRA now requires "could, at a minimum, lead to questions being asked."[91] Instead, the firm suggests, employers could be vaguer. They could "blend these categories of information within a list of myriad categories of personal information collected by the company," which would "enable employers to avoid this employee-relations issue, and only have to list those categories of information that are generally deemed to be "sensitive," such as Social Security and driver's license numbers."[92] In other words, at least one law firm is already counseling employers about how to avoid letting their workers know that the company keeps track of their health data, sexual orientation, or religious beliefs.

ii. California Age-Appropriate Design Code

Although it does not address health privacy specifically, another law relevant to this discussion is the California Age-Appropriate Design Code Act (CAADC). The CAADC was modeled on the UK's Age Appropriate Design Code (UK AADC), which protects people under 18 from certain harmful practices by apps and websites. According to the 5Rights Foundation, the benefits of the UK AADC have included TikTok and Instagram disabling direct messages between children and adults they do not follow, the Google Play Store preventing under 18s from viewing and downloading apps rated as adult-only, and YouTube turning off autoplay for under 18s and turning on break and bedtime reminders by default.[93] California is not the only state to have introduced a bill modeled on the UK AADC, but it is the first state in which the bill has been passed. Lawmakers in Maryland, New Jersey, New

90. Cal. Civ. Code § 1798.106(a).

91. Kwabena A. Appentang, *California Privacy Rights Act for Employers: The New "Notice at Collection" California Employers Must Distribute to the Workforce*, LITTLER, https://www.littler.com/publication-press/publication/california-privacy-rights-act-employers-new-notice-collection (last visited Mar. 31, 2023).

92. *Id.*

93. *Protections for Children Online Introduced in California*, 5RIGHTS FDN. (Feb. 16, 2022), https://5rightsfoundation.com/in-action/protections-for-children-online-introduced-in-california.html. These benefits presuppose that the social media sites know the actual age of the user, which could be easy enough for a teen user to misrepresent.

Mexico, New York, and Oregon have also introduced bills modeled on the U.K. law.[94]

The CAADC regulates "[b]usinesses that develop and provide online services, products, or features that children are likely to access."[95] Under the CAADC, businesses preparing to launch new online services, products, or features are required to prepare a Data Protection Impact Assessment detailing how the feature's design could expose minors to "potentially harmful" materials.[96] The CAADC also prohibits these online businesses from collecting, using, or distributing a child's personal information in any way inconsistent with "the best interests of children."[97]

How would a company know whether its site is one that minors are likely to access? The CAADC requires them either to figure it out or protect the public in general. Under the CAADC, covered businesses have to estimate their users' ages with "a reasonable level of certainty appropriate to the risks that arise from the data management practices of the business" or, alternatively, they have to "apply the privacy and data protections afforded to children to all consumers."[98]

The CAADC, like the UK AADC, requires privacy by design. This is the principle that data privacy should factor into systems and processes from the ground up rather than being tacked on as an afterthought.[99] It encompasses a set of seven design principles that provide, among other things, that sites, applications, and programs should take privacy into consideration throughout the design process.[100]

Privacy by design is commonly attributed to Ann Cavoukian, the former Information and Privacy Commissioner of Ontario, who proposed it in the 1990s. Privacy by design is considered a data privacy best practice by regulators around the world. The GDPR, for example, adopts the privacy by design principles in Article 25 and Recital 78.[101] The CAADC is the first privacy-by-design law in the United States and will take effect in 2024 if it survives the legal challenges to it.

---

94. Cristiano Lima, *Maryland is the Latest State to Weigh Online Safety Rules for Kids*, WASH. POST (Feb. 13, 2023), https://www.washingtonpost.com/politics/2023/02/13/maryland-is-latest-state-weigh-online-safety-rules-kids/.

95. Cal. Civ. Code § 1798.99.29(a).

96. *Id.* § 1798.99.31(a)(1)(B)(i)-(vii).

97. *Id.* § 1798.99.31(b).

98. *Id.* § 1798.99.31(a)(5).

99. *Privacy by Design*, PRIVACYSENSE.NET, https://www.privacysense.net/terms/privacy-by-design/ (May 12, 2022).

100. MARK SETTLE, PRIVACY BY DESIGN: FROM PRINCIPLES TO REQUIREMENTS 7 (2021), https://www.dropbox.com/s/6ebn20uxvko2v6p/Privacy%20by%20Design%20-%20From%20Principles%20to%20Requirements%20White%20Paper.pdf?dl=0.

