Limitless Worker Surveillance

Ifeoma Ajunwa,* Kate Crawford,** and Jason Schultz***

From the Pinkerton private detectives of the 1850s, to the closed-circuit cameras and email monitoring of the 1990s, to new apps that quantify the productivity of workers, and to the collection of health data as part of workplace wellness programs, American employers have increasingly sought to track the activities of their employees. Starting with Taylorism and Fordism, American workers have become accustomed to heightened levels of monitoring that have only been mitigated by the legal counterweight of organized unions and labor laws. Thus, along with economic and technological limits, the law has always been presumed as a constraint on these surveillance activities. Recently, technological advancements in several fields—big data analytics, communications capture, mobile device design, DNA testing, and biometrics—have dramatically expanded capacities for worker surveillance both on and off the job. While the cost of many forms of surveillance has dropped significantly, new technologies make the surveillance of workers even more convenient and accessible, and labor unions have become much less powerful in advocating for workers. The American worker must now contend with an all-seeing Argus Panoptes built from technology that allows for the trawling of employee data from the Internet and the employer collection of productivity data and health data, with the ostensible consent of the worker. This raises the question of whether the law still remains a meaningful avenue to delineate boundaries for worker surveillance.

DOI: https://dx.doi.org/10.15779/Z38BR8MF94

* Fellow, Berkman Klein Center at Harvard University; Assistant Professor, Cornell Industrial and Labor Relations (ILR) School; Associate Faculty, Cornell Law School.

** Visiting Professor, MIT Center for Civic Media; Principal Researcher, Microsoft Research; Senior Fellow, NYU Information Law Institute.

*** Professor of Clinical Law, NYU School of Law. First, the authors wish to thank the editors of the *California Law Review* for their capable and fastidious editing assistance. The authors also wish to thank the attendees of the 2016 Privacy Law Scholars Conference at George Washington University and the 2016 Law and Society Association Conference in New Orleans. Special thanks to Professors Andrew G. Ferguson, Pauline Kim, and Brett Frischmann. We also thank Microsoft Research New York for funding Professor Ajunwa's initial research on these topics.

In this Article, we start from the normative viewpoint that the right to privacy is not an economic good that may be exchanged for the opportunity for employment. We then examine the effectiveness of the law as a check on intrusive worker surveillance, given recent technological innovations. In particular, we focus on two popular trends in worker tracking—productivity apps and worker wellness programs—to argue that current legal constraints are insufficient and may leave American workers at the mercy of 24/7 employer monitoring. We consider three possible approaches to remedying this deficiency of the law: (1) a comprehensive omnibus federal information privacy law, similar to approaches taken in the European Union, which would protect all individual privacy to various degrees regardless of whether or not one is at work or elsewhere and without regard to the sensitivity of the data at issue; (2) a narrower, sector-specific Employee Privacy Protection Act (EPPA), which would focus on prohibiting specific workplace surveillance practices that extend outside of work-related locations or activities; and (3) an even narrower sector and sensitivity-specific Employee Health Information Privacy Act (EHIPA), which would protect the most sensitive type of employee data, especially those that could arguably fall outside of the Health Insurance Portability and Accountability Act's (HIPAA) jurisdiction, such as wellness and other data related to health and one's personhood.

INTRODUCTION

When newsroom workers at the Daily Telegraph arrived at their workplace on January 11, 2016, they discovered an unusual new piece of office equipment—a small, black rectangular box labeled "OccupEye"—attached to the underside of every desk.[1] Management initially justified the equipment as an effort to gather data on energy efficiency and promote environmental sustainability. But, unannounced by management, the devices were in fact part of a system of "automated workspace utilisation analysis" designed to track the motion and heat of individual employees and provide detailed metrics on worker attendance.[2] Employees' suspicion that OccupEye's true purpose was mass surveillance of worker performance quickly led to public outrage, union pressure, and, ultimately, its ejection from the Telegraph building.[3] Although these workers were successfully able to shame their employer into reversing its plan, the public discourse surrounding the incident failed to include any suggestion that the Telegraph's actions had, in any way, violated the law.

Ubiquitous employer surveillance of workers has a long and rich history as a defining characteristic of workplace power dynamics, including the de facto abrogation of almost any substantive legal restraints on its use. This history can be traced through many pivotal points including massive efforts

1. Jim Waterson, *Daily Telegraph Installs Workplace Monitors on Journalists' Desks*, BUZZFEED NEWS (Jan. 11, 2016), http://www.buzzfeed.com/jimwaterson/telegraph-workplace-sensors [https://perma.cc/CBE9-52SW].

2. *Id.*

3. *Id.* (noting that once discovered, Telegraph employees immediately saw the monitoring devices as surveillance apparatuses, with one commenting: "Never before has taking a shit on company time felt so rebellious.").

through warfare, slavery, globalization, and other forms of colonialism[4] used to control and exploit workers. Yet, the role of surveillance innovation itself on the workplace and the corresponding weakness of legal protections for those subjected to it have been less examined. As an example, consider the story of Allan Pinkerton. In 1855, businesses were increasingly struggling with the desire for greater control over their employees, both inside and outside work hours and locations.[5] Pinkerton had consulted with numerous commercial interests, including six Midwestern railroad companies, and determined that a venture offering a solution to this problem was viable. To capitalize on this market, Pinkerton and his attorney, Edward Rucker, formed the North-Western Police Agency, later known as the Pinkerton National Detective Agency. With the incorporation of the Agency, a new form of worker surveillance came into being. "The Pinkertons" (as the agents were called) served a variety of roles for employers—infiltrating and busting unions, enforcing company rules, and monitoring workers deemed to be a threat to the interests of employers.[6] This form of worker surveillance was largely unregulated until Congress passed the Anti-Pinkerton Act of 1893, which limited the federal government's ability to hire the Pinkertons or any similar organization but left private employers' use of such agencies unchecked.[7]

Today, despite the accomplishments of the Pinkertons and their successors, surveillance innovations now enable employers to rely less on human agents to accomplish employee surveillance.[8] Rather, technologies, both digital and otherwise, have become the primary tools of employee monitoring.[9] Indeed, the technological monitoring of employees by employers has moved in lockstep with the advancement of technological capacities. Beginning with punch-card systems, advancing to closed-circuit video cameras and geo-locating systems, workplace surveillance has become a fact of life for the American worker. What is novel, and of real concern to privacy law, is that rapid technological advancements and diminishing costs now mean employee

4. *See, e.g.*, SIMONE BROWN, DARK MATTERS: SURVEILLANCE OF BLACKNESS 12–17 (2015).

5. FRANK MORN, THE EYE THAT NEVER SLEEPS: A HISTORY OF THE PINKERTON NATIONAL DETECTIVE AGENCY 18 (1982).

6. *Id.*

7. *See* Pub. L. No. 89-554, 80 Stat. 416. (1966) (codified at 5 U.S.C. § 3108) ("An individual employed by the Pinkerton Detective Agency, or similar organization, may not be employed by the Government of the United States or the government of the District of Columbia.").

8. Although some organizational theorists make a distinction between "monitoring" (viewed as more benign) and "surveillance" (viewed as less benign), many others do not, as monitoring and surveillance involve the same actions. Whether those actions are benign or not is both a matter of interpretation and of effect. Throughout this Article, we use "monitoring" and "surveillance" interchangeably. *See* Philip E. Agre, *Surveillance and Capture: Two Models of Privacy*, 10 INFO. SOC'Y 101, 101 (1994). *But see* Graham Sewell & James R. Barker, *Coercion Versus Care: Using Irony to Make Sense of Organizational Surveillance*, 31 ACAD. MGMT. REV. 934 (2006).

