THE COLUMBIA
SCIENCE & TECHNOLOGY
LAW REVIEW

VOLUME XXIV STLR.ORG SPRING 2023

NOTE

PANOPTIC EMPLOYMENT: REMOTE WORKER HEALTH DATA UNDER SURVEILLANCE

Benjamin Hewitt*

Remote workers are subjected to constant and intrusive surveillance by employers and health technology companies. Working from home became commonplace as a result of COVID-19, and increasingly employers use health and location tracking software, as well as webcams and facial recognition, to monitor their employees. This surveillance exacerbates risks of discrimination based on health data and other lifestyle factors that have no bearing on work performance, implicates the privacy rights of family members and roommates, and sharpens the power asymmetry between employers and employees. Particularly as States seek to criminalize women seeking abortions following the Supreme Court's overturning of Roe v. Wade*, the safeguarding of health data on fertility-tracking applications has never been more important.*

Given the novelty and rapidity of this transition, state and federal laws fall short of adequately protecting remote workers from incessant surveillance, particularly of their health data. Although several federal laws and agencies appear to address certain aspects of this threat, in practice laws such as HIPAA at the federal level and BIPA and CCPA in Illinois and California, respectively, do not sufficiently regulate the collection of health data from remote workers. In addition to these practical issues, U.S. privacy law generally places undue exclusive emphasis on the individual, relying on notice-and-consent provisions and anonymization. However, the case of remote worker surveillance highlights the deficiencies of this individualized focus. This Note details the prevalence and harm of remote worker surveillance, discusses how the current data privacy legal regime falls short, and offers proposals for strengthening privacy protections for remote workers and their health data.

* Juris Doctor 2023, Columbia Law School.

I. INTRODUCTION 350
II. BACKGROUND ON HEALTH DATA PRIVACY OF REMOTE WORKERS 354
A. Defining Health Data Privacy 354
B. Prevalence of Remote Worker Surveillance 355
C. Risks of Remote Workers' Surveillance 358
D. Remote Worker Surveillance Highlights Flawed Approach to Data Privacy 360
III. CURRENT LEGAL AND REGULATORY LANDSCAPE 363
A. Federal Law and Agencies 363
B. State Laws 369
IV. RECOMMENDATIONS 375
V. CONCLUSION 378

I. INTRODUCTION

When tens of millions of people worked from home to avoid exposure to COVID-19, they were instead exposed to persistent and probing surveillance by their employers. Early in the pandemic, roughly thirty-five percent of American employees worked remotely.[1] While that number has dropped considerably as vaccination rates have improved, tens of millions of workers continue to log-in to work from home.[2] Both on and off the clock, these remote workers may be subjected to not only constant monitoring of their location and emails, but also facial recognition scans and collection of intimate health data.[3] Such rigorous surveillance and data collection from employees in their homes presents critical and underexplored questions as to whether and how this data collection is regulated. This Note argues that the collection of health data of remote workers by employers violates the privacy interests of these workers and that this practice remains inadequately covered by federal or state law.

Surveillance of workers is hardly new, but it has taken a particularly nasty form in recent years. There is a long history of employers monitoring workers both on

[1] Elaine Godfrey, *Another Truth About Remote Work*, THE ATLANTIC (Sept. 20, 2021), https://www.theatlantic.com/politics/archive/2021/09/work-from-home-numbers/620107/.

[2] U.S. Bureau of Labor Statistics, *Labor Force Statistics from the Current Population Survey*, BLS (December 2021), https://www.bls.gov/cps/effects-of-the-coronavirus-covid-19-pandemic.htm#data.

[3] Bennett Cyphers & Karen Gullo, *Inside the Invasive, Secretive "Bossware" Tracking Workers*, ELECTRONIC FRONTIER FOUNDATION (June 30, 2020), https://www.eff.org/deeplinks/2020/06/inside-invasive-secretive-bossware-tracking-workers (describing both visible and invisible monitoring techniques, GPS tracking, and more); *see also* Frank Hersey, *Continuous Facial, Iris Recognition for remote Workers with Princeton Identity, EPAM Partnership*, BIOMETRIC UPDATE (Aug. 2, 2021), https://www.biometricupdate.com/202108/continuous-facial-iris-recognition-for-remote-workers-with-princeton-identity-epam-partnership.

and off the job. In the 1850s, Allan Pinkerton created a private detective agency, whose members became known as "Pinkertons," to keep a watchful eye on workers, enforce various workplace rules, and infiltrate and bust unions.[4] Henry Ford hired private investigators to surveil employees at home to make sure their personal lifestyles and problems did not interfere with their productivity at work.[5] Modern day wellness programs and health tech, which collect intimate data such as heart rate, amount of exercise, hours slept and more, are the modern versions of this long trend of worker surveillance. Employers increasingly collect vast troves of intimate health data from their employees.[6] As more employees work remotely—seeking flexibility, freedom, and balance—productivity- and wellness-tracking devices contribute to an erosion of the line between personal and professional life.[7]

The increase in remote work has corresponded to an increase in remote worker surveillance. In a 2021 survey of 2,000 employers and 2,000 employees, seventy-eight percent of employers reported using employee monitoring software to track employee performance and online activity.[8] In this survey, fifty-nine percent of employees reported feeling stressed or anxious about their employer surveilling their online activity.[9] These monitoring programs can log every keystroke an employee types, watch employees work through their webcams, require facial recognition in order to log back in after a bathroom break, and record their location at all times.[10] Wearable technologies issued by an employer facilitate consistent

[4] Ifeoma Ajunwa, Kate Crawford & Jason Schultz, *Limitless Worker Surveillance*, 105 CAL. L. REV. 735 (2017).

[5] The Week Staff, *The Rise of Workplace Spying*, THE WEEK (July 5, 2015), https://theweek.com/articles/564263/rise-workplace-spying.

[6] For example, companies like Castlight analyze insurance claims to find which female employees have recently stopped using birth control or have made fertility-related searches on its proprietary health app in order to form predictions for employers as to which employees are likely to become pregnant. *See* Ifeoma Ajunwa, Kate Crawford & Joel S. Ford, *Health and Big Data: An Ethical Framework for Health Information Collection by Corporate Wellness Programs*, 44 J. LAW MED. & ETHICS 474, 474–80 (2016). Psychology Compass works with employers to give each worker a mental health and cognition coach to improve mental performance and productivity, collecting data that it can then share with employers if "necessary to provide [individuals] with the services" they offer. *Privacy Policy*, PSYCHOLOGY COMPASS, https://psychologycompass.com/privacy-policy/ (last visited Dec. 22, 2022). A third example is Muse, which offers a wearable headband to measure workers' brain waves to improve resilience, focus and sleep, assigning each employee a "sleep efficiency score." MUSE, https://choosemuse.com. The Muse headband connects to a web application, which is "designed to allow a party [including an] employer participating in a wellness program (the 'Observer') to monitor the Muse sessions of one or more people." *Privacy Policy*, MUSE, https://choosemuse.com/legal/ (last visited Dec. 22, 2022).

[7] Elizabeth Brown, *The Fitbit Fault Line: Two Proposals to Protect Health and Fitness Data at Work*, 16 YALE J. HEALTH POL'Y L. & ETHICS 1, *5—6 (2016).

[8] *ExpressVPN Survey Reveals the Extent of Surveillance on the Remote Workforce*, EXPRESSVPN (May 20, 2021), https://www.expressvpn.com/blog/expressvpn-survey-surveillance-on-the-remote-workforce/#ethics.

[9] *Id.*

[10] Tiffany C. Li, *Privacy in Pandemic: Law, Technology, and Public Health in the COVID-19 Crisis*, 52 LOY. U. CHI. L.J. 767, 781 (2021); *see also* Ashleigh Webber, *PwC Facial Recognition Tool Criticized for Home Working Privacy Invasion*, PERSONNEL TODAY (June 16, 2020),

tracking of remote employees' heart rate, distance moved, sleep duration and quality.[11] This kind of intrusive surveillance can expose sensitive information and facilitate discriminatory employment decisions, as well as cause anxiety and low morale.[12] This surveillance may be mandated, pre-loaded onto employer-issued devices, or may be more discreet, such as rolled into a corporate wellness program.[13] Data from fertility tracking apps may pose a particular threat to remote workers in light of numerous state abortion bans enacted following the Supreme Court's decision in *Dobbs*.[14]

Surveillance of workers at home serves as a fascinating example of a hazard to workers across class divisions. To many, the prototypical example of intrusive employer surveillance may be Amazon warehouse workers or drivers, who undergo persistent surveillance by cameras and scanners in order to meet demanding shipping quotas.[15] Yet remote work is available to a wide variety of white collar and other service jobs.[16] Remote workers are more likely to be highly educated and more likely to be upper-income workers.[17] However, this is hardly an elite phenomenon. The emerging surveillance regime ensnaring remote workers signifies the next step toward a state of constant data collection in all aspects of life. Surveillance has become a near constant in our lives, whether on city streets, in

---

https://www.personneltoday.com/hr/pwc-facial-recognition-tool-criticised-for-home-working-privacy-invasion/; Drew Harwell, *Managers Turn to Surveillance Software, Always-On Webcams to Ensure Employees Are (Really) Working From Home*, WASH. POST (April 30, 2020), https://www.washingtonpost.com/technology/2020/04/30/work-from-home-surveillance/.

[11] Christopher Rowland, *With Fitness Trackers in the Workplace, Bosses Can Monitor Your Every Step – and Possibly More*, WASH. POST (Jan. 16, 2019), https://www.washingtonpost.com/business/economy/with-fitness-trackers-in-the-workplace-bosses-can-monitor-your-every-step--and-possibly-more/2019/02/15/75ee0848-2a45-11e9-b011-d8500644dc98_story.html.

[12] Zoë Corbyn, *'Bossware is Coming for Almost Every Worker': The Software You Might Not Realize Is Watching You*, THE GUARDIAN (Apr. 27, 2022), https://www.theguardian.com/technology/2022/apr/27/remote-work-software-home-surveillance-computer-monitoring-pandemic; *see also* Brown, *supra* note 7 at *48.

[13] Gordon Hull & Frank A. Pasquale, *Toward a Critical Theory of Corporate Wellness*, 13 BIOSOCIETIES 190 (2018).

[14] Rina Torchinsky, *How Period Tracking Apps and Data Privacy Fit into a Post-*Roe v. Wade *Climate*, NPR (June 24, 2022), https://www.npr.org/2022/05/10/1097482967/roe-v-wade-supreme-court-abortion-period-apps.

[15] Annabelle Williams, *5 Ways Amazon Monitors its Employees, from AI Cameras to Hiring a Spy Agency*, BUSINESS INSIDER (Apr. 5, 2021), https://www.businessinsider.com/how-amazon-monitors-employees-ai-cameras-union-surveillance-spy-agency-2021-4?op=1; *see also* Jay Greene, *Amazon's Employee Surveillances Fuels Unionization Efforts: 'It's Not Prison, It's Work'*, WASH. POST (Dec. 2, 2021), https://www.washingtonpost.com/technology/2021/12/02/amazon-workplace-monitoring-unions/.