101. EUROPEAN DATA PROTECTION SUPERVISOR, PRELIMINARY OPINION ON PRIVACY BY DESIGN 8 (2018) (EC), https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf.

Those legal challenges may be substantial. In December 2022, a tech industry group called NetChoice filed suit to block the AADC.[102] NetChoice's members include Amazon, AOL, Google, Meta, and TikTok. NetChoice alleges that the AADC violates the First Amendment, the Fourth Amendment, and the Due Process and Commerce Clauses.[103] motion for a preliminary injunction will be heard on July 27, 2023.[104]

At around the same time the CAADC bill was introduced, a bipartisan pair of U.S. senators introduced a different federal bill to increase the range of parental controls over online platforms for children under 16.[105] The Kids Online Safety Act (KOSA) would, if passed, establish a duty of care for online platforms toward minors under 16. It would also require these platforms to create new safeguards for such minors, including controls over "algorithmic recommendation systems that use a minor's personal data."[106] It would also prohibit any covered app or site to use dark patterns or manipulations "with the purpose or substantial effect of subverting or impairing user autonomy, decision-making, or choice[.]"[107]

iii. California Workplace Technology Accountability Act

In 2022, California Assembly Member Ash Kalra proposed another interesting piece of legislation: the California Workplace Technology Accountability Act.[108] This proposed act sought to regulate the use of monitoring controls in the workplace and to limit the kinds of worker data that could be used by automated decision tools. Some scholars praised this proposed legislation as a step in the right direction for the responsible control of workplace automation.[109] Although the bill died in committee,[110] it provides an interesting model for what additional legal restrictions on the algorithmic use of health data at work might look like.

---

102. Krista Chavez, *NetChoice Sues California to Protect Families & Free Speech Online*, NETCHOICE (Dec. 14, 2022), https://netchoice.org/netchoice-sues-california-to-protect-families-free-speech-online/.

103. Complaint for Declaratory and Injunctive Relief, NetChoice v. Bonta, N.D. Cal. 5:22-cv-08861-BLF (filed Dec. 14, 2022).

104. Order Re Defendant's Motion to Change Time; and Resetting Hearing From June 22, 2023 to July 27, 2023 at 1:30 P.M. NetChoice v. Bonta, N.D. Cal. 5:22-cv-08861-BLF (filed Mar. 10, 2022).

105. S. 3663, 117th Cong. (2022); Cat Zakrzewski, *Senators Unveil Children's Online Safety Bill After Months of Pressure on Silicon Valley*, WASH. POST (Feb. 16, 2022); https://www.washingtonpost.com/technology/2022/02/16/kids-online-safety-act-unveiled-blackburn-blumenthal/.

106. S. 3663, 117th Cong. (2021) § 4(a)(1)(D).

107. S. 3663, 117th Cong. (2021) § 4©(2).

108. Assemb. B. 1651, 2022 Leg., 2021-2022 Sess. (Cal. 2022).

109. Airlie Hilliard, Emre Kazin, Tom Kemp &Kelvin Bageirea, *Overview and Commentary of the California Workplace Technology Accountability Act*, 37 INTL. REV. OF L., COMPUTERS & TECH 93 (2023).

110. Assemb. B. 1651, 2022 Leg., 2021-2022 Sess. (Cal. 2022). as reported by Cal. Legis. Info, https://leginfo.legislature.ca.gov/faces/billStatusClient.xhtml?bill_id=202120220AB1651 (last visited Apr. 23, 2023).

B. *Other State Legislation*

Many other states now either have some form of statutory data protection or are introducing bills to provide limited data privacy protection. The impact of other state laws is comparatively limited because California dwarfs every other state in terms of the size of its economy. Whether the health data of workers is within the scope of these laws, as it is in the GDPR and in the CPRA, varies by state. What is interesting about this development is its geographic scope. The fact that there are so many states introducing these laws underscores the swell of interest in the United States in data privacy protection in general. They also demonstrate the shortcomings of state law with regard to health data privacy in the workplace.

i. Virginia

Virginia was the second state to adopt a comprehensive data privacy law after California. Its Consumer Data Protection Act (CDPA)[111] took effect on January 1, 2023. While it shares several features of the CCPA and CPRA, it uses more of the terminology found in the GDPR.[112] Like the CCPA, it applies only to businesses that control or process the personal data of consumers and derive at least 50% of their personal revenue from the sale of such data.[113] Unlike the California laws, however, it does not set a revenue threshold. Also, unlike the CCPA and CPRA, Virginia's law has no private right of action.