9. Laurie Thomas Lee, *Watch Your Email! Employee E-Mail Monitoring and Privacy Law in the Age of the "Electronic Sweatshop,"* 28 J. MARSHALL L. REV. 139 (1994).

surveillance occurs both inside and outside the workplace—bleeding into the private lives of employees. For example, in 2015, a woman was fired from her job after she deleted an employee tracking app from her phone that recorded her movements at all times, even when she was no longer at work and had turned off the app.[10] In another recent case, characterized as "the mystery of the devious defecator," U.S. District Court Judge Amy Totenberg ordered an employer to pay two of its employees $2.2 million in damages for demanding that the employees provide DNA samples for genetic testing after feces were discovered in the workplace.[11]

Employers have also altered their investments in certain technologies and practices in light of constraining legal frameworks. As a result, there has been a shift in focus from collecting personally-identifying information, such as health records, to wholly acquiring unprotected and largely unregulated proxies and metadata, such as wellness information, search queries, social media activity, and outputs of predictive "big data" analytics.[12]

Thus, we situate this Article within the scholarly literature that contemplates how workers experience surveillance in the workplace.[13] We observe that surveillance in the workplace has mostly moved away from an authoritarian regime, wherein workers were subjected to discreet and predictable surveillance at the hands of employers. Rather, it now evinces an ostensibly participatory character, wherein workers are expected to aid employer surveillance by using productivity applications and wellness programs that employers proffer as beneficial to the workers' interests. Furthermore, as noted by privacy scholar Julie Cohen, this participatory turn to surveillance is championed as a requisite for innovation and progress; such rhetoric seeks to silence legal objections as to the extent and invasiveness of current employee surveillance tactics.[14]

Compounding the shift to participatory surveillance, recent advancements in technology have made the intrusive surveillance of workers much more achievable and economical. However, there have been no sweeping legal changes to address these new technological advancements in surveillance. While some states, like California, have implemented laws that protect its workers, other states, like Massachusetts, have comparatively low protections

---

10. David Kravets, *Worker Fired for Disabling GPS App that Tracked Her 24 Hours a Day*, ARS TECHNICA (May 11, 2015, 9:41 AM), http://arstechnica.com/tech-policy/2015/05/worker-fired-for-disabling-gps-app-that-tracked-her-24-hours-a-day [https://perma.cc/476P-L94B].

11. Daniel Wiessner, *Georgia Workers Win $2.2 Million in 'Devious Defecator' Case*, REUTERS (June 23, 2015, 11:41 AM), http://www.reuters.com/article/2015/06/23/us-verdict-dna-defecator-idUSKBN0P31TP20150623 [https://perma.cc/G356-WR3M].

12. *See* Kate Crawford & Jason Schultz, *Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms*, 55 B.C. L. REV. 93, 95 (2014) (noting "predictive privacy harms").

13. *See* Kirstie Ball, *Workplace Surveillance: An Overview*, 51 LAB. HIST. 87, 87 (2010); *see also* Julie E. Cohen, *The Surveillance-Innovation Complex: The Irony of the Participatory Turn*, *in* THE PARTICIPATORY CONDITION IN THE DIGITAL AGE 207–26 (Darin Barney et al. eds., 2016).

14. Cohen, *supra* note 13, at 213.

for worker surveillance. A major conceit of this Article is that we cannot depend on each individual state's legislature to accomplish piecemeal the work of protecting workers.

We hold the normative view that the protection of workers' privacy is a civil rights issue: both for the protection of human dignity rights and because privacy invasions can serve as vehicles for unlawful discrimination. Federal law can protect against discrimination in a way that state law and the market cannot. History has shown that economic pressures are an unreliable regulator for the preservation of the civil rights of those with comparatively lower economic power. That is, we cannot simply look to the market to curtail abuses of power regarding worker surveillance. Instead, we should look to federal law to rein in such imbalances. For instance, worker protections such as the minimum wage and workplace safety requirements are federally mandated for the protection of all workers, regardless of bargaining power or lack thereof.

To capture the new privacy and discrimination issues arising in the context of workplace surveillance, Part I provides a historical overview of workplace surveillance, and Part II follows with a discussion of the extant spectrum of legal limitations on the practice. Then, Part III transitions into a focused discussion on two arenas of recent expansion: 1) workplace wellness programs and 2) work productivity applications (apps). Part IV concludes by proposing solutions to address those concerns.

I.
WORKER SURVEILLANCE: A BRIEF HISTORY

In this Section, we discuss some of the history of and ethical debate on the limitations on worker surveillance, starting from the 1980s and leading up to the present. We focus on technological limits, such as the constraints on unremitting recording of the worker's movements and actions, and we describe the emerging technologies that have made these limits largely obsolete. Additionally, we evaluate the effects of the changing nature of work on the employer's motivation to more closely surveil its workers.

A. Technological and Economic Limits on Worker Surveillance

The effects of electronic surveillance in the workplace have been debated for decades but came to a significant crossroads in the 1980s, when the United States Office of Technology Assessment (OTA) published *The Electronic Supervisor: New Technologies, New Tensions*, a report that synthesized political, economic, sociological, and psychological perspectives on workplace surveillance.[15] The report found that advances in computer monitoring had raised questions about fairness and privacy in regard to employer surveillance of employees. The report generally noted that because of declines in

15. Ball, *supra* note 13, at 88.

unionization, employees had little power to object to what they considered "unfair or abusive monitoring."[16] Furthermore, although some employees reported feeling "stress" as a result of constant monitoring, the report underscored that there was no legal requirement that employer monitoring be fair.[17]

While the OTA report found that unionization could provide some protections for workers against invasive worker surveillance, such protection would have been limited because at the time the report was issued "[l]ess than 20 percent of the office work force [was] unionized, and even where unions [were] involved, their effectiveness ha[d] been limited because technology choice and productivity measurement [were] often considered 'management rights' under the contract."[18] By 2016, the number of American workers belonging to a union had fallen even further, to just 11.1 percent.[19]

In the following two Sections, we discuss the former technological and economic limits to worker surveillance and explain how technological advancements that make worker monitoring straightforward and inexpensive have dissolved these limits.

1. A Historic Example of the Limits of Employee Surveillance

As early monitoring of employees had to be conducted by human supervisors, such surveillance was hindered by both economic and technological limits. For example, in the early twentieth century, Henry Ford stalked the factory floor with a stopwatch, timing his workers' motions in a push for higher efficiency.[20] He also hired private investigators to spy on his employees' lives away from the factory to discover personal problems that could interfere with their work.[21] As some have noted: "the irony was that in trying to make over his workers in terms of 'Americanization' and 'Fordliness,' Ford created a form of Big Brotherism that was closer to the totalitarian model."[22] Ford charged his Sociological Department with surveilling the

16. U.S. CONG., OFFICE OF TECH. ASSESSMENT, OTA-CIT-333, THE ELECTRONIC SUPERVISOR: NEW TECHNOLOGY, NEW TENSIONS 1 (1987), http://files.eric.ed.gov/fulltext/ED299406.pdf; *see also* https://www.princeton.edu/~ota/disk2/1987/8708/870803.PDF [https://perma.cc/V3QE-2TNT] (*The Electronic Supervisor* report summary).

17. *Id.*

18. *Id.*

19. U.S. DEP'T OF LABOR, BUREAU OF LABOR STATISTICS, USDL-16-0158, UNION MEMBERS—2015 (2016), http://www.bls.gov/news.release/pdf/union2.pdf [https://perma.cc/XPC8-TZJT].

20. RICHARD SNOW, I INVENTED THE MODERN AGE: THE RISE OF HENRY FORD 204–05 (2013).

21. Ted Morgan, *Intrigue and Tyranny in Motor City*, N.Y. TIMES (July 13, 1986), http://www.nytimes.com/1986/07/13/books/intrigue-and-tyranny-in-motor-city.html [https://perma.cc/SAW4-PFC3] (reviewing ROBERT LACEY, FORD: THE MEN AND THE MACHINE (1986)).

22. Morgan, *supra* note 21.

private lives of his employees, and the detectives of the department went into employees' homes to question them about out of factory activities.[23] "It seems amazing that people would tolerate such interrogation, but their jobs depended on it."[24] Similarly, Walmart has been criticized for the union-busting strategies it has had in place since its inception in the 1960s; indeed, employees have expressed fear that dissenting to such strategies might put their jobs at risk.[25]

Yet, it was not humanly possible to maintain 24/7 monitoring of workers without the aid of technologies that became ubiquitous in the twenty-first century. Neither Ford nor his investigators could be in all places at once. Even with the help of the Sociological Department, Ford was constrained by what his human investigators could observe and record. Ford did not have access, for example, to remote technologies that could surveil his workers after hours, nor to the highly accessible genetic testing that was developed in the 1990s, which can now detect whether a worker has a higher than usual propensity for a particular disease.[26]

2. The Rapid Erosion of Technological and Economic Limits

Punch clocks have given way to thumb scans,[27] key cards may soon give way to Radio Frequency Identity (RFID) tags,[28] and internet browser histories are often scrutinized closely. Employers log keystrokes, interested in capturing not only when their employees use private services like Gmail, Facebook, and

---

23. *Id.*

24. *Id.*

25. Susan Berfield, *How Walmart Keeps an Eye on Its Massive Workforce*, BLOOMBERG (Nov. 24, 2015), http://www.bloomberg.com/features/2015-walmart-union-surveillance [https://perma.cc/FK6H-R5FR].