[16] Susan Lund, Anu Madgavkar, James Manyika, & Svene Smit, *What's Next for Remote Work: An Analysis of 2,000 Tasks, 800 Jobs, and Nine Countries*, MCKINSEY GLOBAL INSTITUTE, (November 2020), https://www.mckinsey.com/featured-insights/future-of-work/whats-next-for-remote-work-an-analysis-of-2000-tasks-800-jobs-and-nine-countries#.

[17] Godfrey, *supra* note 1.

schools, or on social media.[18] Our personal data is constantly collected throughout the day, starting as soon as someone picks up their phone, or even earlier if they sleep with a smart watch.[19]

At the federal level, the lack of any comprehensive privacy legislation precludes the adequate protection of workers in this regard. The federal law most relevant to health data is the Health Insurance Portability and Accountability Act ("HIPAA"), which imposes protections against non-consensual access to health records, but the scope of which excludes most employee surveillance.[20] While several states are further ahead in regulating data collection, these too fall short of what is required to curb intrusive surveillance of remote workers by collecting health data.[21] These inadequacies are both practical and conceptual. The particular threat of data surveillance of remote workers falls between the cracks of privacy laws. But conceptually, privacy law in the United States tends to focus solely on the individual-level, where the true harms of data collection may be diffused as compared to the population-level effects.

Despite these privacy risks, the health data privacy rights of remote workers have been under-analyzed and inadequately addressed by federal or state law. Federal law consists of a patchwork of relatively narrow domains of information privacy.[22] States like Illinois and California have made great strides in protecting intimate information like biometric data and comprehensive consumer privacy laws, respectively, but neither of these laws directly address the privacy risks posed to remote workers.[23]

This Note will proceed as follows. Part II explores the nature of health data privacy and how the privacy intrusions caused by its collection pose novel and grave risks to the dignity of workers and their families. Part III describes the current

---

[18] Rob Kitchin, *Reframing, Reimagining and Remaking Smart Cities*, The Programmable City Working Paper 20, Aug. 16, 2016 ("Indeed, many smart city technologies capture personally identifiable information and household level data about citizens – their characteristics, their location and movements, and their activities – link these data together to produce new derived data, and use them to create profiles of people and places and to make decisions about them."); *see also* Marta Ziosi, Benjamin Hewitt, Prathm Juneja, Mariarosario Taddeo & Luciano Floridi, ***Smart Cities: Mapping Their Ethical Implications***, SSRN (Jan. 5, 2022), https://ssrn.com/abstract=4001761; Drew Harwell, "Cheating-detection companies made millions during the pandemic. Now students are fighting back," WASH. POST (Nov. 12, 2020), https://www.washingtonpost.com/technology/2020/11/12/test-monitoring-student-revolt/.

[19] CARISSA VÉLIZ, PRIVACY IS POWER 4 (2021).

[20] *See infra* Part III.A.1.

[21] Three States currently have comprehensive data privacy laws: California has the California Consumer Privacy Act (CCPA); Colorado has the Colorado Privacy Act (ColoPA); and Virginia has the Virginia Consumer Data Privacy Act (VCDPA). Though not as comprehensive, Illinois has the Biometric Information Privacy Act (BIPA). Thorin Klosowski, *The State of Consumer Privacy laws in the US (And Why It Matters)*, N.Y. TIMES (Sept. 6, 2021), https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/; *see also infra* Part III.B.

[22] Anupam Chander, Margot Kaminski & William McGeeveran, *Catalyzing Privacy Law*, 105 MINN L. REV. 1733, 1748 (2019).

[23] *See infra* Part III.B.

regulatory regime, summarizing approaches taken by leading federal agencies like the Federal Trade Commission ("FTC"), Equal Employment Opportunity Commission ("EEOC"), and Department of Health and Human Services ("HHS"), as well as state laws that could address these privacy risks. Ultimately, these laws suffer from both practical and conceptual defects that leave open unfortunate gaps in the protection of employee privacy, and caselaw regarding reasonable expectations of privacy may not help. Part IV offers recommendations for legislation that recognizes not only the privacy vulnerabilities of remote workers, but also the need to look beyond the individual as the most relevant subject of data privacy law.

II. BACKGROUND ON HEALTH DATA PRIVACY OF REMOTE WORKERS

This section delves deeper into the practices of collecting health data on remote workers and justifies its importance as a subject of regulation. Health data collection of workers poses critical privacy risks that can cause anxiety and low morale, as well as discrimination and privacy risks to family.[24] These risks are particularly salient in the case of remote workers, implicating both the modes of data collection and the consequences for the divide between one's home and workplace.[25] This part will proceed first by defining health data privacy, then by detailing the prevalence and harms of the collection ***en masse*** of health data from remote workers, and then arguing that this kind of privacy invasion highlights a broader conceptual inadequacy of U.S. privacy law generally.

A. Defining Health Data Privacy

As a threshold matter, it is worth examining what is meant by health data privacy. Data privacy may refer to different kinds of phenomena. A significant portion of the literature, headlines, and legislation surrounding data privacy concern breaches.[26] Data breaches may be caused by callousness or carelessness; by cyberattacks or poor security practices.[27] Yet the focus of such incidents is usually

---

[24] Jessica L. Roberts, *Protecting Privacy To Prevent Discrimination*, 56 WM. & MARY L. REV. 2097, 2105 (2015); Reid Blackman, *How to Monitor Your Employees – While Respecting Their Privacy*, HARV. BUS. R. (May 28, 2020), https://hbr.org/2020/05/how-to-monitor-your-employees-while-respecting-their-privacy.

[25] Li, *supra* note 10, at 784. ("Context collapse occurs when individuals face a collision or collapse between boundaries of two or more previously segmented social spaces, for which they previously presented or performed their own identities in different manners, often due to the differing norms and natures of the social spaces. The context collapse of work and home, writ large across the world, will cause a fundamental shift in our understanding of public and private spaces . . .").

[26] *See* Daniel J. Solove & Woodrow Hartzog, BREACHED! WHY DATA SECURITY LAW FAILS AND HOW TO IMPROVE IT 1-14 (Oxford University Press 2022).

[27] The World Economic Forum found that 95% of cybersecurity issues can be traced to human error. World Economic Forum, THE GLOBAL RISKS REPORT 2022 17th Edition 52 (2022). This large role of operational security failures in cybersecurity incidents has given rise to an acronym widely used among tech support personnel, "PEBCAK," which stands for "problem exists between chair and keyboard," as well as an "IBM error" which stands for "idiot behind machine"

on the companies themselves, rather than the individuals affected.[28] Even less discussed is why the company or data controller had the data in the first place. It is therefore more illuminating to frame health data surveillance as implicating data-governance law, which Salomé Viljoen aptly defines as "the legal regime that governs how data about people is collected, processed, and used."[29] This still-young legal regime is vitally important as companies continue to collect data about every facet of individuals' lives in an effort to make profitable predictions, in a system that Shoshana Zuboff calls "surveillance capitalism."[30]

Health data is particularly sensitive. It includes data about one's medications, medical treatment, heart rate, exercise, sleep, mental and emotional states, and more.[31] This data was valuable enough that Congress passed HIPAA, one of the few privacy laws in the U.S. Code, to try to protect it.[32] Although as discussed in the following section, this law does not adequately address the health data collection of workers by employers.

B. Prevalence of Remote Worker Surveillance

Testifying before the House Subcommittee on Civil Rights and Human Services at a hearing on the Future of Work, Professor Ifeoma Ajunwa described the severe surveillance that remote workers must undergo.[33] In particular, she notes that measures such as video surveillance, GPS systems, e-mail and keystroke tracking, and even occasionally "microchips embedded under the skin" have "become a ubiquitous feature" in the United States, without any federal law protecting workers.[34]

The market for employee surveillance technology has skyrocketed in recent years.[35] Employee surveillance technology, also called "bossware," includes devices and software that range from monitoring emails and keystrokes to constant,

---

error. Amanda Holland, ***What is PEBKAC?***, INFOBLOOM (Jan. 30, 2022), https://www.infobloom.com/what-is-pebkac.htm.

[28] ***See*** Solove & Hartzog, ***supra*** note 26.

[29] Salomé Viljoen, ***A Relational Theory of Data*** Governance, 131 YALE L. J. 573, 577 (2020).

[30] SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER (2019) ("[Surveillance Capitalists] accumulate vast domains of new knowledge ***from us***, but not ***for us***. They predict our futures for the sake of others' gain, not ours.").

[31] Jianyan Fang, ***Health Data at Your Fingertips: Federal Regulatory Proposals for Consumer-Generated Mobile Health Data***, 4 GEO. L. TECH. REV. 125, 137 (2019) (defining "health data" as data that is "intrinsically of medical significance" or to the extent that is intended to be or in fact is used to conduct health-related analysis or make health-related predictions or conclusions).

[32] Health Insurance Portability and Accountability Act of 1996, Pub. L. 104–191, 110 Stat 1936 (1996) (codified as amended at scattered sections of 29 and 42 U.S.C.).

[33] Ifeoma Ajunwa, ***Protecting Workers' Civil Rights in the Digital Age***, 21 N.C. J.L. & TECH. 1 (2020).

[34] ***Id.***

[35] Ajunwa, Crawford & Schultz, ***supra*** note 4 at 135 (Productivity trackers and other workplace management apps represent an $11 billion industry.).

live video feeds of the employee's screen or webcam.[36] Employers can also collect biometric data through facial recognition, scanning workers' faces throughout the day to determine whether they are happy and satisfied on the job.[37]

The pervasiveness of surveillance devices is driven by individuals as well as companies and governments, contributing to a normalization of surveillance that facilitates the surveillance of remote workers' health data. People buy devices for themselves that capture much of this data, in order to learn more about themselves or engage in competitions with friends over who can walk the most.[38] This recreational use of devices that track health and location data has been coined "luxury surveillance," which contributes to a normalization of tracking technology more broadly.[39] The normalization of data tracking has overshadowed critical reflection about the implications of sharing sensitive data with under-regulated third parties.[40] The exponential increase in quantification and wearable technology has drawn comparisons to Foucault's concepts of the panopticon and biopower.[41] Biopower refers to the disciplining, optimization and extortion of human bodies for population control.[42] This concept is particularly apt in the case of employee surveillance, where one of the express purposes is to increase worker productivity.[43]

Wellness programs have also become a common feature of employer-sponsored healthcare plans. In 2020, 54.4% of people in the United States were covered by employment-based health insurance.[44] The Affordable Care Act has several

---

[36] Cyphers & Gullo, *supra* note 3.