In the context of worker health data privacy, Virginia's law has limited effect because of its definition of "consumer." The CDPA defines a consumer as a "natural person who is a resident of the Commonwealth acting only in an individual or household context."[114] It specifically excludes from this definition people who are "acting in a commercial or employment context."[115] The CDPA thus excludes employees and other workers from the scope of its data privacy protection, at least insofar as it relates to data collected at or used by an employer.

Other exceptions to the CDPA specifically exclude health-related data. For example, its protections do not apply to certain health records, PHI under HIPAA, information created for the Health Care Quality Improvement Act of 1986, or "information originating from, and intermingled to be indistinguishable with [...] information that is maintained by a covered entity or business associate as defined by HIPAA[.]"[116] This exception appears to set

111. VA. CODE ANN. § 59.1-575 (2021).

112. *Legal Update, Virginia's New Data Privacy Law: Comparing to California and Preparing for Next Steps*, MAYER BROWN (Mar. 10, 2021), https://www.mayerbrown.com/-/media/files/perspectives-events/publications/2021/03/virginias-new-data-privacy-law.pdf.

113. VA. CODE ANN. § 59.1-576(A) (2021).

114. VA. CODE ANN. § 59.1-575 (2021).

115. *Id.*

116. *Id.* § 59.1-576(C)(1), (5), and (8).

aside health-related data that is close to what HIPAA protects, but is not necessarily protected by HIPAA itself.

ii. Colorado

When Colorado became the third state to pass a data privacy law, it did not break much new ground. The Colorado Privacy Act (CPA), like the CCPA in California and the CDPA in Virginia, applies to any business that controls or processes the personal data of at least 100,000 consumers each year.[117] Like the CDPA, the CPA does not set a minimum revenue that a company must have from the sale of data in order for the law to apply. But unlike either California or Virginia's laws, the CPA applies no matter how small a percentage of the company's annual revenue comes from selling data. The CPA does not provide for a private right of action, but it does allow either the Attorney General or a district attorney to enforce the law.[118]

More importantly for present purposes, the CPA also excludes workers from the scope of its protection. It protects only consumers, defining a consumer as "a Colorado resident acting only in an individual or household context."[119] It explicitly does not include individuals acting in "a commercial or employment context, as a job applicant, or as a beneficiary of someone acting in an employment context."[120] Employers, therefore, do not have to consider the CPA when collecting, processing, or using the health data of their own workers.

iii. Washington

In Washington, a law passed in April 2023 called the "My Health My Data Law" restricts the collection, sharing, and selling of consumer health data.[121] While the reference to "consumer health data" appears to focus on consumers rather than workers, that is a distinction without a difference in some contexts. If an employer provides a health-related app to workers in Washington, for example, those workers are in effect consumers for the purpose of this law. The restrictions the law establishes apply to the app developers, limiting the amount of information the apps can collect and then share with the employer or anyone else.

The new Washington law creates obligations for "regulated entities."[122] These include any entity doing business in Washington and which, either alone or collaboratively, "determines the purpose and means of collecting, processing, sharing, or selling of consumer health data."[123] That includes the

117. COLO. REV. STAT. § 6-1-1304 (2021).
118. COLO. REV. STAT. § 6-1- 1311(1)(a) (2021).
119. COLO. REV. STAT. § 6-1-1303(6)(a) (2021).
120. COLO. REV. STAT. § 6-1-1303(6)(b) (2021).
121. H.B. 1155, 68th Leg. (Wa. 2023).
122. *Id.*
123. *Id.*

makers of any health-related software that is available in Washington, but it is not so limited. That category also includes employers with Washington-based workers who are making decisions about how to collect the health data of their staff.

Regulated entities have to maintain a clear, public "consumer" health data privacy policy that spells out what is being collected and shared.[124] They may not collect any health data without consent unless it is necessary to provide a service the "consumer" has asked for.[125] The Washington law also gives subjects the right to confirm the scope of data collection, withdraw consent, and have data deleted within 30 days of a confirmed request.[126]

Consent is an important exception to the protections these laws provide. Under Washington law, for example, an entity can sell consumer health data if the consumer has authorized that sale. It is easy to imagine an app developer including a standard consent to sell data in the terms and conditions that the users must sign before getting access to the app. The lack of effective notice and choice is a persistent problem with regard to privacy, especially in the context of apps and other software.