26. Since the 1990s, the technology for genetic testing has developed rapidly and there is now a proliferation of direct-to-consumer genetic testing services that any worker might use for detecting their propensity for disease. *See, e.g.*, Elizabeth Murphy, *Inside 23andMe Founder Anne Wojcicki's $99 DNA Revolution*, FAST COMPANY (Oct. 14, 2013), https://www.fastcompany.com/3018598/for-99-this-ceo-can-tell-you-what-might-kill-you-inside-23andme-founder-anne-wojcickis-dna-r [https://perma.cc/2E5B-BRN3].

27. Esther Kaplan, *The Spy Who Fired Me: The Human Costs of Workplace Monitoring*, HARPER'S MAG. 31 (Mar. 2015), http://www.populardemocracy.org/sites/default/files/HarpersMagazine-2015-03-0085373.pdf [https://perma.cc/5RC3-HK8A].

28. Radio Frequency Identity (RFID) is a generic term for technologies that use radio waves to automatically identify people or objects. There are several methods of identification, but the most common is to store a serial number that identifies a person or object, and perhaps other information, on a microchip. The microchip may be embedded under the skin. *See Frequently Asked Questions*, RFID J., https://www.rfidjournal.com/site/faqs [https://perma.cc/49N9-XNSL] (last visited Feb. 28, 2017). In 2006, CityWatcher became the first employer to inject RFID tags into the triceps of two of its employees in lieu of keycards to access areas where sensitive information is stored. *See Two U.S. Employees Injected with RFID Microchips at Company Request*, SPYCHIPS.COM (Feb. 9, 2006), http://www.spychips.com/press-releases/us-employees-verichipped.html [https://perma.cc/X8LF-LB92].

Twitter, but also what they publish there.[29] According to "a survey from the American Management Association, at least 66 percent of U.S. companies monitor their employees' internet use, 45 percent log keystrokes, and 43 percent track employee emails."[30] Employer-provided cellphones, an increasingly common piece of worker equipment, now offer employers the ability to pinpoint a worker's precise location through GPS.[31] As summed up by Ellen Bayer of the American Management Association: "Privacy in today's workplace is largely illusory."[32] Worse, many workers may be unaware of the extent to which they are being tracked by their employer; only two states, Delaware and Connecticut, mandate that employers inform their employees of electronic tracking.[33]

The rapid erosion of technological and economic constraints on employee monitoring has magnified the invasiveness of surveillance activities. Now, with the advent of almost ubiquitous network records, browser history retention, phone apps, electronic sensors, wearable fitness trackers, thermal sensors, and facial recognition systems, there truly could be limitless worker surveillance.[34]

It is important to note that employers justify these new privacy invasions on the basis that collection of such data serves the employer's business interest in improving efficiency and innovation. For example, Boston-based analytics firm Sociometric Solutions has developed employee ID badges fitted with a microphone, location sensor, and accelerometer, and it is testing them on twenty companies.[35] Sociometric Solutions claims that it doesn't record conversations or provide employers with individuals' data.[36] Instead, Sociometric's stated goal is to discover how employee interactions affect the employee performance.[37] But the unspoken caveat is that there is no legal barrier to the employer's acquisition of the raw data, which could be used for any purpose the employer wishes.

Take, as another example, UPS's surveillance program. In 2009, UPS fitted its delivery trucks with about two hundred sensors that track everything from driving speeds to stop times.[38] This allowed the firm to find out which drivers were taking unauthorized breaks and to determine how many deliveries

---

29. *The Rise of Workplace Spying*, WEEK (July 5, 2015), http://theweek.com/articles/564263/rise-workplace-spying [https://perma.cc/NKP9-VSJZ].

30. *Id.*

31. *Id.*

32. *Id.*

33. Kaplan, *supra* note 27.

34. It is important to note that prior to the technological advances we detail here, other scholars have grappled with the public policy aspects of worker privacy. *See, e.g.*, Pauline T. Kim, *Privacy Rights, Public Policy, and the Employment Relationship*, 57 OHIO ST. L.J. 671, 671–730 (1996).

35. *The Rise of Workplace Spying*, *supra* note 29.

36. *Id.*

37. *Id.*

38. Kaplan, *supra* note 27.

could be squeezed into one day.[39] Within four years, the company was handling 1.4 million additional packages a day with one thousand fewer drivers.[40] Similarly, Amazon, perhaps the largest retailer in America, requires their workers to carry electronic tablets that record both their speed and efficiency as the workers retrieve merchandise to fulfill orders by online shoppers; and in some hospitals, nurses now wear electronic badges that track how often the nurses wash their hands.[41]

But even as employers tout the efficiency gains from the surveillance of workers, what they leave unsaid is the cost to workers themselves. The demand to meet electronically monitored goals means that workers take risks and push themselves physically in ways that result in more injuries.[42] While it is well established that lack of transparency and adequate monitoring can result in organizational deviance and misconduct,[43] the converse is also true. Too much monitoring creates stress, fear, and incentives to "beat the system." In the case of UPS workers, the "mental whip" of the constant telematics system's monitoring means that many workers resort to breaking safety rules that put themselves and others in danger.[44] Sociologist Karen Levy also found in her ethnography of long-distance truck drivers that there were negative effects to the constant electronic monitoring of those workers, resulting in pressure for the worker to not take mandated breaks[45] and to continue working even when

39. *Id.*

40. *Id.*

41. *The Rise of Workplace Spying*, *supra* note 29.

42. Union organizers have highlighted the dark side of constant electronic surveillance, which drives workers to extreme productivity and results in adverse physical effects. "'If you go to one of these UPS facilities at shift-change time, you'd think you were at a football game, the way people are limping, bent over, with shoulder injuries, neck injuries, knee injuries,' said David Levin, an organizer with Teamsters for a Democratic Union, a reform caucus within the Teamsters. 'It's fifteen years of rushing, rushing, rushing, working when you're exhausted, working those long days, running up and down stairs with boxes.'" Kaplan, *supra* note 27, at 31.

43. *See* Ifeoma Ajunwa, *"Bad Barrels": An Organizational-Based Analysis of the Human Rights Abuses at Abu Ghraib Prison*, 17 U. PA. J.L. & SOC. CHANGE 75, (2014) (explaining that organizational secrecy and lack of external monitoring can be contributing factors to the organizational misconduct and deviant acts at any organization).

44. "A UPS spokesperson told me that telematics has improved safety overall and lifted seat-belt compliance to an 'almost perfect' 98.8 percent. But UPS drivers tell a different story. One wrote on an online forum about a new hire who was beating his quota by an hour and a half to two hours every day. 'This guy has literally told me he will buckle the seat belt behind him and not wear it,' he wrote, saying the driver also has high backing speeds, an 'absurd amount of bulkhead door events'—driving with the back door open—and many misdelivered packages. 'People get intimidated and they work faster,' Rose told me. 'It's like when they whip animals. But this is a mental whip.'" Kaplan, *supra* note 27, at 31.

45. "Even when drivers are off-duty, employers can see where they are, and can contact them using systems' communication functions—which sometimes lack a 'mute' function for drivers to silence employer attempts at communication, even during sleep breaks." Karen E.C. Levy, *The Contexts of Control: Information, Power, and Truck-Driving Work*, 31 INFO. SOC'Y 160, 169 (2015).

sleep was necessary.[46] There is also the question of whether invasive employee surveillance will ultimately lower employee morale and result in higher employee turnover.[47]

Although we have focused on the ways that employers present electronic monitoring itself as a tool for increasing productivity, we must also remain cognizant of the fact that "productivity" has now extended so far as to try and capture more subjective attributes of workers. The figure below shows that worker surveillance is now so pervasive that it goes beyond merely monitoring productivity in the workplace; rather, it seeks to discover the individual behaviors and personal characteristics of workers.