[37] Corbyn, *supra* note 12; Danielle Abril & Drew Harwell, *Keystroke Tracking, Screenshots, and Facial Recognition: The Boss May Be Watching Long After the Pandemic Ends*, WASH. POST (Sept. 24, 2021), https://www.washingtonpost.com/technology/2021/09/24/remote-work-from-home-surveillance/; Martin Anderson, *Recognizing Employee Stress Through Facial Analysis at Work*, UNITE.AI (Nov. 24, 2021), https://www.unite.ai/recognizing-employee-stress-through-facial-analysis-at-work/.

[38] STEFFEN MAU, THE METRIC SOCIETY: ON THE QUANTIFICATION OF THE SOCIAL 12 (2019) (describing the emergence of a new "quantitative mentality," whereby numbers are accorded an "almost auratic pre-eminence when it comes to identifying social phenomena" and where "everything can, should or must be measured.").

[39] Chris Gilliard & David Golumbia, *Luxury Surveillance*, REAL LIFE MAG (July 6, 2021), https://reallifemag.com/luxury-surveillance/ (last visited Mar. 13, 2022).

[40] Chris Gilliard, *The Rise of 'Luxury Surveillance,'* THE ATLANTIC (Oct. 18, 2022), https://www.theatlantic.com/technology/archive/2022/10/amazon-tracking-devices-surveillance-state/671772/.

[41] Jean-François De Moya & Jessie Pullud, *From Panopticon to Heautopticon: A New Form of Surveillance Introduced by Quantified-Self Practices*, 30:6 INFORMATION SYS. J. 940, 946 (2020).

[42] MICHEL FOUCAULT, THE HISTORY OF SEXUALITY; VOLUME I: AN INTRODUCTION 139 (1978).

[43] Ifeoma Ajunwa, *Law, Technology, and the Organization of Work: Algorithms at Work: Productivity Monitoring Applications and Wearable Technology as the New Data-Centric Research Agenda for Employment and Labor Law*, 63 ST. LOUIS L. J. 21, 25 (2018).

[44] Katherine Keisler-Starkey & Lisa N. Bunch, *Health Insurance Coverage in the United States: 2020*, U.S. CENSUS BUREAU (Sept. 14, 2021), https://www.census.gov/library/publications/2021/demo/p60-274.html.

provisions promoting wellness programs.[45] Many of these wellness programs involve tracking health data, whether through user inputs or wearable technology like smart watches.[46] These smart watches and fitness trackers collect data on the individual's heart rate, diet, exercise, sleep, location, blood oxygen levels, and more.[47] This data collection is often justified as an effort to increase productivity, although the link between the two is unproven.[48] Even where such programs are nominally consensual, they may in practice be coerced by health insurance costs or by the precarity of many jobs.[49] Or, employees may not fully understand how much information they are turning over to their employers.[50]

Vast troves of collected data are often used to make mathematical models that help make decisions.[51] These predictions can be embarrassing, inconvenient, or discriminatory. In a famous example, Target analyzed shoppers' demographic data and shopping habits to assign each online customer a "pregnancy prediction" score.[52] Based on these scores, Target sent coupons for baby items to a teenage girl's home, which is how her father learned that she was pregnant.[53] In another instance, faulty and incomplete training data led a facial recognition algorithm to identify Black people as gorillas.[54] In the criminal justice system, algorithms for determining sentencing and recidivism risk factor in a defendant's circumstances of birth and upbringing, including family, neighborhood and friends, to determine how much time a defendant will stay in prison.[55] Yet as Cathy O'Neill points out, these models are subject to human bias and may create pernicious feedback loops by creating an environment that justifies the model's assumptions.[56] Still, these algorithmic outputs are inordinately trusted because of "automation bias," the tendency of people to "defer to computational judgments, even where they are

---

[45] Ajunwa et al., *supra* note 6, at 475.

[46] Brown, *supra* note 7, at *16.

[47] *Id.* at *7.

[48] Hull & Pasquale, *supra* note 13, at 190.

[49] Brown, *supra* note 7, at *14, *23.

[50] Daniel Susser, *Notice After Notice-and-Consent: Why Privacy Disclosures Are Valuable Even If Consent Frameworks Aren't*, 9 J. INFO. POLICY 1, 6 (2019) ("Most people do not read privacy notices. Those who do are confronted with notoriously long, technical contracts rendered in dense legalese.").

[51] AJAY AGRAWAL, JOSHUA GANS & AVI GOLDFARB, PREDICTION MACHINES: THE SIMPLE ECONOMICS OF ARTIFICIAL INTELLIGENCE 7 (2018).

[52] Kashmir Hill, *How Target Figured Out a Teen Girl Was Pregnant Before Her Father Did*, FORBES (Feb. 16, 2012), https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/?sh=125c9e7e6668.

[53] *Id.*

[54] Maggie Zhang, *Google Photos Tags Two African-Americans As Gorillas Through Facial Recognition Software*, FORBES (July 1, 2015), https://www.forbes.com/sites/mzhang/2015/07/01/google-photos-tags-two-african-americans-as-gorillas-through-facial-recognition-software/?sh=3471052a713d.

[55] CATHY O'NEILL, WEAPONS OF MATH DESTRUCTION (2016); Emily Barber, *Navigating* Miller v. Alabama *With COMPAS: How Risk Assessment Instruments Square with a Meaningful Opportunity for Release*, 77 NATL. LAW. GUILD REV. 1 (2020).

[56] O'Neill, *supra* note 55, at 10.

capable of recognizing that the situation calls for another choice."[57] Likewise, skewed training data for algorithms in the health data context can create acute risks for remote workers.

C. Risks of Remote Workers' Surveillance

Data privacy risks can be even more acute in the case of remote workers. These risks include discrimination, surveillance of family members and roommates, and unjust enrichment by employers selling intimate data without employees' permission.[58] This is in part due to the abrupt transition that many workers made to remote work, with few legally recognized protections.[59] In addition, by virtue of being at home, the surveilled employee opens up their personal lives to employers. This has the effect of blurring the line between home and work, impeding the employee's ability to have a personal life closed off to one's boss.[60] These intrusions into the homes of remote workers also implicate the privacy rights of family members or roommates.[61] For example, in 2017, a BBC interview went viral when Professor Robert Kelly's children entered his office.[62] Yet it is easy to imagine the same incident occurring in the case of a remote worker under constant monitoring, collecting audio and visual data about that child and penalizing the employee for the distraction. Webcam monitoring can also reveal whether an employee is pregnant, living with extended family, or of a certain sexual orientation.[63] The same is true for collection of genetic information and other kinds of health data that shed light on the personal health data of others.[64]

Independent contractors working for tech platforms, often called "gig workers," face even more pernicious monitoring.[65] In 2018, more than fifty-seven million

---

[57] Karen Yeung, *Algorithmic Regulation: A Critical Interrogation*, 12 REG. & GOVERNANCE 505, 516 (2018).

[58] Ajunwa, s*upra* note 43, at 35.

[59] Tiffany Li, *supra* note 10, at 781; *see also* Joseph J. Lazzarotti, *Out of Sight Is Not Out of Mind – Monitoring Workers Working from Home*, NATL. L. REV., (April 27, 2020), https://www.natlawreview.com/article/out-sight-not-out-mind-monitoring-workers-working-home.

[60] Jamie K. McCallum, *Remote Controlled Workers*, THE AMERICAN PROSPECT (Feb. 24, 2021), https://prospect.org/labor/remote-controlled-workers-digital-surveillance/.

[61] Jonathan Keane, *Bosses Putting a 'Digital Leash' on Remote Workers Could Be Crossing a Privacy Line*, CNBC (May 27, 2021), https://www.cnbc.com/2021/05/27/office-surveillance-digital-leash-on-workers-could-be-crossing-a-line.html.

[62] Simon Usborne, *The Expert Whose Children Gatecrashed His TV Interview: 'I Thought I'd Blown It in Front of the Whole World'*, THE GUARDIAN (Dec. 20, 2017), https://www.theguardian.com/media/2017/dec/20/robert-kelly-south-korea-bbc-kids-gatecrash-viral-storm.

[63] Corbyn, *supra* note 12.

[64] ALONDRA NELSON, THE SOCIAL LIFE OF DNA: RACE, REPARATIONS, AND RECONCILIATION AFTER THE GENOME 5 (2016); The Genetic Information Nondiscrimination Act (GINA) was enacted in 2008 and prohibits employers from discriminating against employees based on genetic information. Genetic Information Nondiscrimination Act of 2008, Pub. L. No. 110-233, 122 Stat. 881 (2008).

[65] JAMIE WOODCOCK & MARK GRAHAM, THE GIG ECONOMY: A CRITICAL INTRODUCTION 13 (Polity Press 2020).

U.S. workers were part of the gig economy, which includes Uber drivers, Etsy merchants, and other freelance workers.[66] Although gig workers have successfully mobilized to fight for better work conditions, they still lack significant benefits and employment law protections.[67] As such, gig workers face constant surveillance through rating systems, location tracking, and wearable technology.[68]

Health data collection poses critical privacy risks to workers. There are two main reasons why this is the case. The first is that much health data, and certainly the subset of biometric data, is immutable.[69] It cannot be changed like a password in the case of a breach, raising the stakes of its collection and its need for protection. This collection itself may be discriminatory, capturing inaccurate data if the technology has been exclusively fed data about and tested on white men.[70] Second, health data includes some of the most intimate information about a person. The collection of this data poses a range of privacy harms.[71] Employers may use this health data to make negative inferences about their employees. For example, an employer could review his employees' sleep patterns, exercise, caloric intake, or mood to make promotion considerations.[72]

Employers can also use data collected from fertility tracking apps to discriminate against women who are pregnant or trying to conceive.[73] As more states ban abortion, privacy of fertility data may have criminal implications. After the Supreme Court overruled ***Roe*** and ***Casey*** and held that the Constitution does not confer a right to abortion in ***Dobbs v. Jackson Women's Health***, privacy activists expressed concerns that insecure data from fertility-tracking apps could result in advertisers, employers, and law enforcement knowing when people are pregnant.[74] Third party software such as menstrual tracking apps are not bound by federal privacy laws, and may share that data with law enforcement or employers.[75] It is

---

[66] TJ McCue, *57 Million U.S. Workers Are Part of the Gig Economy*, FORBES (Aug. 31, 2018), https://www.forbes.com/sites/tjmccue/2018/08/31/57-million-u-s-workers-are-part-of-the-gig-economy/?sh=7a21bc767118.

[67] Miriam A. Cherry & Ana Santos Rutschman, *Gig Workers as Essential Workers: How to Correct the Gig Economy Beyond the COVID-19 Pandemic*, 35 ABA J. LAB. & EMP. L. 11, 12—13 (2020).

[68] Alex Kirven, *Whose Gig Is It Anyway? Technological Change, Workplace Control and Supervision, and Workers' Rights in the Gig Economy*, 89 U. COLO. L. REV. 249, 265 (2018); Alex Rosenblat & Luke Stark, *Algorithmic Labor and Information Asymmetries: A Case Study of Uber's Drivers*, 10 INTL. J. COMM. 3758, 3772 (2016).