III. A Three-Part Proposal to Better Protect Worker Health Data Privacy

Whether the best way to protect workers from the misuse of their health data is through regulation, through the efforts of private industry, or through a combination of means is a critical question. The best solution may combine public and private initiatives. The threats workers face from misuse of their health data come from multiple sources. I propose a three-part approach to mitigating this threat. A comprehensive approach to protecting the privacy of worker health data should include limiting the kinds of health data that can be collected from the apps and websites that an employer might access, as well as an employer-level restriction, on the collection, use, analysis, and sale of its workers' health data that could be gathered from other sources.

The three stages of this proposal are designed to enhance privacy from first collection to optional employer use. First, the U.S. should adopt a privacy-by-design requirement for all apps and websites, modeled in part on the Age-Appropriate Design Codes. Second, federal law should be developed to require all U.S. employers to restrict the worker health data they collect and use via federal legislation that resembles but improves on the CPRA. Third, companies should be incentivized to provide greater privacy benefits than the law requires, while seeking ways to remediate the widening socioeconomic gaps in privacy that such perks may help to create.

This comprehensive approach is unfortunately complex. This complexity, however, is appropriate given how difficult health data is to protect at work and the potential consequences of its misuse. We can think of it as a

124. *Id.* § 4 (1)(a)-(c).
125. *Id.* § 5 (1).
126. *Id.* § 6 (1)-(3).

staged campaign. Outside the workplace, there should be limits on the kinds of health data that apps and websites can collect, use, track, share, and sell. Within the workplace, there should be a parallel line of defense that limits what employers can do with the worker health data that comes into their hands. In addition, employers should be encouraged to provide additional privacy protections as a benefit in order to increase worker satisfaction, improve retention, and promote sustainable labor practices.

A. *Privacy By Design Requirements*

If there were limits on the kinds of health-related data that apps and websites could collect initially, there would be less potentially damaging health-related data that an employer might misuse. A first line of defense, therefore, might be to adopt the kinds of privacy by design restrictions that the U.K. codified in the UK AADC. While some privacy statutes including the CCPA and Virginia's CDPA contain a prohibition limiting the collection of data to that which is relevant and reasonably necessary, a more stringent set of privacy by design standards would provide greater protection at the data intake level. There are excellent models for importing privacy by design laws into the United States. California has already shown that such laws can be passed at the state level through the CAADC, and at least five other states are considering similar laws. This suggests that there is a viable model for a federal privacy by design law to improve the privacy protections of worker health data.

I propose the adoption of privacy by design legal requirements that protect not only children, but all users, from the collection or retention of health-related data without narrower constraints on the use and transfer of that data than there are for other kinds of data. Using the privacy by design principles, apps, websites, and other programs should be proactive in protecting data rather than remedial. They could be designed with the privacy interests of the user as a priority instead of as an afterthought.

Computer science scholars have been developing design tools to implement privacy by design in health data apps and websites for nearly a decade. In 2015, Kim Wuyts designed a methodology for implementing privacy by design in software development called LINDDUN, so named for the threats it addresses (Linkability, Identifiability, Nonrepudiation, Detectability, Disclosure of information, Unawareness, Non-compliance).[127] Recently, a team of scholars presented the PARROT tool (PrivAcy by design Tool for InteRnet Of Things).[128] This framework, developed in consultation with a privacy lawyer, is designed to "offer an intuitive and user-friendly interface to assist software developers in deciding how to include privacy into

127. Kim Wuyts & Wouter Joosen, LINDDUN Privacy Threat Modeling: a Tutorial, Tech. Report (CW Reports), Vol. CW685, Dept. Comp. Sci., Ku Leuven (2015).

128. Nada Alhirabi et al., *Demo Abstract: PARROT: Privacy by Design Tool for Internet of Things*, 2022 IEEE/ACM 7TH INT'L. CONF. ON INTERNET-OF-THINGS DESIGN & IMPLEMENTATION 107, 108 (2022).

their system design."[129] The advent of privacy by design tools like PARROT should make privacy by design easier to achieve for all software developers.