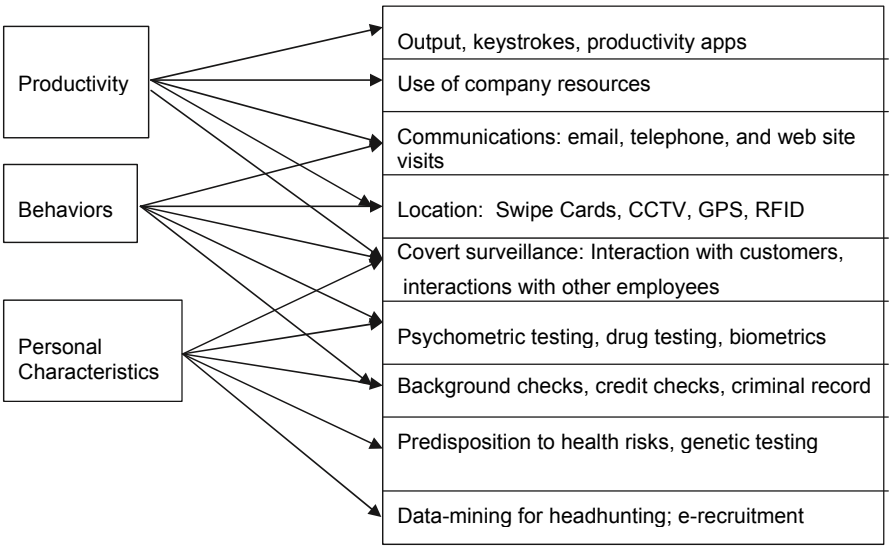

Figure 1: Adapted from Ball, K. (2010). Workplace Surveillance: An Overview

B. The Changing Nature of Work and Its Effects

The changing nature of work in America—in particular, the increase in the number of employees who work remotely and the increased use of "contract" or "freelance" workers[48]—is a sociological seismic shift that has

46. "As another driver put it: 'You, as a professional, you know when your body is tired. You know when your mind is fatigued. You know when you need to stop and rest. That dispatcher doesn't know. And by God, that electronic device certainly does not know.'" *Id.* at 170.

47. Conor Dougherty & Quentin Hardy, *Managers Turn to Computer Games, Aiming for More Efficient Employees*, N.Y. TIMES (Mar. 15, 2015), http://www.nytimes.com/2015/03/16/technology/managers-turn-to-computer-games-aiming-for-more-efficient-employees.html [https://perma.cc/BB9P-4FNB].

48. According to Business Dictionary: "Working on a contract basis for a variety of companies, as opposed to working as an employee for a single company." *Freelance*, BUS.

affected both the employer and employee roles. What these new developments signify is that the employer now has even more incentive for intrusive surveillance of its workers, as workers are less likely to be bounded within a physical workplace and there is less opportunity to develop a relationship of trust within a traditional employer-employee relationship.

Statistics show that working remotely rose "79 percent between 2005 and 2012 and now telecommuters make up 2.6 percent of the American work force, or 3.2 million workers, according to statistics from the American Community Survey."[49] In fact, the percentage of telecommuters that make up the workforce would reveal itself to be even larger if one "include[s] the self-employed; those whose work has to be done outside an office, such as taxi drivers, plumbers, truckers and construction workers; companies where everyone works remotely, so there is no brick-and-mortar office; and those who work at home one day or less a week."[50] With all those workers accounted for, "the number of Americans who work remotely would reach as high as 30 percent."[51] A larger number of workers are also now expected to be on call 24/7.[52]

Additionally, more workers are now considered "contract" or "freelance" workers than in the past. In 2014, Forbes magazine found that one in three American workers was a freelance worker.[53] To surveil freelance workers, companies are employing strategies such as "taking photos of workers' computer screens at random, counting keystrokes and mouse clicks and snapping photos of [the workers] at their computers."[54] Some employers even go as far as deploying technology that will "instantaneously detect anger, raised voices or children crying in the background on workers' home-office calls."[55] Monitoring tools are built into freelance work websites like Upwork (formerly

---

DICTIONARY, http://www.businessdictionary.com/definition/freelance.html [https://perma.cc/G7VL-CLHP] (last visited Feb. 28, 2017).

49. Alina Tugend, *It's Unclearly Defined, but Telecommuting Is Fast on the Rise*, N.Y. TIMES (Mar. 7, 2014), http://www.nytimes.com/2014/03/08/your-money/when-working-in-your-pajamas-is-more-productive.html [https://perma.cc/58SE-JXNZ].

50. *Id.*

51. *Id.*

52. Ilya Marritz, *In New Economy, Minimum-Wage Workers Are Always on Call*, WNYC (Nov. 21, 2013), http://www.wnyc.org/story/new-economy-many-employers-expect-open-availability [https://perma.cc/67F7-EXLB]; *see also* Herd Weisbaum, *How 'On-Call' Hours Are Hurting Part-Time Workers*, CNBC (Dec. 5, 2013 6:00 AM), http://www.cnbc.com/2013/12/04/how-on-call-hours-are-hurting-part-time-workers.html [https://perma.cc/ZCZ5-26WV] (the blog maintained by the UpWork administration mentions this practice).

53. Laura Shin, *1 in 3 American Workers Freelances. But Is the Phenomenon Growing?*, FORBES (Sept. 8, 2014, 12:00 AM), http://www.forbes.com/sites/laurashin/2014/09/08/1-in-3-american-workers-freelances-but-is-the-phenomenon-growing [https://perma.cc/9FK3-M7SY].

54. Sue Shellenbarger, *Work at Home? Your Employer May Be Watching*, WALL ST. J., (July 30, 2008, 11:59 PM), http://www.wsj.com/articles/SB121737022605394845 [https://perma.cc/HU36-HUGQ].

55. *Id.*

oDesk[56]); the Upwork worker monitoring system "takes random snapshots of workers' computer screens six times an hour, records keystrokes and mouse clicks and takes optional Web cam photos of freelancers at work."[57] The freelance workers are available for hire by anyone and, once hired, their clients have the capacity to log into the system at any time to check whether their contractors are working.[58] The monitoring is not covert or unobtrusive, as the freelance workers are alerted by "a small computer-screen icon [that] pops up at the bottom of their screen each time a screen shot has been taken."[59] They are regularly made aware that they are being observed.[60]

The pressure on employers to monitor workers who are increasingly seen as "independent" and thus further away from direct control also comes from heightened fears of corporate and global espionage, especially from sophisticated nation-states. Recently, the U.S. government has stepped up efforts to strengthen economic cybersecurity and federal trade secret law to address extraterritorial attempts to infiltrate and acquire domestic proprietary information from employers.[61]

So while there have been rapid technological innovations in scrutinizing and surveilling workers, and political frameworks within which to justify the use of those surveillance techniques, there has been little innovation when it comes to privacy protections for workers.

II.
EXTANT LEGAL PROTECTIONS

There are no federal laws that expressly address employer surveillance or limit the intrusiveness of such surveillance. The federal laws that have been created for the benefit of workers focus instead on protecting them from employment discrimination while largely disregarding privacy claims. When federal laws have proscribed worker surveillance, such proscription has been incidental to curtailing employment discrimination of protected minority groups.

---

56. *See Introducing Upwork—Our New Name and Platform*, UPWORK GLOB., https://www.upwork.com/blog/2015/05/odesk-is-now-upwork [https://perma.cc/3BTC-2925] (last visited Feb. 28, 2017) (The Upwork website serves as an intermediary between freelance workers and individuals or corporate entities who would like to hire the workers for specific work projects. The website then receives a percentage of the fee paid to the worker as commission.).

57. *Id.*

58. Shellenbarger, *supra* note 54.

59. *Id.*

60. *Id.*

61. *See* Lesley Stahl, *The Great Brain Robbery*, CBS NEWS (Jan. 17 2016), http://www.cbsnews.com/news/60-minutes-great-brain-robbery-china-cyber-espionage [https://perma.cc/4VYM-NJEQ]; Sens. Orrin Hatch & Chris Coons, *Pass the Defend Trade Secrets Act*, HILL (Jan. 27, 2016, 7:00 PM), http://thehill.com/opinion/op-ed/267205-pass-the-defend-trade-secrets-act [https://perma.cc/H7SQ-ZXUD].