[69] Alterman, *'A Piece of Yourself:' Ethical Issues in Biometric Identification*, 5 ETHICS AND INFO. TECH. 139 (2003).

[70] Elizabeth Brown, *The Femtech Paradox: How Workplace Monitoring Threatens Women's Equity*, 61 JURIMETRICS J. 289, 296 (2021).

[71] Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U. L. REV. 793 (2022).

[72] Brown, *supra* note 7, at 19–20.

[73] Brown, *Femtech Paradox*, *supra* note 70, at 310.

[74] Dobbs v. Jackson Women's Health Org., 142 S. Ct. 2228 (2022); Lil Kalish, *Meet Abortion Bans' New Best Friend – Your Phone*, MOTHER JONES (Feb. 16, 2022), https://www.motherjones.com/politics/2022/02/meet-abortion-bans-new-best-friend-your-phone/.

[75] Cynthia Conti-Cook, *Surveilling the Digital Abortion Diary*, 50 U. BALT. L. REV. 1, 73 (2020); Natasha Singer, *When Apps Get Your Medical Data, Your Privacy May Go With It*, N.Y.

not merely speculative that fertility data will be shared without users' knowledge. There are dozens of data brokers that promote access for advertisers to tens of millions of people in the United States identified in data sets as "actively pregnant" or "shopping for maternity products."[76] Electronic payment information and location tracking can also be used to potentially identify pregnant people and those who are seeking abortions.[77] A remote worker who goes to an abortion clinic but cannot part with her work phone may unwittingly be revealing this sensitive information to her employer. Under the guise of corporate wellness programs, employers are already tracking employees' menstrual cycles.[78]

D. Remote Worker Surveillance Highlights Flawed Approach to Data Privacy

The lack of privacy protections for remote workers, described below in Part III, highlights a more conceptual problem with current privacy law. Overemphasis on consent and anonymity, and an underemphasis on the equity of data collection, limit the ability of U.S. privacy law to address the greatest surveillance harms.

The first conceptual problem of current privacy law is an overreliance on consent. Current data privacy law generally operates by a notice-and-consent regime.[79] Under this approach, so long as the individual is notified about the data collection and consents to it, data controllers can do essentially whatever they please.[80] Yet this is often consent in name only. Privacy scholars Richards and Hartzog identify what they call "gold standard consent," defined as "agreements between parties who have equal bargaining power, significant resources, and who *knowingly* and *voluntarily* agree to assume contractual or other legal obligations.[81] This definition fails when applied to remote worker data surveillance, where the power asymmetry between employers and employees remains a barrier to worker

---

TIMES (Sept. 3, 2019), https://www.nytimes.com/2019/09/03/technology/smartphone-medical-records.html.

[76] Shoshana Wodinsky & Kyle Barr, *These Companies Know When You're Pregnant—And They're Not Keeping It a Secret*, GIZMODO (July 30, 2022), https://gizmodo.com/data-brokers-selling-pregnancy-roe-v-wade-abortion-1849148426.

[77] Ron Lieber & Tara Siegel Bernard, *Payment Data Could Become Evidence of Abortion, Now Illegal in Some States*, N.Y. TIMES (June 29, 2022), https://www.nytimes.com/2022/06/29/business/payment-data-abortion-evidence.html?smid=nytcore-ios-share&referringSource=articleShare; *see* Kalish, *supra* note 74 (describing how geo-fencing–the use of location data to target people in a given area–can be used to track people who visit abortion clinics).

[78] Drew Harwell, *Is Your Pregnancy App Sharing Your Intimate Data With Your Boss?*, WASH. POST (Apr. 10, 2019), https://www.washingtonpost.com/technology/2019/04/10/tracking-your-pregnancy-an-app-may-be-more-public-than-you-think/.

[79] Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 WASH. U. L. REV. 1461 (2019).

[80] Julie E. Cohen, *How (Not) to Write a Privacy Law*, KNIGHT FIRST AMENDMENT INSTITUTE AT COLUMBIA UNIVERSITY (Mar. 23, 2021), https://knightcolumbia.org/content/how-not-to-write-A-privacy-law.

[81] Richards & Hartzog, *supra* note 79, at 1463.

autonomy.[82] Where health data is collected under threat of health insurance premium increases or other penalties, coercion precludes consent. Requiring notice and consent gives employees power to control what data is collected about them, but only up to a point. Although a worker could refuse to sign the consent form mandated by the law, in practice doing so would jeopardize that worker's employment.[83]

Yet there is a deeper problem than the practical issues of obtaining this "gold standard consent" in an employment context. Not only may workers not fully understand the scope of data collection or its purpose when they consent, but there are certain uses of data that are undesirable even if a worker consents to it, such as those that result in discrimination or other inequities.

A second pillar of privacy law is anonymity. Some may dismiss concerns about data collection based on the presumption that the data is anonymized and therefore unobtrusive.[84] Not so fast. First, it may not even claim to be anonymous. Second, even if it purports to be anonymized, it may be easy to figure out the identity in a process called "reidentification."[85] In one experiment, eighty-seven percent of the U.S. population (216 million) was identifiable based on zip code, gender, and date of birth.[86] More recently, researchers compared movie reviews on IMDB with an anonymized dataset of 500,000 Netflix users to successfully identify Netflix users, down to their political preferences and other sensitive information.[87] Even if the data does remain anonymous, it can still breach employee privacy and cause harm. The internalized surveillance effect of being constantly monitored infringes upon individual autonomy and may chill expression.[88] Also, employers can rely on aggregated data from all employees to make judgments about individuals.[89]

---

[82] Cyphers & Gullo, *supra* note 3; Gabrielle Neace, *Biometric Privacy: Blending Employment Law with the Growth of Technology*, 53 UIC J. MARSHALL L. REV. 73, 101 (2020) ("[E]mployees may rebel against biometric timekeeping and risk losing their employment when they refuse to relinquish their biometric data.").

[83] Widespread reports of a "worker shortage" or the "Great Resignation" does not negate this power imbalance. Even if there are other jobs available to a worker who refuses to consent to electronic monitoring, to lose a job for that or any other reason can be disruptive or debilitating. Also, as more employers adopt electronic monitoring and health data surveillance measures, finding a comparable job that does not engage in such data collection will become increasingly difficult. *See I.R.S. Report*, THE STATE OF LABOR MARKET COMPETITION (Mar. 7, 2022), https://home.treasury.gov/system/files/136/State-of-Labor-Market-Competition-2022.pdf.

[84] Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1701 (2010) ("Anonymization plays a central role in modern data handling, forming the core of standard procedures for storing or disclosing personal information.").

[85] *Id.*

[86] Latanya Sweeney, *Simple Demographics Often Identify People Uniquely*, CARNEGIE MELLON UNIVERSITY DATA PRIVACY WORKING PAPER 3 (2000).

[87] Arvind Narayanan & Vitaly Shmatikov, *Robust De-Anonymization of Large Sparse Datasets*, 29TH ANNUAL IEEE SYMPOSIUM ON SECURITY AND PRIVACY, 111—125 (2008).

[88] Neil Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1935 (2013).

[89] Abigail Gilbert & Anna Thomas, *The Amazonian Era: The Gigification of Work*, INSTITUTE FOR THE FUTURE OF WORK 31 (May 2021).

A third concern is one that we may call equity sharing. Employers who collect health data to maximize the productivity of their workforce gain considerable advantage from these inferences.[90] The employees, meanwhile, suffer losses from the harvesting of their potentially profitable personal information.[91] The power asymmetry in employer surveillance manifests in not only unfairness but also increased financial inequality and the emergence of a "surveilled class."[92] By emphasizing the circumstances of data collection and breaches over the intended uses, privacy law fails to provide any kind of fair benefit-sharing between employees who turn over intimate data and the employers who profit from it.

Yet there is a deeper, conceptual issue with the privacy laws than the issues described above. Underlying this overreliance on consent and anonymity is a fundamentally individual approach to governing data. An exclusive focus on trees overlooks the forest of data surveillance that most seriously impacts the data subjects. Brent Mittelstadt noted that shared ownership of identity is largely ignored in data privacy law and argues for legally recognized privacy rights of ad hoc groups that are formed, often without the knowledge of those involved, for purposes of data inferences and predictions.[93] This grouping of individuals and the data analysis of individuals that are associated creates community harms that cannot be sufficiently understood nor addressed without a collective frame.[94]

Salomé Viljoen has argued that the wrongfulness of data collection occurs when it materializes unjust social relations, such as unfair wealth distributions or group oppression.[95] Instead of an individualistic framing, Viljoen advocates the concept of "data as a democratic medium" ("DDM"), which recognizes the population-level interests that arise from data production.[96] Under this view, the focus on individual notice-and-consent cannot meaningfully address the power imbalances between data collectors and individuals (what Viljoen calls the "vertical axis") nor the impact that one person's data collection may impact one or many other people (the "horizontal axis").[97] Proposals that align with the DDM approach include public management authorities to ensure that vast troves of collected data are only used to the public benefit.[98] A more group-centric data governance regime would better recognize and stem the hazards of health data surveillance of remote workers than

---

[90] Julie E. Cohen, *The Biopolitical Public Domain: The Legal Construction of the Surveillance Economy*, 31 PHILOS. TECH. 213, 222 (2018).

[91] *Id.* at 226.

[92] Richards, *supra* note 88, at 1956.

[93] Brent Mittelstadt, *From Individual to Group Privacy in Big Data Analytics*, 30 PHILOSOPHY & TECH. 475, 479 (2017).

[94] Astha Kapoor, "Data Stewardship: Collective Bargaining for Privacy," OBSERVER RESEARCH FOUNDATION, Oct. 3, 2020, https://www.orfonline.org/expert-speak/data-stewardship-collective-bargaining-for-privacy-74488/.

[95] Viljoen, *supra* note 29, at 631.

[96] *Id.* at 634–638.

[97] *Id.* at 607.

[98] *Id.* at 645.

individual-focused privacy law. A careful examination of relevant federal and state laws and regulations lays bare these deficiencies.

III. CURRENT LEGAL AND REGULATORY LANDSCAPE

Federal privacy law consists of a patchwork of sector-specific laws.[99] The Health Insurance Portability and Accountability Act ("HIPAA") establishes national standards for protecting individually identifiable health information, but it does not apply to employers specifically or consistently.[100] Federal agencies like the FTC, EEOC, and others have yet to squarely address the harms of remote workers' health data surveillance.[101] At the State level, even California and Illinois, two of the most privacy-protective states, still fall short of adequately addressing this pervasive surveillance.[102] As such, Part IV will discuss various proposals to expand privacy protections for remote workers.