Given the state of regulatory uncertainty around health data collection, app and website developers might welcome a clear privacy by design requirement – especially to the extent that it might help absolve them of future liability for data misuse. In the spring of 2023, federal agencies began to express greater concern about how health care companies market their services. The Federal Trade Commission and the Office for Civil Rights within the HHS both launched investigations into potential privacy violations by telehealth companies.[130] In March 2023, the FTC announced that it fined online therapy provider BetterHealth $7.8 million for sharing customer data illicitly.[131] Health care companies, worried about being subject to these investigations, began to slash their spending on targeted Google and Facebook ads. In the first three months of 2023, that spend was a quarter of what it had been in the same period in 2022, according to one ad industry monitor.[132] And an increasing number of other companies have filed data breach reports with the HHS acknowledging the collection of patient data, presumably hoping to preempt investigations and fines.[133]

If the U.S. were to adopt a privacy by design requirement for telehealth companies and any other company that is likely to be used to generate health-related data, providers would benefit from greater clarity about what data they can collect and use initially. While they would likely lose the revenue they may have been collecting from the sale and sharing of this data, increasing federal scrutiny and the rise of state laws prohibiting such uses compel that result anyway. The outcome of the Netchoice litigation will determine whether this strategy is feasible, at least in the short term. If Netchoice succeeds in blocking the CAADC from taking effect, there would be considerable legal challenges to the likelihood of other states or the federal government enacting similar laws.

B. *Restrict Employer Access to Worker Health Data*

The second reform I propose is the adoption at the federal level of a data privacy law comparable to the CPRA or the GDPR. Worker health data privacy would likely be protected under the broader legal shield that such a federal law would presumably provide. These laws would mitigate the risk of health data misuse by prohibiting employers from using their workers' health-related data without a legitimate basis. It would also empower workers by giving them greater rights of access to the health-related data their employers are collecting about them and the rights to correct or delete that information.

---

129. *Id.*
130. Reader, *supra* note 57.
131. *Id.*
132. *Id.*
133. *Id.*

Scholars have been advocating for the adoption of a national privacy law for the U.S. modeled after the GDPR since the GDPR took effect, while recognizing the fundamental challenges to doing so.[134] Professors Kim Houser and Greg Voss have noted that the GDPR already has important consequences for U.S. companies, and that the costs of noncompliance can be significant.[135] Others have observed that adopting certain principles of the GDPR would foster economic justice, another compelling argument for this legal convergence.[136]

One reason that the U.S. might not follow California's lead in developing a law similar to the CPRA is that there is no comparable federal justification for such a law. In California, there is a constitutional right to privacy. Californians voted in 1972 to amend their state Constitution to include the right of privacy among the "inalienable" rights of its citizens.[137] This established a legally enforceable right to privacy for Californians that has no counterpart in the U.S. Constitution. In the U.S., privacy has been construed as a right indirectly, by inference from explicit provisions in the Bill of Rights.[138] But as Americans learned in *Dobbs*, what constitutes a "right" in the U.S. can vanish even after fifty years of security in a single Supreme Court decision if its underpinnings are not secure.

There is also the question of preemption. Whether a federal data privacy law similar to the CPRA would preempt potentially conflicting state laws depends in part on the wording of the law. In theory, a broad federal privacy bill could effectively roll back state laws that offer stronger protections if it is not carefully constructed to avert such preemption. The Electronic Frontier Foundation has suggested that if a previous federal privacy bill had been enacted, there would have been a danger of preempting state privacy laws in California and other states.[139] It would be critical that any federal data privacy law serve as a floor, rather than a ceiling, for stronger state statutes.

C. *Securing Worker Health Data Privacy Voluntarily Has Multiple Benefits*

The third suggestion is to incentivize private entities to offer more privacy than they are legally bound to do. There are sound reasons for employers to protect worker health data privacy voluntarily. Indeed, in many sectors, companies choose to protect other forms of data as a voluntary matter,

---

134. *See* Shaun Jamison, *Creating a National Data Privacy Law for the United States*, 10 CYBARIS INTELL. PROP. L. REV. 1, 5 (2019) (arguing that there is a need for a national privacy law in light of the shortcomings of existing relevant federal laws).

135. 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, 51 (2018).