Due to the lack of explicit federal protection, most employees are or will be subject to employer surveillance. It is well established, for example, that government employees (both federal and state) have no reasonable expectation of privacy at work;[62] the employee's office or work space is subject to search by the employer without permission;[63] and any electronic device provided to the employee by the employer generally remains the property of the employer,[64] meaning that such electronic device could also be subject to search without permission.[65] The same holds true for employees of private companies where the general principle of "at-will employment" allows the private employer to demand acquiescence to surveillance as part of the employment bargain.[66] In practice, this means most employees should expect employers to monitor their work mail (both paper and electronic), company-associated social media accounts, company credit cards, company-provided phones, etc.[67]

In the following Sections, we discuss how certain federal laws could be read to afford workers some protection against surveillance. We also examine the limitations to such re-interpretations or expansions of extant federal antidiscrimination laws to address privacy concerns. With the illustrative example of laws that protect workers who smoke outside the workplace, we also discuss which states have stronger protections for worker privacy versus states with weaker protections.

A. Federal Law

As no federal laws directly address or limit the employer surveillance of workers, it could be said that under federal law, worker surveillance is limitless. Some might believe that the Electronic Communications Privacy Act of 1986 (ECPA)[68] or the Computer Fraud and Abuse Act (CFAA)[69] would afford employees protection, but that belief is erroneous. Title I of the ECPA, known as the Wiretap Act, governs electronic communication in transit[70] and expressly prohibits the interception of electronic communication without

62. City of Ontario v. Quon, 560 U.S. 746, 756–57 (2010).

63. O'Connor v. Ortega, 480 U.S. 709, 715–16 (1987).

64. *Quon*, 560 U.S. at 762.

65. *Id.* at 761.

66. The employee surveillance practices at the retail company Amazon are an example of the greater employer bargaining power to enact stringent employee surveillance policies without effective employee resistance. *See The Rise of Workplace Spying*, *supra* note 29.

67. Bob E. Lype, *Employment Law and New Technologies: Emerging Trends Affecting Employers*, 47 TENN. B.J. 20, 24 (2011).

68. 18 U.S.C. §§ 2510–2522 (2012); *see also* Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 874 (9th Cir. 2002) (reiterating that "Title I of the ECPA amended the federal Wiretap Act, which previously addressed only wire and oral communications, to 'address . . . the interception of . . . electronic communications.'").

69. 18 U.S.C. § 1030(a)–(h) (2012).

70. *See* 18 U.S.C. § 2511 (2012).

consent.[71] Title II of the ECPA, known as the Stored Communications Act (SCA),[72] governs electronic communication that has already been sent and is in storage.[73]

The ECPA's weaknesses to shield employees from employer surveillance are self-evident. The Wiretap Act is focused on the *interception* of electronic information. An employer need not intercept the electronic information employees send from work devices or even from personal devices. Technological advances mean that most electronic communications are stored in some form *after* they have been sent and even after the sender attempts to erase the information. Furthermore, the Wiretap Act allows monitoring if at least one party provides consent. As we discuss below, at-will employment makes such consent regimes risible as a protective measure.[74]

The SCA is similarly of little help to employees. It focuses on *authorization* to access a *facility* in which electronic information is stored.[75] The phrasing of the Act belies its age; the SCA was enacted before the advent of the Internet and subsequent advances in the storage of electronic information. With much electronic communication now taking place over the Internet, there is generally no need to enter (with or without authorization) any physical facility in which electronic communication is stored. As the now popular saying goes: "it's all in the cloud." Similarly, the SCA focuses on the limits of authorization.[76] The SCA prohibits access to stored electronic

---

71. The ECPA states defines a violation as when any person "(a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication; (b) intentionally uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication . . . ; (c) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection; . . . shall be punished [as stated subsequently in the statute]." *Id.* at § 2511(a)–(d). The ECPA defines electronic communication as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce . . . " 18 U.S.C. § 2510 (2012).

72. *See* 18 U.S.C. § 2701 (2012).

73. The SCA, 18 U.S.C. § 2701(a), states: "Except as provided [below,] whoever:

(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or

(2) intentionally exceeds an authorization to access that facility;

and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in [this section]."

74. *See infra* Part II.B.3. Note also that at least one court has held that the ECPA does not apply to physical monitoring of electronic workplace devices, even when the monitoring results in interception of electronic communications. United States v. Ropp, 347 F. Supp. 2d 831, 837–38 (C.D. Cal. 2004); *see also* Pauline T. Kim, *Bargaining with Imperfect Information: A Study of Worker Perceptions of Legal Protection in an At-Will World*, 83 CORNELL L. REV. 105 (1997) (noting the limited negotiation power left to the employee under an at-will employment contract).

75. *See* 18 U.S.C. §§ 2701–2712 (2012).

76. *See* 18 U.S.C. § 2701; *supra* text accompanying note 73.

information without proper authorization. Thus, an employer who has authorization to access an employee's electronically stored information whether through e-mail or social media or GPS tracking would not be found in violation of the SCA. A violation is pursuant only to exceeding authorization to access this type of information such as when it is done beyond work hours.[77] The SCA does nothing to address today's reality that electronic communication may be accessed remotely. Finally, the emphasis on authorization also overlooks at-will employment contracts with adhesive provisions that compel employees to submit to electronic monitoring as a prerequisite to employment or as part of employment expectations.

The CFAA[78] prohibits individuals or entities from "knowingly access[ing] a computer without authorization or exceeding authorized access" and thereby obtaining information.[79] Once again, this law affords little protection to the employee because its provisions do not take into account the nature of present day employer-employee relationships. In most workplaces, employers provide employees with computers, meaning that the employer owns the computer and does not need an employee's authorization to access it.

Some existing federal laws that are designed to prohibit discrimination against certain protected groups could be interpreted to also afford privacy protection against certain types of employee surveillance. These existing laws and their application to privacy protections are discussed below; however, we ultimately conclude that these protections are inadequate.

1. Title VII of the Civil Rights Act of 1964

Title VII of the Civil Rights Act of 1964 (Title VII) prohibits discrimination based on certain individual characteristics—race, color, religion, sex, or national origin.[80] It makes it illegal for employers to discriminate against individuals based upon those protected characteristics regarding the terms, conditions, and privileges of employment.[81] Further, employment agencies may not discriminate when hiring or referring applicants, and labor organizations are also prohibited from basing membership or union classifications on race, color, religion, sex, or national origin.[82]

---

77. *See* Penrose Comput. Marketgrp., Inc. v. Camin, 682 F. Supp. 2d 202, 210–11 (N.D.N.Y. 2010).

78. 18 U.S.C. § 1030(a)–(h) (2012).

79. 18 U.S.C. § 1030(a) (2012). The CFAA applies only when the conduct causes a "loss to [one] or more persons during any [one]-year period . . . aggregating at least $5,000 in value." *Id.* § 1030(a)(5). Losses under the statute include "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or consequential damages incurred because of the interruption of service." *Id.* § 1030(e)(11).

80. Pub. L. No. 88-352, §703, 78 Stat. 241, 255–57 (1964) (codified at 42 U.S.C. § 2000e-2 (2012).

81. *See id.*

82. *See id.*

Thus, for example, if an employee-applicant chooses not to identify their religion, one could interpret Title VII as protecting that candidate from an employer's attempts to determine the candidate's religion, even after the candidate is hired as an employee. To illustrate, an employer could be legally prohibited from surveilling its employees to determine who prayed at break time, who chose not to eat pork, or who abstained from other religiously proscribed practices. Under this reading of Title VII, this information only holds value as a tool of discrimination by the employer (particularly since the employee has chosen not to share it).