A. Federal Law and Agencies

1. HIPAA

At the Federal level, current laws and regulations inadequately protect the data privacy of remote workers. Even where federal law regulates the collection of health data, significant gaps remain.[103] The United States lacks a comprehensive federal privacy law.[104] Instead, federal privacy statutes constitute a patchwork of sector-specific laws that offer privacy protections for certain kinds of information within a narrow domain.[105]

For present purposes, the most relevant of these federal laws is HIPAA.[106] HIPAA was passed in 1996 to protect patients' health records and personally identifiable medical information, recognizing for the first time the particular sensitivity of health data, and imposed rigid restrictions on the transfer of medical records and other health information.[107] Under HIPAA and corresponding HHS regulations, covered entities may not use or disclose protected health information except under certain conditions, and must disclose what information they have

---

[99] Chander et al., *supra* note 22, at 1748.

[100] Kevin J. Haskins, *Wearable Technology and Implications for the Americans with Disabilities Act, Genetic Information Nondiscrimination Act, and Health Privacy*, 33 A.B.A. J. LAB. & EMP. L. 69, 76 (2017).

[101] *See infra* Part III.A.1–5.

[102] *See infra* Part III.B.

[103] Brown, *supra* note 7, at 21.

[104] Daniel J. Solove & Paul M. Schwartz, *ALI Data Privacy: Overview and Black Letter Text*, 68 UCLA L. REV. 1252 (2022) (noting the lack of a "comprehensive federal privacy law" in the United States).

[105] Chander et al., *supra* note 22.

[106] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified as amended in scattered sections of 29 and 42 U.S.C.).

[107] Timothy Newman & Jennifer Kreick, *The Impact of HIPAA (and Other Federal Law) on Wearable Technology*, 18 SMU SCI. & TECH. L. REV. 429 (2015).

about an individual to them upon request.[108] HIPAA also prohibits group health plans from requesting, requiring or purchasing genetic information from anyone enrolled in the plan.[109]

However, HIPAA provisions only apply to "covered entities," which are health plans, healthcare clearinghouses, and health care providers, as well as some "business associates" who carry out healthcare functions for covered entities.[110] Thus, HIPAA does not apply to most third-party software companies that collect health information from users and then may sell it to advertisers.[111]

The Department of Health and Human Services is responsible for implementing HIPAA, and includes a division called the Office of Civil Rights ("OCR"). The OCR is charged with enforcing HIPAA's Privacy, Security, and Breach Notification Rules, among other things.[112]

Most employers are not considered covered entities under HIPAA. The OCR has stated that on workplace wellness programs "offered by an employer directly and not as part of a group health plan, the health information that is collected from employees by the employer is not protected by the HIPAA Rules."[113] The OCR clarifies on its website that even if you work for a covered entity, your employment records are not covered by the HIPAA privacy rule. Instead, HIPAA protects the employee's medical or health plan records as a patient of the provider or member of the health plans.[114] The OCR also issued guidance that an app developer is not a business associate of a covered entity if a doctor recommends to a patient an app for dieting, exercising, or weight management.[115] A health tracking app, according to this guidance, would be covered under HIPAA if the app was offered by the health plan, but not for a direct-to-consumer app.[116]

Even if employers were categorically included in HIPAA, whether by judicial interpretation or legislative amendment, it would still fall short of addressing the regulatory gap of employee data collection laid out in the previous Part. One main

---

[108] 45 C.F.R. § 164.502(a) (2022).

[109] 29 U.S.C. § 1182(d)(2).

[110] 45 C.F.R. § 160.103 (2022); Brown, *supra* note 7, at 24.

[111] HHS Office for Civil Rights, *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, HHS.GOV, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html (last visited Dec. 20, 2022).

[112] HHS Office for Civil Rights, *About Us*, HHS.GOV, https://www.hhs.gov/ocr/about-us/index.html (last visited Mar. 2, 2022).

[113] HHS Office for Civil Rights, *HIPAA Privacy and Security and Workplace Wellness Programs*, HHS.GOV, https://www.hhs.gov/hipaa/for-professionals/privacy/workplace-wellness/index.html (last visited Jan. 30, 2022).

[114] HHS Office for Civil Rights, *Employers and Health Information in the Workplace*, HHS.gov, https://www.hhs.gov/hipaa/for-individuals/employers-health-information-workplace/index.html (last reviewed Nov. 2, 2020).

[115] HHS Office for Civil Rights, *Health App Use Scenarios & HIPAA*, HHS.GOV, https://www.hhs.gov/sites/default/files/ocr-health-app-developer-scenarios-2-2016.pdf (last visited Jan. 30, 2022).

[116] *Id.*

issue with HIPAA is that it only applies to "individually identifiable" data. Health information that is aggregated or de-identified within the meaning of the Act is not covered by the privacy protections.[117] Yet even with aggregated data, employers can make or receive from health tech companies inferences that intrude upon the privacy rights of workers or their families.[118] Plus, HIPAA does not grapple with novel modes of re-identifying data that may render the anonymization requirement a small speed bump rather than a meaningful hurdle.[119] Therefore, reliance on HIPAA to stem the abusive surveillance practices of employers upon remote workers will fall short unless there are fundamental changes that recognize this particular harm.

HIPAA also only applies to health data collection in an employment context under certain circumstances. If the data is collected as part of a wellness program that is offered through a group health plan, then the individually identifiable health information collected or created about participants is protected health information ("PHI") and thus covered by the HIPAA Rules.[120] If HIPAA does apply to vendors of wellness programs and health tech, then the information must be kept confidential and workers could demand a copy of the data and control its uses.[121]

2. FTC

Under the leadership of Lina Khan, the FTC has taken active measures to increase privacy protections for consumers, including from health apps. In September 2021, the FTC released a policy statement offering guidance on its Health Breach Notification Rule, 16 C.F.R. Part 318.[122] The Rule requires vendors and custodians of personal health records ("PHR") and PHR-related entities to notify U.S. consumers and the FTC if there has been a breach of identifiable health information, under threat of civil penalties.[123] Although the rule is only triggered when there is a breach of security, a "breach" includes any sharing of sensitive health information without the individual's authorization.[124] An app developer or other health technology company is covered by the Rule if they obtain personal health records from multiple sources, such as from the app directly and from its corresponding fitness tracker, or if it collects health information as well as non-health data, from the phone's calendar, for instance.[125]

---

[117] Brown, *supra* note 7, at 26.

[118] Alicia Solow-Niederman, *Information Privacy and the Inference Economy*, 117 NW. U. L. REV. 357 (2022).

[119] Brown, *supra* note 7, at 26.; s*ee also* Ohm, *supra* note 84, at 1706.

[120] Newman & Kreick, *supra* note 107.

[121] Ajunwa et al., *supra* note 6, at 477.

[122] FTC, *Statement of the Commission on Breaches by Health Apps and Other Connected Devices*, FED. TRADE COMM'N (Sept. 15, 2021), https://www.ftc.gov/system/files/documents/public_statements/1596364/statement_of_the_commission_on_breaches_by_health_apps_and_other_connected_devices.pdf.

[123] *Id.*

[124] *Id.*

[125] *Id.*

This policy guidance is encouraging insofar as it demonstrates that the FTC is sensitive to the widespread collection of health data by private entities. However, it does nothing to curb the collection of intimate health data in the first place, focusing instead on notification after the fact.[126] The rule was intended merely to patch one hole in the enforcement of HIPAA, and to bring accountability to certain non-covered entities under HIPAA when they experience a data breach.[127]

3. EEOC

The EEOC, among other things, sues employers for violations of the Americans with Disabilities Act ("ADA").[128] The ADA prohibits employers from requiring employees to undergo medical examinations and disability-related inquiries, unless shown to be job-related and consistent with business necessity.[129] The EEOC has sued employers where hiring, firing and promotion decisions were based on data that amounts to discrimination based on protected class.[130]

However, these efforts by the EEOC to constrain employers have so far proven unsuccessful. In various cases where the EEOC sued to limit the collection of health data or enjoin the fining of employees who decline to participate in wellness programs, courts have ruled against the agency. For example, in ***EEOC v. Flambeau***, the EEOC sued an employer who conditioned participation in a health insurance plan on completing a "health risk assessment and biometric screening test."[131] Except for information regarding tobacco use, the health risks and medical conditions were aggregated before the employer saw it.[132] The employer incentivized participation in the plan with a six hundred dollar credit, without which the insurance plan was unaffordable to some employees.[133] The court determined that the wellness program requirement fell within the ADA's safe harbor provision, which does not "prohibit or restrict" an employer from administering "the terms of a bona fide benefit plan that are based on underwriting risks, classifying risks, or administering such risks."[134] Absent a clear showing of "disability-based distinctions" involved, the court found the employer's plan to be "based on" a legitimate business purpose, and denied EEOC's motion for summary judgment.[135]

---

[126] *Id.*

[127] *Id.*

[128] Overview, EQUAL EMPLOYMENT OPPORTUNITY COMMISSIONS, https://www.eeoc.gov/overview (last visited Mar. 9, 2022).

[129] 42 U.S.C. § 12112(d)(4)(A).

[130] *See, e.g.*, EEOC v. Orion Energy Sys., 209 F. Supp.3d 989 (E.D. Wis. 2016); *see also* Sharona Hoffman & Andy Podgurski, *Artificial Intelligence and Discrimination in Health Care*, 19 YALE J. POL'Y, L. & ETHICS 1 (2020).

[131] EEOC v. Flambeau, Inc., 131 F.Supp.3d 849 (W.D. Wis. 2015).

[132] *Id.* at 852.

[133] *Id.*

[134] 42 U.S.C. § 12201(c)(2).

[135] *EEOC v. Flambeau*, at 857; *see also* EEOC v. Orion Energy Sys., Inc., 208 F.Supp.3d 989 (E.D. Wis. 2016) (interpreting ADA safe harbor provision broadly to include employer's use of wellness programs).

In *EEOC v. Honeywell*, the EEOC sued to enjoin an employer from levying penalties against employees who refused to undergo biomedical testing as part of the company's wellness program.[136] Enrollees in Honeywell's High Deductible Health Plan[137] were subject to financial surcharges of about $500 if they declined to participate in the wellness program, which was designed to inform participants about their health status and encourage improvement of health goals.[138] Noting "great uncertainty" as to how the Affordable Care Act ("ACA"), ADA, The Genetic Information Nondiscrimination Act ("GINA") and other federal laws are intended to interact, the court denied EEOC's motion for a preliminary injunction, finding no risk of irreparable harm to employees whose data is collected, because the financial surcharge could be refunded later.[139]

These cases highlight three problems with data governance law that are relevant here. First, the lack of true consent by employees to participate; that is, the levying of fines or withholding of financial credit to employees who decline to participate in wellness programs renders the collection of health data from employees coercive.[140] The EEOC in *Honeywell* only sought to enjoin the financial penalties for those who declined to participate, but this effort was rejected.[141] Second, the aggregation of data does not obviate the privacy risks. As described above, purely individualistic conceptions of data privacy fail to capture the extent of harm that can occur from surveillance of sensitive data, even where it may be nominally anonymized.[142] Third, these cases brought under the ADA are too narrowly focused on overt discrimination, as opposed to more subtle but no less sinister discrimination based on data analytic inferences that may be unknown to the employee.[143] But even where no such discrimination occurs, collection and analysis of health data can be severely intrusive.