136. Michele E. Gilman, *Five Privacy Principles (from the GDPR) the United States Should Adopt To Advance Economic Justice*, 52 ARIZ. ST. L.J. 368, 412 (2020).

137. Cal. Const. art. 1 § 1.

138. Griswold v. Connecticut, 381 U.S. 479, 483 (1965).

139. Hayley Tsukuyama, *Federal Preemption of State Privacy Law Hurts Everyone*, ELEC. FRONTIER FDN. (July 28, 2022), https://www.eff.org/deeplinks/2022/07/federal-preemption-state-privacy-law-hurts-everyone.

adhering to industry standard codes or best practices. There is no immediate barrier to the development and adoption of a code that businesses might opt into in order to protect worker health data privacy, and many benefits to doing so beyond any regulatory obligation.

Employers have good reasons to choose to protect worker health data privacy even when the law does not require them to. In many ways, the digital privacy environment appears to be converging toward allowing a greater individual control of data overall.[140] Some observers have noted that consumer mistrust and market forces, in addition to the regulatory trends described above, are shifting businesses toward an increased personalization of data control.[141] Employers would be wise to follow this trend and stay ahead of worker expectations.

i. Privacy As Perk

Offering workers greater privacy protection could increase job satisfaction and retention, help attract talent, and improve morale and productivity overall. A potential downside to offering enhanced privacy as a benefit, however, is that it is likely to exacerbate the existing socioeconomic differences in who gets surveilled.

As public awareness of the risks of data misuse grows, even as legal prohibitions lag outside of California, there are sound reasons why an employer might nonetheless choose to offer enhanced health data privacy to its workers voluntarily. In this context, it may be useful to think of paid parental leave, which private employers are not obligated to provide under federal law. Yet many entities do offer paid parental leave for workers above a certain executive level. Paid parental leave is a benefit that many employers feel they must offer in order to remain competitive and to help them attract and retain the best talent. Indeed, studies have shown that offering paid parental leave tends to increase employee engagement and increase overall satisfaction, commitment, and retention.[142]

Might employers do something similar to what they have done with parental leave and treat privacy as a benefit? There is every reason to believe that offering something that an increasing number of Americans value and to which they are not generally entitled, like health data privacy, would be mutually beneficial for employers and workers. Workers are more likely to want to work for a company that offers health data privacy than for one that

140. Hossein Rahnama and Alex "Sandy" Pentland, *The New Rules of Data Privacy*, HARV. B. REV. (Feb. 25, 2022), https://hbr.org/2022/02/the-new-rules-of-data-privacy.

141. *Id.*

142. Daniela Clark, *The Front Lines: Employer Provided Paid Parental Leave in the United States*, CORNELL HR REV. (2017) at 7 (observing that paid parental leave increases morale and retention); PATRICK HAMMER & RICKARD PALMGREN, HOW PARENTAL LEAVE POLICIES INFLUENCE EMPLOYEE ENGAGEMENT 60 (2019), available at https://www.diva-portal.org/smash/record.jsf?pid=diva2%3A1331586&dswid=1380 (demonstrating conclusions of independent empirical studies).

does not, all other things being equal. Employers are more likely to enjoy a higher quality applicant pool, improved morale, and increased retention, among other positive developments.

A potential downside of offering increased health data privacy as a perk is that it may widen the gap between those who are higher earners, and therefore less likely to be surveilled in the first place, and those who are historically more subject to surveillance and monitoring. If privacy is a perk rather than a right, it is more likely that it will be offered to people in higher earning positions whose retention value is greater to the employer.

There is a socioeconomic disparity to biometric monitoring. The people who are most likely to be subject to such monitoring are people in low-wage and hourly wage positions, in which the tasks are more easily measured.[143] Data-driven metrics are easier to use and deploy in these fields. The people who work in these fields are more likely to be women, people of color, and recent immigrants, people who historically have been subject to greater surveillance.[144] Their perspectives are often missing from debates among scholars, managers and policymakers about the impact of data-driven monitoring in the workforce.[145]

For these reasons, it is important that employers offer enhanced health data privacy protection to all workers, regardless of seniority, job title or status. Normalizing health data privacy is likely to benefit all workers, especially those who are statistically more likely to be monitored in other ways. Ensuring that all workers receive these protections is a form of ethical management.

ii. Privacy As Competitive Advantage

Why would a business provide more worker health data privacy protections than it has to have? There are at least two reasons. First, it creates a competitive advantage. Second, it is a form of corporate social responsibility.