2. Americans with Disabilities Act

The Americans with Disabilities Act of 1990 (ADA) was enacted to eliminate discriminatory barriers against qualified individuals with disabilities, individuals with a record of a disability, and individuals who are perceived as having a disability.[83] It prohibits discrimination based on a physical or mental handicap and requires employers to make reasonable accommodations for disabled workers.[84]

President Franklin Delano Roosevelt carefully guarded his disability arising from the poliovirus from the media in order to avoid any biases regarding his ability to lead and discrimination by voters in future elections.[85] What FDR had to obscure his disability from others that few employees have today was the full force of the Secret Service behind him. As was noted in the *Editor & Publisher* in 1936, "if agents saw a photographer taking a picture of Roosevelt, say, getting out of his car, they would seize the camera and tear out the film."[86] This statement was confirmed by a 1946 survey of the White House photography corps which found that anyone the Secret Service caught taking banned photographs "had their cameras emptied, their films exposed to

83. *See* U.S. DEP'T OF JUSTICE, CIVIL RIGHTS DIV., A GUIDE TO DISABILITY RIGHTS (2009), http://www.ada.gov/cguide.htm#anchor65610 [https://perma.cc/96FC-9VKQ] ("Rehabilitation Act" section); *see also* 42 U.S.C. § 12101(b)(1) (2012) (noting that the ADA was enacted in part, "to provide a clear and comprehensive national mandate for the elimination of discrimination against individuals with disabilities"); *Id.* § 12102(1) (defining "disability" as "with respect to an individual—(A) a physical or mental impairment that substantially limits one or more major life activities of such individual; (B) a record of such an impairment; or (C) being regarded as having such an impairment."). The Americans with Disabilities Act Amendment Act (ADAAA) broadened the definition of the disabled individual under the ADA such that those individuals with systemic or cellular level pathologies are covered. Tasneem Dharamsi, Note, *Human Embryonic Stem Cells: Will* Sherley v. Sebelius *Expand the Definition of the Disabled Individual?*, 14 N.C. J.L. & TECH. ON. 239, 253 (2013). Thus, courts have also found that the HIV-positive status of an individual is enough for the individual to be protected under the ADA, despite the fact that the disease has not progressed to full-blown AIDS. *Id.* at 254–55.

84. *See* Americans with Disabilities Act, U.S.C. 42, §§ 12101–1212 (2008).

85. Curtis Roosevelt & International Herald Tribune, *FDR: A Giant Despite His Disability*, N.Y. TIMES (Aug. 5, 1998), http://www.nytimes.com/1998/08/05/opinion/05iht-edcurl.t.html [https://perma.cc/3W2Q-8UWA].

86. Matthew Pressman, *The Myth of FDR's Secret Disability*, TIME (July 12, 2013), http://ideas.time.com/2013/07/12/the-myth-of-fdrs-secret-disability [https://perma.cc/T7DR-65XT].

sunlight, or their plates smashed."[87] This stringent policy against photography was accepted as extra-legal and indulged as a *de facto* form of *lèse majesté*. As one correspondent mused: "By what right they do this I don't know . . . but I have never seen the right questioned."[88]

Yet, one could potentially interpret the ADA as affording protection against employee surveillance intended to discover an employee's disability. Much like how the pursuit of information relating to a protected category under Title VII could serve the ends of unlawful employment discrimination, a quest to uncover an employee's private disability could be the preparatory start to employment discrimination. Thus, an employee who is under surveillance for the employer's purpose of discovering a disability may have recourse under the ADA.

3. Age Discrimination in Employment Act

The Age Discrimination in Employment Act (ADEA)[89] is a remedial statute that was enacted to curb extant age discrimination in employment. The language and purposes behind the ADEA are similar to those of Title VII. As a result, courts look to Title VII cases as authoritative when deciding ADEA cases.[90] The ADEA generally prohibits employment discrimination against individuals who are forty years old or older.[91] Like Title VII, the ADEA also applies to employment agencies[92] and labor organizations.[93] However, the ADEA includes exceptions for individuals hired or to be hired as firefighters and police officers.[94]

The ADEA, also like Title VII, may be interpreted to protect against certain types of employer surveillance. As the ACLU has reported, a growing number of employers are asking prospective employees to provide access to their social media passwords.[95] An employer can often glean enormous amounts of protected information, including an employee's age, with access to that employee's social media accounts, such as Facebook. The employer could learn of the employee's age directly from the section of the user's profile that allows the individual to list their birth date, or the employer could deduce the

87. *Id.*
88. *Id.*
89. Pub. L. No. 90-202, 81 Stat. 602 (1967) (codified as amended at 29 U.S.C. §§ 621–34).
90. Since what is prohibited conduct under the ADEA was decided following the prohibitions expressed under Title VII, it follows that decisions regarding sections of Title VII that are analogous to the ADEA would be helpful in deciding cases regarding personal staff exemption under the ADEA. *See* EEOC v. Reno, 758 F.2d 581, 583–84 (11th Cir. 1985).
91. *See* 29 U.S.C. § 631(a).
92. § 623(b).
93. § 623(c).
94. § 623(j).
95. *Employers, Schools, and Social Networking Privacy*, ACLU, https://www.aclu.org/employers-schools-and-social-networking-privacy [https://perma.cc/3WYL-24K8] (last visited Feb. 28, 2017).

employee's age from the employee's high school graduation, another feature available on Facebook. An argument could be made then, that the ADEA should provide recourse to individuals residing in states that have not yet passed laws banning employers from requesting social media account passwords from their employees and applicants.[96]

4. The Employment Non-Discrimination Act

The Employment Non-Discrimination Act (ENDA), which is still under consideration in Congress, prohibits private employers with more than fifteen employees from discriminating on the basis of sexual orientation or gender identity.[97] Religious organizations are provided an exception, which is broader than the exception provided in the Civil Rights Act of 1964.[98] Non-profit membership-only clubs, except labor unions, are similarly exempt.[99] President Barack Obama signed an executive order on July 21, 2014, that made the ENDA applicable to federal contractors.[100] President Obama also amended a separate executive order to extend the ENDA workplace protections to federal government employees. President Obama's executive order does not include a religious exemption for federal employees.[101]

President Obama's executive order could mean that employers (including the federal government) cannot legally subject federal employees to surveillance meant to detect either sexual orientation or biological sex. In the context of a white-collar office in the United States, the ENDA would prevent an employer from subjecting a federal employee to surveillance meant to uncover that employee's sexual orientation. It could also mean, for example, that an employee asserting the right to use a sex-segregated bathroom would not have to submit to surveillance to prove that their reproductive organs corresponded to the requisite sex.

---

96. Delaware recently signed such a law into effect. "The Employee/Applicant Protection for Social Media Act prevents employers from demanding access to an employee's or applicant's personal social media accounts. Under the new rule, employees are also protected from being forced to log in for the employer, accepting the employer as a 'friend,' or being forced to disable their account's privacy settings so that the employer can view their full online profile." *Delaware Governor Signs Internet Privacy, Safety Package into Law*, GOV'T TECH. (Aug. 10, 2015), http://www.govtech.com/internet/Delaware-Governor-Signs-Internet-Privacy-Safety-Package-into-Law.html [http://perma.cc/LW6J-JNQ9].

97. *See* Employment Non-Discrimination Act of 2013, S. 815, 113th Cong. (2014).

98. *Id.*

99. *Id.*

100. Steve Benen, *Obama Advances Anti-Discrimination Policy with Executive Order*, MSNBC (July 21, 2014, 12:53 PM), http://www.msnbc.com/rachel-maddow-show/obama-advances-anti-discrimination-policy-executive-order [https://perma.cc/5DW6-YXGK].

101. *Id.*

5. Pregnancy Discrimination Act

The Pregnancy Discrimination Act (PDA) is an amendment to Title VII of the Civil Rights Act of 1964.[102] The Act provides that discrimination on the basis of pregnancy, childbirth, or related medical conditions constitutes unlawful sex discrimination under Title VII.[103] The PDA mandates that

> an employer cannot refuse to hire a woman because of her pregnancy related condition as long as she is able to perform the major functions of her job. An employer cannot refuse to hire her because of its prejudices against pregnant workers or because of the bias of co-workers, clients, or customers. The PDA also forbids discrimination based on pregnancy when it comes to any other aspect of employment, including pay, job assignments, promotions, layoffs, training, fringe benefits, firing, and any other term or condition of employment.[104]

The PDA could afford women some protection against certain types of surveillance in the workplace—notably, one could read the PDA to provide employee protection from surveillance meant to determine her pregnancy status. Notwithstanding the PDA, however, the instances of pregnancy discrimination seem to be on the rise. In 2006, the Equal Employment Opportunity Commission (EEOC) saw nearly five thousand complaints of pregnancy-based discrimination, which represented a 30 percent jump from the previous decade, and more than six thousand complaints in 2010.[105] So, despite legislatures' attempts to curb surveillance that is intended to determine one's pregnancy status, the rise in the number of complaints suggests that such attempts have been ineffective.