The EEOC has begun to address potential bias in artificial intelligence in hiring, but so far has neglected the risks of employee health data collection. More recently, the EEOC has taken efforts to curb the abuses of artificial intelligence in the employment context. In October 2021, the EEOC announced an initiative to ensure that applications of artificial intelligence in hiring, promotion, and firing decisions

---

[136] EEOC v. Honeywell Int'l, Inc., No. 14–4517, WL 5795481 at *1 (D. Minn. 2014).

[137] Individuals with high-deductible health plans pay lower monthly insurance premiums but pay more out of pocket for medical expenses until their deductible is met. Robin A. Cohen & Emily P. Zammitti, *High-Deductible Health Plan Enrollment Among Adults Aged 18-64 With Employment-based Insurance Coverage*, CDC NAT'L CTR. HEALTH STAT. DATA BRIEF, AUGUST 2018, AT 1, https://www.cdc.gov/nchs/products/databriefs/db317.html.

[138] *EEOC v. Honeywell Int'l*, *supra* note 136, at *1.

[139] *Id.* at *5.

[140] Nearly sixty percent of Americans reported not having enough money saved to cover a $500 unplanned expense. Karthyn Vasel, *6 in 10 Americans Don't have $500 in Savings*, CNN MONEY (Jan. 12, 2017), https://money.cnn.com/2017/01/12/pf/americans-lack-of-savings/index.html.

[141] *EEOC v. Honeywell Int'l*, *supra* note 136, at *6.

[142] *See, e.g.*, Mittelstadt, *supra* note 93, at 475–494 ("algorithmically grouped individuals have a collective interest in how information describing the group is generated and used.").

[143] Roberts, *supra* note 24, at 2113.

do not run afoul of federal civil rights laws.[144] The Justice Department is also reviewing whether guidance on algorithmic fairness and the use of AI may be necessary and effective at preventing discrimination in hiring, according to Kristen Clarke, Assistant Attorney General for Civil Rights.[145]

4. NLRB

The National Labor Relations Board ("NLRB") has not made significant progress on employee privacy. Established in 1935 by the National Labor Relations Act ("NLRA"), the NLRB protects workers' right to organize and bargain collectively.[146] Yet this protection does not extend to some of the workers subject to the most stringent surveillance, namely independent contractors or gig workers, who are similarly incessantly tracked.[147] Independent contractors are expressly exempted from the NLRA.[148] To the extent that the NLRB has developed privacy rules, such rules have focused on safeguarding contact information of workers eligible to vote in union elections.[149] While this is an important privacy protection for workers engaged in collective bargaining, it does not extend to remote worker surveillance writ large.

5. Other Agencies

Recent regulations from other agencies are no more attentive to remote employees' specific privacy needs. Instead, these tend to be more focused on the security of company information rather than the privacy of employees. The National Institute of Standards and Technology ("NIST") and the Cybersecurity and Infrastructure Security Agency ("CISA") have issued rules about authentication protocols, encrypted VPNs, anti-malware software and so forth.[150]

---

[144] Press Release, from Equal Emp. Opportunity Comm'n, "EEOC Launches Initiative on Artificial Intelligence and Algorithmic Fairness" (Oct. 28, 2021), https://www.eeoc.gov/newsroom/eeoc-launches-initiative-artificial-intelligence-and-algorithmic-fairness.

[145] Kristen Clarke, Keynote on AI and Civil Rights for the Department of Commerce's National Telecommunications and Information Administration's (NTIA) Virtual Listening Session (Dec. 14, 2021), https://www.justice.gov/opa/speech/assistant-attorney-general-kristen-clarke-delivers-keynote-ai-and-civil-rights-department.

[146] Kate Andrias, *The New Labor Law*, 126 YALE L.J. 2, 13—14 (2016).

[147] *See, e.g.*, Miriam Cherry, *Beyond Misclassification: The Digital Transformation of Work*, 37 COMPAR. LAB. L. & POL'Y J. 577, 583 (2017) (describing how Uber maintains "almost a constant surveillance over workers, with consumers deputized to manage the workforce").

[148] National Labor Relations (Wagner) Act § 2(3), 29 U.S.C. § 152(3) (2012); Andrias, *supra* note 146, at 29.

[149] Representation-Case Procedures: Voter List Contact Information; Absentee Ballots for Employees on Military Leave, Federal Register Vol. 85, No. 146, (proposed July 29, 2020).

[150] Comput. Sec. Res. Ctr., Nat'l Inst. Standards Tech., SP 800-46 Rev. 2, Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security, (2016), https://csrc.nist.gov/publications/detail/sp/800-46/rev-2/final; Cybersecurity Infrastructure Sec. Agency, Trusted Internet Connections 3.0 Interim Telework Guidance (2020) https://www.cisa.gov/sites/default/files/publications/CISA-TIC- TIC%203.0%20Interim%20Telework%20Guidance-2020.04.08.pdf.

But, as discussed above, this is a different kind of data privacy than that which concerns employees themselves for the purposes of wellness programs or other means of data collection.

Therefore, federal agencies are not adequately equipped under the existing legal and regulatory regime to address the privacy risks of health data.[151]

B. State Laws

Numerous states have gone further than the federal government in recognizing the importance of data privacy and health data in particular and enacting robust protections for employees and consumers. The California Consumer Privacy Act ("CCPA") in California and the Biometric Information Privacy Act ("BIPA") in Illinois are two notable examples.[152] BIPA and CCPA offer an illustrative dichotomy in approaches to state-level privacy laws. BIPA went into effect in 2008 while the CCPA went into effect in January 2020, with enforcement beginning in August of that year.[153] BIPA covers a relatively narrow, though important, kind of data, that regarding biometric identifiers such as retina or iris scans, fingerprints, voiceprints, or scans of hand or face geometry.[154] The CCPA, by contrast, has a much broader scope covering "personal information," defined as that which "identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."[155] Both privacy laws include private rights of action, allowing individuals to recover damages or injunctive relief for violations of the law, although individuals may only sue under the CCPA following a data breach.[156]

This Part shows that even Illinois and California, two states with some of the strongest and most comprehensive privacy laws in the country, still do not adequately protect remote workers from surveillance of their intimate health data.

---

[151] Even this existing regulatory regime may be in jeopardy after *West Virginia v. EPA*, 142 S.Ct. 2587 (2022), where the Supreme Court invoked the "Major Questions Doctrine" to find that the EPA lacked "clear congressional authorization" to implement the Obama-era "Clean Power Plan." *West Virginia*, 142 S.Ct., at 2595. Legal scholars have argued that the Major Questions Doctrine, purportedly only for extraordinary occasions, could be used more broadly to strike down agency regulations. *See, e.g.*, Rachel Frazin, *Supreme Court's EPA Ruling Could Put Other Regs in Danger*, THE HILL (June 30, 2022), https://web.archive.org/web/20220706212510/https://thehill.com/policy/energy-environment/3543285-supreme-courts-epa-ruling-could-put-other-regs-in-danger/. *See also* Elizabeth Kolbert, *The Supreme Court Case that Could Upend Efforts to Protect the Environment*, THE NEW YORKER (January 10, 2022), https://www.newyorker.com/news/daily-comment/the-supreme-court-case-that-could-upend-efforts-to-protect-the-environment.

[152] California Consumer Privacy Act (CCPA), CAL. CIV. CODE §§ 1798.100-1798.199 (West 2022); Biometric Information Privacy Act, 740 Ill. Comp. Stat., 14/1 (2008).

[153] California Consumer Privacy Act (CCPA), CAL. CIV. CODE §§ 1798.100-1798.199 (West 2022); Biometric Information Privacy Act, 740 Ill. LComp. Stat., 14/1(2008).

[154] Biometric Information Privacy Act, 740 Ill. LComp. Stat., 14/1(2008).

[155] CCPA § 1798.140(o)(1).

[156] CCPA § 1798.150; BIPA § 20.

As such, this Part establishes that different legislative and regulatory approaches are needed, which will be examined in Part IV.

1. Illinois

Illinois broke new ground in statutory protection of information when it passed the BIPA in 2008.[157] Many cases have been brought under the BIPA, several of which concern employees' privacy rights.[158]

BIPA regulates the "collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information."[159] Biometric identifiers are defined in the Act as "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry."[160] The Act prohibits any private entity from collecting, capturing, purchasing, receiving through trade or otherwise obtaining a person's biometric identifiers or information unless they provide written notice as to the collection, its purpose and the duration of storage, and receive written consent.[161]

Biometric information, which is any information based on an individual's biometric identifier used to identify an individual, often overlaps with health data, with similarly sensitive inferences that may be drawn. [162] One case that highlights the intersection between BIPA and privacy of employees' health data is the ongoing litigation of ***Naughton v. Amazon***.[163] Around June 2020, Amazon began requiring workers to provide scans of their face geometry as part of wellness checks before they were permitted to enter the facility.[164] William Naughton, an Amazon employee in Joliet, Illinois, alleges that Amazon violated BIPA by collecting face geometry scans of individuals without their knowledge or consent.[165] The District Court denied Amazon's motion to dismiss, and the case proceeds as of this writing.[166]

Examining how the Illinois courts analyze an employee's expectation of privacy may shed light on how protected employees will be when they are working from home. In ***People v. Neal***, for example, the court held that a police officer did not have a reasonable expectation of privacy over his police-issued raincoat pouch containing fraudulent traffic citations, inside his police-issued squad car, both of

---

[157] Biometric Information Privacy Act, 740 Ill. Comp. Stat. §§ 14/1-14/99 (2008).

[158] ***Id. See also*** Jake Holland, ***As Biometric Lawsuits Pile Up, Companies Eye Adoption With Care***, BLOOMBERG LAW (Feb. 9, 2022), https://news.bloomberglaw.com/privacy-and-data-security/as-biometric-lawsuits-pile-up-companies-eye-adoption-with-care.

[159] BIPA § 5(g).

[160] ***Id.*** at § 10.

[161] Rosenbach v. Six Flags Ent. Corp., 129 N.E.3d 1197, 1203 (2019).

[162] BIPA § 10.

[163] Naughton v. Amazon.com, Inc., No. 20-CV-6485, 2022 U.S. Dist. WL 19324 (N.D. Ill. Jan. 3, 2022).

[164] ***Id.***

[165] ***Id.*** at *1.

[166] ***Id.*** at *4.

which were subject to regular inspections.[167] Additionally, in ***People v. Popely***, the defendant argued the trial court erred in denying his motion to suppress evidence relating to an attempted rape allegation.[168] The officer seized articles that he saw through a glass door; items were found on the floor of the office, in a wastebasket, and in an aisle between desks.[169] The office was not reserved for defendant's exclusive use nor was defendant present when the search occurred. Therefore, the court said, there was no expectation of privacy.[170]

Although these cases concerned a criminal case and a government search, ***Popely*** and ***Neal*** are instructive as to an employee's reasonable expectation of privacy in Illinois. Both suggest that an employee has no expectation of privacy in their work-issued clothing or devices, nor in spaces that are shared with other employees. Yet therein lies a contradiction that is relevant to this Note. Namely, what happens when data is collected from an employee through a work-issued device, in the employee's private home? This is a tension that Courts have not yet addressed, and which no legislation directly resolves.