Using the law as a source of strategic advantage in general is a sound management theory that thought leaders have been recommending for many years.[146] More recently, scholars have noted the potential that companies have for using the GDPR in particular to gain an edge over their competition even when those companies are not obligated to comply with it.[147]

---

143. Michael Chui et al., *Where Machines Could Replace Humans—and Where They Can't (Yet)*, MCKINSEY Q. (July 8, 2016), https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/where-machines-could-replace-humans-and-where-they-cant-yet.

144. Sidney Fussell, *How Surveillance Has Always Reinforced Racism*, WIRED (June 19, 2020), https://www.wired.com/story/how-surveillance-reinforced-racism/.

145. AIHA NGUYEN, THE CONSTANT BOSS: WORK UNDER DIGITAL SURVEILLANCE 5 (2021).

146. *See, e.g.*, Robert C. Bird, *Law as a Source of Competitive Advantage* (Feb. 20, 2007), https://ssrn.com/abstract=964329; Robert C. Bird and David Orozco, *Finding the Right Corporate Legal Strategy,* MIT SLOAN MGMT. REV. (Sept. 16, 2014), https://sloanreview.mit.edu/article/finding-the-right-corporate-legal-strategy/.

147. W. Gregory Voss & Kimberly A. Houser, *Personal Data and the GDPR: Providing a Competitive Advantage for U.S. Companies*, 56 AMER. BUS. L.J. 287 (2019) (observing that U.S. employers not bound by the GDPR might still use its principles as a source of competitive advantage); Timo Jakobi et al., *Data*

There are strong competitive arguments for businesses to create more substantial health data privacy programs than they must have. A coalition of lawyers and in-house privacy officers offered some of those in a 2021 report entitled "Privacy as a Competitive Differentiator: Building and Effective and Strategic Healthcare Privacy Program."[148] The authors developed what they called "a set of recommendations for operating a healthcare privacy function that supports privacy compliance while also helping drive innovation and growth." While the legal landscape has changed since that report issued, especially with regard to state privacy laws, the proposition that health care privacy programs can be a strategic asset remains compelling.

In fact, the CPRA allows for opt-ins. The CPRA recognizes that some businesses may choose to follow its guidelines for the protection of health data for workers and consumers even if they do not have to do so. Entities doing business in California may voluntarily certify to the California Privacy Protection Agency that they are in compliance with the CPRA even if the statutory definition of "business" would not include them. [149]

iii. Privacy as CSR

Data privacy may also be a form of corporate social responsibility. For many years, scholars have been recognizing the potential for data privacy to form part of a company's CSR program.[150] By providing a greater level of health data security for workers, businesses are likely to enjoy many of the benefits of CSR associated with more satisfied workers.[151]

Employers could adapt existing measures to improve their worker health data privacy practices beyond their legal requirements. One way for employers to ensure that they are using worker health data responsibly would be to develop an ethics checklist. Ethics checklists for data use and collection already exist for other applications, including digital health research in psychiatry.[152] These checklists could help employers balance the ethical, legal, and managerial implications of their worker health data collection practices against the legitimate benefits of using that data. Once adopted in principle,

---

Privacy: A Driver for Competitive Advantage, *in* THE MACHINE AGE OF CUSTOMER INSIGHT 147 (Martin Einhorn et al. eds., Emeral Publishing Limited 2021).

148. Jiayan Chen et al., *Privacy as a Competitive Differentiator: Building and Effective and Strategic Healthcare Privacy Program*, IAPP (Oct. 2021), https://iapp.org/resources/article/white-paper-privacy-as-a-competitive-differentiator/.

149. CAL. CIV. CODE § 1798.140(d)(4).

150. Irene Pollach, *Online Privacy as a Corporate Social Responsibility: An Empirical Study*, 20 BUS. ETHICS: EUR. REV. 88 (2011); Alexis M. Allen and John Peloza, Someone to Watch Over Me: The Integration of Privacy and Social Responsibility, 58 BUS. HORIZONS 635, 636 (2015).

151. Christopher W. Bauman & Linda J. Sitka, *Corporate Social Responsibility as a Source of Employee Satisfaction*, 32 RES. IN ORG. BEHAVIOR 63 (2012); Patricia Gazzola & Piero Mella, *Can CSR Influence Employees[sic] Satisfaction*, 7 ECONOMIA AZIENDALE 331 (2016).