6. The Genetic Information Non-Discrimination Act

The Genetic Information Non-Discrimination Act (GINA),[106] signed into law by President George Bush in 2008, protects Americans from genetic discrimination in the healthcare insurance coverage and employment contexts. GINA remains a primarily administrative law, meaning that the EEOC is charged with enforcing it and that a private plaintiff must exhaust administrative procedures within the EEOC before bringing suit under the auspices of GINA.

---

102. *See* Pregnancy Discrimination Act, S. 995, 95th Cong. (1978); *see also Pregnancy Discrimination Fact Sheet*, U.S. EQUAL EMPLOYMENT OPPORTUNITY COMMISSION https://www.eeoc.gov/laws/statutes/pregnancy.cfm [https://perma.cc/LGX3-N4N7].

103. *Pregnancy Discrimination*, U.S. EQUAL EMP'T OPPORTUNITY COMM'N, http://www.eeoc.gov/eeoc/publications/fs-preg.cfm [https://perma.cc/FY3W-8243] (last visited Feb. 28, 2017).

104. *Id.*

105. Darlena Cunha, *When Bosses Discriminate Against Pregnant Women*, ATLANTIC (Sept. 24, 2014), http://www.theatlantic.com/business/archive/2014/09/when-bosses-discriminate-against-pregnant-women/380623 [https://perma.cc/T65L-EBCX].

106. The Genetic Information Nondiscrimination Act of 2008, Pub. L. 110-233, 122 Stat. 881 (2008).

One of the early cases to allege a GINA violation was that of Pamela Fink, a resident of Connecticut who was fired from her job in 2009 (the year GINA took effect) allegedly because her employers discovered that she was the carrier of a mutated gene linked to breast cancer (BRCA2) through her choice of a prophylactic double mastectomy.[107] According to Fink, she had been an exemplary employee and had received her first negative review only after her double mastectomy and the day before her reconstructive surgery.

Unlike in Fink's case, the "devious defecator" case involved more active employer conduct. There, a group of employees alleged that their employer had, under threat of dismissal, compelled them to produce DNA samples, which the employer then subjected to genetic testing in order to discover the identity of the employee who had been leaving feces around the perimeter of the workplace.[108] The employees alleged that the employer's actions were a violation of GINA. Although this case does not squarely fit into what GINA, as an anti-discrimination law, was designed to accomplish, privacy advocates were heartened by the outcome of the case—not only was this the first GINA case brought to trial, but it also resulted in a $2.25 million award to the employees. As of this writing, the case has yet to be overturned on appeal.[109]

While GINA ordinarily prohibits employers from collecting genetic information—such as family medical history—through wellness programs, a recent EEOC guideline has reconciled GINA's prohibitions with the government's backing of wellness programs. The EEOC guideline has established that the voluntary collection of family medical histories as a part of wellness programs does not constitute a violation of GINA.[110] However, this recent set of guidelines still conflicts with the pending lawsuits that the EEOC has brought against wellness programs that it contends violate the ADA, GINA, and the Health Information Portability and Accountability Act.[111]

---

107. Emily Friedman, *Pamela Fink Says She Was Fired After Getting a Double Mastectomy To Prevent Breast Cancer*, ABC NEWS (Apr. 30, 2010), http://abcnews.go.com/Health/OnCallPlusBreastCancerNews/pamela-fink-fired-testing-positive-breast-cancer-gene/story?id=10510163 [https://perma.cc/9DS6-WRM3].

108. Daniel Wiessner, *Georgia Workers Win $2.2 Million in 'Devious Defecator' Case,* REUTERS (June 23, 2015, 11: 41 AM), http://www.reuters.com/article/2015/06/23/us-verdict-dna-defecator-idUSKBN0P31TP20150623 [https://perma.cc/G356-WR3M].

109. *Id.*

110. "Subsequently, in enacting rules under the Genetic Information Nondiscrimination Act (GINA), which allows the voluntary provision of genetic information in the context of wellness programs (42 U.S.C. § 2000ff-1(b)(2)), the EEOC rejected the HIPAA approach, instead requiring employers to make clear that employees could qualify for HRA incentives even if they declined to answer questions requiring genetic information." Kristin Madison, *The ACA, The ADA, and Wellness Program Incentives*, HEALTH AFFAIRS BLOG (May 13, 2015), http://healthaffairs.org/blog/2015/05/13/the-aca-the-ada-and-wellness-program-incentives [http://perma.cc/W8P4-3MJW].

111. For a discussion of the allegations in the three lawsuits the EEOC has brought against employers regarding their workplace wellness programs, see *infra* Part II.A.2.

7. Health Information Portability and Accountability Act

Like GINA, HIPAA has been employed to protect interests that it was not necessarily designed to protect. HIPAA's fundamental function is to allow the transfer of health records (including electronic health records) between health care providers and to insurance companies for billing purposes.[112] However, one popular misconception is that HIPAA was designed to protect the privacy interests of patients.[113] This erroneous assumption is understandable given that there is no other federal law that comprehensively protects health information.[114] Yet, HIPAA's protection of health information is limited.

Although HIPAA does not provide a private tort cause of action, in *Acosta v. Byrum,* the court employed the standard of care from HIPAA to establish a tort claim of negligent infliction of emotional distress in a suit brought in state court regarding the improper disclosure of electronic medical information.[115] The *Acosta* plaintiff, a patient, sued her psychiatrist for negligent infliction of emotional distress.[116] The plaintiff alleged that the doctor wrongfully allowed an office manager to access her medical records using the doctor's own medical record access number.[117] The plaintiff further alleged that she suffered severe emotional distress, humiliation, and anguish when the office manager then disclosed her medical records to other parties.[118] In her complaint, the plaintiff asserted that, by providing his medical access code to the office manager, the doctor violated the rules and regulations established by HIPAA.[119] Although she did not assert a HIPAA claim, the plaintiff cited HIPAA as establishing the appropriate standard of care in her case.[120] The trial court dismissed the case on the grounds that HIPAA does not grant an

112. *See* U.S. DEP'T OF LABOR, EMP. BENEFITS SEC. ADMIN., FACT SHEET: THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (2015), https://www.dol.gov/agencies/ebsa/about-ebsa/our-activities/resource-center/fact-sheets/hipaa [https://perma.cc/W4SA-KB55] (noting that HIPAA's function is to "improve portability and continuity of health insurance coverage").

113. Many wrongly assume that the "P" in HIPAA stands for "privacy." *See HIPAA and PHI: What is HIPPA?*, WEILL CORNELL MED., https://its.weill.cornell.edu/security-and-privacy/hipaa-and-phi [https://perma.cc/7TUB-YPDX] (last visited Feb. 28, 2017); *but see Medical Privacy,* ELECTRONIC FRONTIER FOUND., https://www.eff.org/issues/medical-privacy [https://perma.cc/W7JN-GVCJ] (last visited Feb. 28, 2017).

114. *See Medical Privacy*, *supra* note 113.

115. Acosta v. Byrum, 638 S.E.2d 246, 250–52, 254 (N.C. Ct. App. 2006) (holding, first, that the plaintiff was allowed to derive a "standard of care" from HIPAA rules, defining the physician's duty to protect the confidentiality of the patient's records, and, second, that a patient could establish a sufficient claim for negligent infliction of emotional distress against her physician for an incident in which he gave his computer security code to his office manager, who then accessed the patient's confidential healthcare records and disclosed the information to other parties).

116. *Id.* at 249.

117. *Id.*

118. *Id.*

119. *Id.* at 253.

120. *Id.*

individual a private cause of action.[121] But the appellate court reversed, agreeing with the plaintiff that HIPAA's provisions may be referred to for the appropriate standard of care in the case, even though this was a suit based on a negligence cause of action and no HIPAA violation was being alleged.[122] This precedent means that employees could use HIPAA, like GINA, to protect themselves against surveillance meant to discover genetic condition.

It is worth noting, however, that *Acosta* allowed HIPAA to serve as the standard of care where the plaintiff alleged an actual harm (i.e., emotional distress). A significant problem in using HIPAA and the other federal laws previously discussed to protect against employer surveillance is that the harm those laws were designed to protect against is employment discrimination; loss of privacy is not currently recognized as a harm at the federal level.