Regardless, BIPA suffers from serious defects. The primary requirement in BIPA is informed consent from employees to have their biometric information collected.[171] Aside from a few proscribed uses of this biometric data, companies may do whatever they want with biometric information once they obtain employees' one-time consent, with no provision for revoking consent.[172] BIPA imposes no restrictions on the hiring, promoting or firing of employees based on inferences they have made from that information.[173] For instance, if a geometric face scan, collected with the consent of the employee, indicates through software the presence of swollen lymph nodes, there is nothing in BIPA to prevent an employer from passing over that employee for a promotion based on a likelihood that that person may be developing a sickness.[174]

2. California

The California Constitution includes privacy as an inalienable right.[175] To plead a privacy violation under the California Constitution, a plaintiff must allege that "(1) they possess a legally protected privacy interest, (2) they maintain a reasonable

---

[167] People v. Neal, 486 N.E.2d 898, 5, 32, 34, 36 (Ill. 1985).
[168] People v. Popely, 345 N.E.2d 125, 126 (Ill. App. Ct. 1976).
[169] *Id.* at 129.
[170] *Id.*
[171] Bryant v. Compass Grp. USA, Inc., 958 F.3d 617, 619 (7th Cir. 2020).
[172] Cohen, *supra* note 80.
[173] *Id.*
[174] Dennis D. Hirsch, *That's Unfair! Or is it? Big Data, Discrimination and the FTC's Unfairness Authority*, 103 KY. L.J. 345, 350–352 (2015).
[175] Cal. Const. art. 1, § 1.

expectation of privacy, and (3) the intrusion is 'so serious … as to constitute an egregious breach of the social norms' such that the breach is 'highly offensive.'"[176]

California has its own version of HIPAA at the state level: The California Confidentiality of Medical Information Act ("CMIA").[177] This law provides a private right of action for violations, which HIPAA does not.[178] The CMIA also explicitly acknowledges the role of applications and software in the collection and transfer of health information. Under the law,

> "Any business that offers software or hardware to consumers, including a mobile application or other related device that is designed to maintain medical information, as defined in subdivision (g) of Section 56.05, in order to make the information available to an individual or a provider of health care at the request of the individual or a provider of health care, for purposes of allowing the individual to manage his or her information, or for the diagnosis, treatment, or management of a medical condition of the individual, shall be deemed to be a provider of health care subject to the requirements of this part."[179]

However, § 56.05(g) covers only "health care service plans," defined as "any entity regulated pursuant to the Knox-Keene Health Care Service Plan Act of 1975 (Chapter 2.2 (commencing with Section 1340) of Division 2 of the Health and Safety Code)."[180] As a result, this law does not adequately cover the dynamics of information collection of employees by employers, nor does it extend to wellness and fitness programs which may be entirely removed from employer-sponsored health insurance plans.

In January 2020, the CCPA went into effect, with corresponding regulations effectuated in August 2020.[181] Unlike BIPA, which has a narrow focus on biometric information, the CCPA takes a comprehensive approach to consumer privacy.[182] Its privacy protections extend to inferences drawn from personal information to "create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.[183] In November 2020, California voters passed

---

[176] ***In re*** Facebook, Inc. Internet Tracking Litigation, 956 F.3d 589, 601 (9th Cir. 2020) (citing Hernandez v. Hillsides, Inc., 211 P.3d 1063, 1073 (Cal. 2009)).

[177] Confidentiality of Medical Information Act, CAL. CIV. CODE §§56–56.37 (Deering 2022).

[178] CAL. CIV. CODE § 56.36(b) (Deering 2022); Payne v. Taslimi, 998 F.3d 648, 660 (4th Cir. 2021) (concluding and collecting cases that likewise held that HIPAA does not create a private right of action).

[179] CAL CIV. CODE § 56.06(b) (Deering 2022).

[180] ***Id.*** at 56.05(g), 56.06(b).

[181] CCPA Regulations, https://oag.ca.gov/privacy/ccpa/regs (last visited Mar. 6, 2022).

[182] Solow-Niederman, ***supra*** note 118, at 373.

[183] California Consumer Privacy Act, CAL. CIV. CODE § 1798.140(o)(1)(K) (Deering 2022).

Proposition 24, which expands various provisions in the law.[184] Proposition 24 adds the right to correct inaccurate personal information held by a business, expands the right to opt-out of data-sharing, and requires data collectors to provide specific notice when sensitive information is collected.[185] Companies found to be intentionally violating the CCPA may be fined up to $7500 per violation, whereas non-intentional violations can result in fines of no more than $2500 per violation.[186]

The CCPA is neither designed for nor adequate to address the privacy harms inflicted upon remote workers when their health data is collected. The CCPA applies to consumers, which the law defines as a "natural person who is a California resident."[187] Personal information is defined to explicitly include "professional or employment-related information."[188] However, the provisions only apply to businesses covered by the CCPA.[189] A company is covered by the CCPA if it does business in California and falls within one of three thresholds.[190] Furthermore, the law says that it does not apply to "personal information that is collected by a business about a natural person in the course of the natural person acting as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or contractor of that business to the extent that the natural person's information . . . ."[191]

Like BIPA, privacy intrusions under the CCPA depend in part on an employee's reasonable expectation of privacy, and therefore California caselaw interpreting this expectation is instructive as to the scope of privacy protections that remote workers can enjoy. In *Hernandez v. Hillsides*, the California Supreme Court considered an employer who had secretly videotaped employees in their closed-door office, where employees often changed, because the employer suspected someone, though neither of the plaintiffs, of using workplace computers to watch pornography.[192] The court said that "plaintiffs have not established, and cannot reasonably expect to establish, that the particular conduct of defendants that is challenged in this case was highly offensive and constituted an egregious violation of prevailing social norms."[193] This outcome is not encouraging for enhancing

[184] CCPA Regulations, *supra* note 181.

[185] *Prop 24 and CCPA*, IMMIX LAW GROUP (Jan. 27, 2021), https://immixlaw.com/prop-24-and-ccpa/.

[186] CAL. CIV. CODE § 1798.155(b).

[187] CAL. CIV. CODE § 1798.140(g) (2018).

[188] CAL. CIV. CODE § 1798.140(o)(1)(I).

[189] CAL. CIV. CODE §§ 1798.100 *et seq.*; *see also id.* § 1798.140(c).

[190] *Employee Data Under the California Consumer Privacy Act*, CLARIP, https://www.clarip.com/data-privacy/employee-data-ccpa/ (last visited Oct. 20, 2022); A California business is covered by the CCPA if it has annual gross revenues in excess of twenty-five million dollars; buys, receives, sells, or shares, for commercial purposes, the personal information of 50,000 or more consumers, households, or devices; or derives fifty percent or more of its annual revenues from selling consumers' personal information. CAL. CIV. CODE § 1798.140(c)(1)(A)—(B).

[191] CAL. CIV. CODE § 1798.145(h)(1)(A) (2018).

[192] Hernandez v. Hillsides, Inc., 47 Cal. 4th 272 (2009).

[193] *Id.* at 300–01.

privacy protection for remote workers, but the reasoning may be. Certainly, an employee would have a reasonable expectation of more privacy while working from home than in the office. Whether courts in California or elsewhere will recognize this distinct and novel expectation of privacy remains an open question.

In addition to California and Illinois, several other states have made progress in enacting privacy protections for workers.[194] State Attorneys General also play a major role in enforcing and expanding privacy protections.[195] Yet none of these goes further than California or Illinois in protecting remote workers' health data privacy.[196] Even California and Illinois, leaders in the United States in employee

[194] On November 8, 2021, New York Governor Kathy Hochul signed into law Senate Bill S2628, which requires employers to provide notice to their employees of any electronic monitoring they are subject to, including the use of radio or electromagnetic, photoelectronic or photo-optical systems. NY Senate, S.B. S2628, signed by Governor, introduced by Sen. Sanders; *See also* Lindsey Tonsager, Libbie Canter, Alexandra Scott, Jayne Ponder, & Frank Broomell, *Utah Legislature Passes Comprehensive Privacy Bill*, Inside Privacy, COVINGTON & BURLING (Mar. 4, 2022), https://www.insideprivacy.com/united-states/state-legislatures/utah-legislature-passes-comprehensive-privacy-bill/; Jake Holland, *Florida House Passes Consumer Privacy Bill With Right to Sue*, BLOOMBERG LAW (Mar. 2, 2022), https://www.bloomberglaw.com/product/privacy/bloomberglawnews/exp/ewogICAgImN0eHQiOiAiRE9DIiwKICAgICJpZCI6ICJYM1AzMkFKSzAwMDAwMD9yZXNvdXJjZV9pZD0wN2ZiZDI0YzMwYTljZGM4NWNhOTM4NDZmNzEyYWUzOCIsCiAgICAic2lnIjogInI2ZUNldmZSVHdJZnYxRXdTdHh6MHM3REd2ND0iLAogICAgInRpbWUiOiAiMTY0NjM0NDg5OSIsCiAgICAidXVpZCI6ICJcL05HXC9RbGw0eDZjY0JLRmwxZzZcL2x3PT1nZEM5d0hYeGZuYnA4QVFVcEFQU2VRPT0iLAogICAgInYiOiAiMSIKfQo=?isAlert=true&udvType=Alert; Jake Holland, *Wisconsin Assembly Passes Data Privacy Bill With Right to Cure*, BLOOMBERG LAW (Feb. 24, 20220), https://www.bloomberglaw.com/product/privacy/bloomberglawnews/exp/ewogICAgImN0eHQiOiAiRE9DIiwKICAgICJpZCI6ICJYREkxSzNPUzAwMDAwMD9yZXNvdXJjZV9pZD0wN2ZiZDI0YzMwYTljZGM4NWNhOTM4NDZmNzEyYWUzOCIsCiAgICAic2lnIjogInkwVHF6TE9XeEx4NWtYTFNla2cxbElhWENNUT0iLAogICAgInRpbWUiOiAiMTY0NTgyNjUxOSIsCiAgICAidXVpZCI6ICJBY1wvK2xBRWtCc2ZrVzBvdDV6Mnl4Zz09OFwvUldCdjNDdTU3QnpwZmprQndHYkE9PSIsCiAgICAidiI6ICIxIgp9Cg==?isAlert=true&udvType=Alert (Assembly Bill 957 was passed 59–77, giving consumers the right to know what personal data is being collected about them and ask for it to be corrected or deleted.).