152. Francis X. Shen et al., *An Ethics Checklist for Digital Health Research in Psychiatry: Viewpoint*, J. MED. INTERNET RES., Feb. 2022, at 1.

the employer could then ensure that its own worker health data use and any such data use it controls through outside vendors satisfies those requirements.

It also may be helpful for employers to develop internal policies in this area by referencing a model worker health data privacy policy. Such a policy could start from generally accepted principles of privacy protection that have been in use for fifty years. The Fair Information Practice Principles (FIPPs) are a set of nine core principles that are widely used to evaluate any program, system or process that affects individual privacy. They were first developed in a 1973 report from the Department of Health, Education and Welfare Advisory Committee called "Records, Computers, and the Rights of Citizens."[153] Perhaps in part because their use has not been limited to any kind of technology or data, they have served as a bedrock for privacy program development around the world.[154] In the GDPR, for example, the FIPPS are codified in Article 5.[155] The FIPPS include the principles of ensuring transparency, data minimization, access and amendment rights, clarity, and security, among others.[156] For example, the principles of data minimization and data destruction worker health data. These differences may affect the optimal structure of a model policy.

If employers were incentivized to act according to these FIPPS, many of the concerns about the potential misuse of worker health data would likely abate. At present, however, employers in the United States are not generally required to abide by the FIPPs. That is not to say that none of them do, however. Many employers choose to use privacy programs administered either in-house or by external providers whose tools build on the FIPPS, sometimes mapping onto them explicitly.[157]

---

153. *Records, Computers and the Rights of Citizens: Report of the HEW Advisory Committee on Automated Personal Data Systems* (July 1973), https://epic.org/documents/hew1973report/.

154. Cheryl Saniuk-Heinig, *50 Years and Still Kicking: An Examination of FIPPs in Modern Regulation*, IAPP (May 25, 2021), https://iapp.org/news/a/50-years-and-still-kicking-an-examination-of-fipps-in-modern-regulation/.

155. Regulation 2016/679, art. 5, 2016 O.J. (L 119) 1 (EU).

156. The nine FIPPS are: (1) Access and amendment, or the individual right to access or correct their data; (2) accountability, or the need to be accountable for compliance and provide training as needed; (3) authority, or only collecting data necessary to accomplish a legitimate specified purpose; (4) minimization, or collecting only the data that is relevant and required for the entity's purpose; (5) quality and integrity in data collection; (6) participation, or the inclusion of individuals, ideally with their consent, and establishing procedures to handle individual concerns; (7) purpose specification and use limitation, requiring the entity to collect and use data only for the purposes it has specified to the individuals; (8) security, or establishing safeguards for the data; and (9) transparency regarding their data policies and practices. *Fair Information Practive Principles*, FED. PRIV. COUNCIL, https://www.fpc.gov/resources/fipps/ (last visited August 11, 2023).

157. *See, e.g.*, *Manage Subject Rights Request at Scale With Microsoft Priva*, MICROSOFT (Mar. 16, 2022), https://www.microsoft.com/en-us/security/blog/2022/03/16/manage-subject-rights-requests-at-scale-with-microsoft-priva/.

CONCLUSION

The privacy of workers' health data is an urgent and intimate issue, requiring a complex strategy for protection. In light of the expansion of health data generated by our devices, our apps, our locations, and ourselves, as well as the myriad ways in which that health data might be used against us by our employers, it is important to step back and consider how we might curb the potential for damage that might arise from privacy invasions. This is especially true for women workers whose reproductive health data might be used against them in ways that were hard to imagine ten years ago. As we become more comfortable tracking our own health data and disclosing information relating to our health online, we must develop stronger protections against the misuse of that and other health data by employers in the future.

The fragile nature of privacy as a legal obligation in the U.S., together with the fragmented nature of privacy regulation in this country, underscores the need for an innovative approach. In this article, I have suggested a three-part strategy encompassing private sector initiative, federal legal reform of employment practices, and a privacy by design requirement for all websites and apps that are likely to collect health-related data. The voices of more practitioners, scholars, advocates, policymakers and scholars will be necessary to help challenge and refine this approach. The privacy of worker health data concerns us all, and the solutions we generate collectively will be improved by debate, practice and refinement.

* * *