[195] Danielle Citron, *The Privacy Policymaking of State Attorneys General*, 92 NOTRE DAME L. REV. 747, 749 (2016). The advocacy role of State officials was exemplified in Washington State, where the Washington Privacy Act failed in 2021 for the third year after lawmakers deadlocked over whether to include a private right of action, and after the Washington Solicitor General testified against the bill; Jake Holland, *2022 Privacy Legislation Success Viable as Three States Lead Way*, BLOOMBERG LAW (Jan. 3, 2022), https://www.bloomberglaw.com/product/privacy/bloomberglawnews/exp/ewogICAgImN0eHQiOiAiRE9DIiwKICAgICJpZCI6ICJYNDIyUEZJSzAwMDAwMD9yZXNvdXJjZV9pZD0wN2ZiZDI0YzMwYTljZGM4NWNhOTM4NDZmNzEyYWUzOCIsCiAgICAic2lnIjogIjVsNVVUcEpwZzFReldiTGk4cnlhOUpBaFBOZz0iLAogICAgInRpbWUiOiAiMTY0MTI0NzMxMCIsCiAgICAidXVpZCI6ICIwMFJSMzFEemZDQnlQdmRaN1MzUXFRPT1uZ2JQaFlmQzBBMmoraDQxcnVabXN3PT0iLAogICAgInYiOiAiMSIKfQo=?isAlert=true&udvType=Alert.

[196] Casey Leins, *States With the Strongest Online Privacy Protections*, U.S. NEWS (Oct. 23, 2019), https://www.usnews.com/news/best-states/articles/2019-10-23/states-with-the-strongest-online-privacy-laws.

data privacy, lack adequate protections for remote workers under surveillance by employers.

This Part has shown that existing privacy laws in the United States fail to protect remote workers subjected to surveillance. In the absence of a comprehensive federal privacy law, the privacy risks posed by remote worker surveillance of health data falls through the cracks. Even California and Illinois, recognized as national leaders in privacy protections, do not have legislation that adequately protects remote workers. These laws fall short both by failing to recognize the novel risks to remote workers, but also by overlooking the aggregate, population-level effects of health data collection. The next Part discusses various proposals for strengthening privacy protections for remote workers.

IV. RECOMMENDATIONS

Federal legislation would likely be the most enduring way to protect the privacy of remote workers. A federal law addressing employee privacy would provide uniformity, predictability, and broad protection to workers regardless of where they live. Federal legislation could also close the gaps between state laws and resolve conflicts of law that arise from efforts to apply state data privacy laws to workers in other states.[197] There are aspects of various proposed bills that would significantly advance privacy protections of remote workers.

The Uniform Law Commission ("ULC") in July 2021 unveiled a standardized data protection bill called the Uniform Personal Data Protection Act ("UPDPA").[198] The ULC is a group of lawyers, law professors, judges, and legislators appointed by state governments to provide uniformity across state laws.[199] Introduced in legislatures in Washington, D.C., Nebraska, and Oklahoma, the UPDPA would significantly increase privacy protections in just about any state where it is enacted, and even more so at the federal level.[200] However, the Act does not adequately address the collection of health data from remote workers.[201] Perhaps the most

---

[197] For general discussion of conflicts of law in cyberspace, *see* Joanna Zakalik, *Law Without Borders in Cyberspace*, 43 WAYNE L. REV. 101, 113—14 (1996); Jack Goldsmith, *The Internet and the Abiding Significance of Territorial Sovereignty*, 5 IND. J. GLOBAL LEGAL STUD. 475 (1998); David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 45 STAN. L. REV. 1367 (1996).

[198] ULC, *Uniform Personal Data Protection Act*, UNIFORM LAW COMMISSION (July 11, 2021), https://www.uniformlaws.org/committees/community-home?CommunityKey=28443329-e343-4cbc-8c72-60b12fd18477.

[199] ULC, *About Us*, UNIFORM LAW COMMISSION, https://www.uniformlaws.org/aboutulc/overview (last visited Mar. 2, 2022). The ULC is most well-known for its work with the American Law Institute to create the Uniform Commercial Code. ULC, *Uniform Commercial Code*, ULC, https://www.uniformlaws.org/acts/ucc (last visited Mar. 2, 2022).

[200] ULC, *Personal Data Protection Act*, *supra* note 198.

[201] Section 7(a) of UPDPA says that a data controller or processor may engage in a "compatible data practice without the data subject's consent." A "compatible data practice" includes that which "advances the economic, health, or other interests of the data subject."

promising aspect of UPDPA is how it understands privacy harms. Under the Act, a data controller may not engage in processing personal data if it is likely to subject a data subject to specific and significant (A) financial, physical or reputational harm; (B) embarrassment, ridicule, intimidation, or harassment; or (C) physical or other intrusion on solitude or seclusion if the intrusion would be highly offensive to a reasonable person.[202] Whereas harms (A) and (B) are commonly recognized by courts, harm (C) is a significant and novel way to characterize a prohibited data practice.[203]

Privacy scholars Ajunwa et al. propose an "Employee Privacy Protection Act" ("EPPA") that would expressly prohibit surveillance outside the workplace in terms of physical location privacy and activity privacy.[204] They note that a restriction of such surveillance to "work-related purposes" would not suffice because employers could plausibly claim that much of the information they collect is work-related.[205] Yet this same reasoning cuts against the effectiveness of this hypothetical EPPA because for remote workers, all work occurs outside the workplace.

The Data Elimination and Limiting Extensive Tracking and Exchange Act ("DELETE Act") is a bipartisan bill introduced in the Senate that would require data brokers to abide by opt-out requests and register with an FTC data-broker dashboard.[206] Mandating registration and disclosure of data collection practices would be valuable, particularly since a majority of remote employee surveillance technologies are "silent," meaning the employees do not even know they are being monitored.[207] However, none of the three bills mentioned above specifically cover remote worker surveillance.

Building on these proposals and the deficiencies of state and federal laws described in Part III, I propose legislation that includes elements missing from these efforts. This legislation should have several features. First, it should at the very least ban silent or invisible methods of monitoring workers at home. The invasiveness and risks of constant surveillance as a default for all employees outweigh the productivity-tracking justifications. Second, Congress should amend HIPAA to include manufacturers and developers of health-tracking technology.[208] This

---

UPDPA §7(a)(6). This provision could be used to justify collecting the health data of remote workers to the extent the collection is justified as promoting wellness among employees.

[202] UPDPA §9, ULC, https://www.uniformlaws.org/viewdocument/final-act?CommunityKey=28443329-e343-4cbc-8c72-60b12fd18477&tab=librarydocuments.

[203] Danielle Citron & Daniel Solove, *Privacy Harms*, 102 B. U. L. REV. 793 (2022).

[204] Ajunwa et al., *supra* note 4 at 140.

[205] *Id.*

[206] Press Release, Sen. Bill Cassidy, Cassidy, Ossoff, Trahan Introduce Bill to Protect Americans' Online Privacy and Data (Feb. 9, 2022), https://www.cassidy.senate.gov/newsroom/press-releases/cassidy-ossoff-trahan-introduce-bill-to-protect-americans-online-privacy-and-data.

[207] Cyphers & Gullo, *supra* note 3.

[208] Brown, *Fitbit Fault Line*, *supra* note 7, at *46–47.

amendment should also extend HIPAA protections to the aggregated analysis of and inferences drawn from health data.[209]

Another important element to include is a private right of action, which is included in BIPA and CCPA in cases of data breaches. A private right of action allows individuals to pursue claims against companies or employers themselves, rather than relying on a data commissioner or state Attorney General to enforce the law.[210] However, standing doctrine remains in flux, especially after ***TransUnion v. Ramirez.***[211] There, the Supreme Court held that plaintiffs did not suffer a concrete harm by having their credit reports falsely flagged as appearing in the Office of Foreign Assets Control ("OFAC") list of terrorists, drug traffickers, and other serious criminals, unless they proved that the data was made available to third-parties without consent.[212] In order to bring a private right of action in federal court, a plaintiff must establish standing, which the Supreme Court has interpreted to exclude many privacy violations.[213] Yet given the sensitive nature of health data, courts may recognize an injury in fact where an employee's health data is collected or analyzed without prior consent.

Another important legal tool is auditing algorithms for fair predictions. This is a tricky business, given the sophisticated technology involved and trade secret law that can take precedence over individuals' legal rights.[214] However, there are various proposals for doing so that would give individuals the right to contest the predictions that are made about them. Sandra Wachter, for instance, argues that the European Union's General Data Protection Regulation ("GDPR") does not, but should, include a right to reasonable inferences such that individuals could access and correct the predictions that algorithms make about their preferences, lifestyle, or other material algorithmic output.[215] This argument may not be obviously applicable given that the United States does not have a GDPR, but a right to reasonable inferences is nonetheless an important principle for States to consider as they propose and enact privacy laws. Also, Wachter's argument could be invoked to fashion a data transparency law, applicable to remote worker's health data privacy.

---

[209] Newman & Kreick, *supra* note 107.

[210] Citron & Solove, *supra* note 203, at 811.

[211] TransUnion v. Ramirez, 141 S. Ct. 2190, 2200 (2021).

[212] *Id.*

[213] *See* Seth Kreimer, *"Spooky Action at a Distance": Intangible Injury in Fact in the Information Age*, 18 J. CONST. L. 745 (2016).

[214] Rebecca Wexler, *Life, Liberty, and Trade Secrets*, 70 STAN. L. REV. 1343 (2018) ("A death penalty defendant in Pennsylvania state court was denied access to the source code for a forensic software program that generated the critical evidence against him; the program's commercial vendor argued that the code is a trade secret.").

[215] Sandra Wachter & Brent Mittelstadt, *A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI*, 2019 COLUM. BUS. L. REV. 494 (2019).

V. CONCLUSION

Rampant data collection, particularly of health data, poses significant risks of intrusions on the privacy of remote workers. From inducing stress and anxiety to facilitating discrimination, this surveillance risks causing great harm. Absent comprehensive data privacy legislation, the patchwork of federal law and state laws of varying scope does not adequately address this harm. Although several proposals have been brought forward to ameliorate some aspects of this problem, such as improved notice-and-consent provisions or amendments to covered entities, much of data privacy law thus far has underemphasized the network-level effects of data collection and analysis.

Looking ahead, these issues will only grow in magnitude. As more money and development goes into virtual reality and the "metaverse," questions about how to regulate the collection of sensitive data of remote employees will only become more salient.[216] Further advances in surveillance technology will give employers even more control over their employees, and the increased prevalence of flexible working arrangements will continue to raise the stakes. Indeed, the stakes are immense. Without public intervention, remote workers will likely face ever more constant and detailed surveillance, with little about their private lives outside of their employers' scrutiny. Such an outcome would be detrimental to remote workers, in-person workers, and anyone concerned about privacy. In order to prevent a panoptic future, in which employers may surveil any worker anywhere at any time, federal data privacy laws must curb the collection and use of intimate health information.

[216] *See* Mark Lemley & Eugene Volokh, *Law, Virtual Reality, and Augmented Reality*, 166 PENN. L. REV. 1051 (2018).