B. State Law

There is a divide between the private (corporate entities) and public (government employers) sectors when it comes to surveillance. While the Constitution may protect workers from government surveillance, workers employed by a private employer cannot rely on the Constitution for protection since a "state action" would be required for an employee to invoke a constitutional right. As a result, public-sector employees enjoy far greater privacy rights than do private-sector employees.[123] For the average private-sector worker, the only legal shields against intrusive employer surveillance are various state statutes or the common law tort of invasion of privacy.[124] Even, then, "[t]he protection provided by these remedies varies widely from jurisdiction to jurisdiction and in some cases has not protected against even outrageous forms of employer intrusions."[125]

1. States with Stronger Protections

Some states have explicitly promulgated privacy protections for workers as part of their state constitution. For example, ten state constitutions protect the privacy of public employees: Alaska, California, Florida, Hawaii, Illinois, Louisiana, Montana, New York, South Carolina, and Washington. The California Constitution also protects data privacy.[126]

Of the states that do not have privacy provisions in their state constitution, several have nonetheless instituted laws that restrict the employer's capacity to surveil employees. Legal scholars have found that prior to 2012, these laws fell

121. *Id.*
122. *Id.* at 253–54.
123. S. Elizabeth Wilborn, *Revisiting the Public/Private Distinction: Employee Monitoring in the Workplace,* 32 GA. L. REV. 825, 828–29 (1998).
124. *Id.*
125. *Id.*
126. CAL. CONST. art. I, § 13.

into three broad categories. The first category mimics the Wiretap Act by allowing for video surveillance but no corresponding audio; therefore, laws in this category offer no explicit protection from video only monitoring. The second category, even narrower than the first, protects only the most intimate employee spaces, such as restrooms and changing rooms, from video surveillance. The third category, which is the least protective, demands only a notice requirement to alert employees to the fact that they are being surveilled.[127] The criticism of these laws is that they do not do enough to protect the worker, and that they merely "give[] employers a legal safety net to avoid litigation simply by posting a notice of surveillance, and . . . ignore[] employees' dignity rights."[128]

Since 2012, some states have gone further in their bid to protect worker privacy by also instituting laws that afford workers protection for their social media accounts:

> In May 2012, Maryland became the first state to restrict employers' ability to demand that employees or prospective employees disclose their "user name, password, or other means for accessing a personal account or service through an electronic communications device." California, Illinois and Michigan followed suit that year with similar prohibitions, and in 2013, Arkansas, Colorado, Nevada, New Jersey, Oregon, Utah and Washington enacted laws protecting the privacy of job applicants' and employees' personal social media accounts. New Mexico also enacted a law in 2013 that affects only job applicants and doesn't mention current employees.[129]

The Delaware governor recently signed into law the Employee/Applicant Protection for Social Media Act, which prevents employers from demanding access to an employee or applicant's personal social media accounts. The law also protects employees from "being forced to log in for the employer, accepting the employer as a 'friend,' or being forced to disable their account's privacy settings so that the employer can view their full online profile."[130]

In addition, some states have passed laws to address the location tracking of workers. For example, in California it is a misdemeanor to use an electronic tracking device to determine the location or movement of a person without his or her consent.[131] And in Connecticut, a statute prohibits any employer from

---

127. Alexandra Fiore & Matthew Weinick, *Undignified in Defeat: An Analysis of the Stagnation and Demise of Proposed Legislation Limiting Video Surveillance in the Workplace and Suggestions for Change*, 25 HOFSTRA LAB. & EMP. L.J. 525, 542–43 (2008).

128. *Id.*

129. Bryan Knedler & William Welkowitz, *States Continue to Protect Workers' Social Media Privacy in 2014*, BLOOMBERG BNA (Feb. 10, 2015) https://www.bna.com/states-continue-protect-n17179922967/ [https://perma.cc/ML6D-7QMW].

130. *Delaware Governor Signs Internet Privacy, Safety Package into Law*, *supra* note 96.

131. Kendra Rosenberg, *Location Surveillance by GPS: Balancing an Employer's Business Interest with Employee Privacy,* 6 WASH. J.L. TECH. & ARTS 143, 149 (2010).

electronically monitoring an employee's activities without prior notice to all employees who may be affected.[132]

California has particularly strong worker privacy protections. In *Mintz v. Mark Bartelstein & Associates Inc.*,[133] an employee filed a complaint against his employer, alleging violation of the CFAA and California Data Access and Fraud Act and asserting various state law claims. The court found that the undisputed allegation that the former employer used plaintiff's Gmail account to view information about the terms of plaintiff's employment with his subsequent employer, including his compensation was an act that "clearly implicated Plaintiff's legally protected interest in the privacy of his employment and financial affairs."[134] Further, the court noted the California Supreme Court's recognition that "an individual's expectation of privacy in a salary earned in public employment is significantly less than the privacy expectation regarding income earned in the private sector"; this observation, the district court found, reinforces the premise that individuals have a legitimate privacy interest with respect to income earned in the private sector.[135] California courts have similarly recognized employees' protected privacy interest in their own employment personnel files.[136]

2. States with Weaker Protections

In contrast to California, some states have particularly weak protections for worker privacy. Massachusetts is illustrative of these weaker protection states. Massachusetts courts have emphasized that privacy cases require a careful balancing of an employer's legitimate business interest in obtaining an employee's private information and the employee's interest in keeping personal information private.[137] However, before a court may even proceed with the "balancing test," the employee plaintiff must first establish that they have a protected privacy interest in the information at issue.[138] Problematically, Massachusetts's courts have not found an employee privacy interest in acts committed outside the workplace.

Rodrigues v. EG Systems, Inc.,[139] provides a representative snapshot of how an employee's acts outside of the workplace may not be deemed private information. Rodrigues, a conditional employee, was dismissed from

132. *Id.*
133. *See* 906 F. Supp. 2d 1017 (C.D. Cal. 2012).
134. *Id.* at 1033.
135. *Id.*
136. *Id.*; *see also* El Dorado Sav. & Loan Ass'n v. Superior Court, 190 Cal. App. 3d 342, 345 (Cal. Ct. App. 1987) (noting that a personnel file may contain information that an employee "has an interest in keeping private").
137. *See* Webster v. Motorola, Inc., 637 N.E.2d 203, 207 (Mass. 1994); Bratt v. Int'l Bus. Machs. Corp., 467 N.E.2d 126, 135 (Mass. 1984); Folmsbee v. Tech Tool Grinding & Supply Inc., 630 N.E.2d 586, 588 (Mass. 1994).
138. *See, e.g.*, Rodrigues v. EG Sys., Inc., 639 F. Supp. 2d 131, 134 (D. Mass. 2009).
139. *Id.* at 131.

consideration for permanent employment after test results showed nicotine use, revealing that he was a smoker. In response to this dismissal, Rodrigues "sued [the] employer, asserting state statutory claims for violation of privacy and civil rights violation, as well as common-law wrongful termination claim, and also asserting [a] claim under Employee Retirement Income Security Act (ERISA)."[140]

The Massachusetts court found that Rodrigues did not have a protected privacy interest in the fact that he was a smoker because he did not keep that fact private. The court noted that in his deposition, Rodrigues admitted to smoking openly in public and he had testified that "he smokes while walking down the street heading to the post office, that he smokes with others in the parking lot of a McDonald's restaurant, and that he openly purchases cigarettes wherever they are sold."[141] According to the court, also pertinent to determining the privacy of Rodrigues' act was the fact that "during the time he was working with Scotts [another employer], a supervisor noticed a pack of cigarettes in plain view on the dashboard of Rodrigues's vehicle and gave him a written warning as a result."[142] The Massachusetts court found that because of these admissions, Rodrigues had no cause of action to contest his dismissal under the Massachusetts privacy statute.[143]

Of special interest to our arguments in this Article are the Massachusetts courts' rulings on medical information. In *Bratt v. International Business Machines Corporation*,[144] an "[e]mployee brought action against employer, its agent, and another employee alleging libel and invasion of privacy."[145] The holding on appeal was that:

> (1) loss of a defendant's conditional privileges to defamatory materials through 'unnecessary, unreasonable or excessive publication' requires proof that defendant acted recklessly; (2) employer can lose privilege as to disclosure of defamatory medical information only if employee proves that disclosure resulted from an expressly malicious motive, was recklessly disseminated, or involved reckless disregard for truth or falsity of information; (3) disclosure of private facts about an employee among other employees in same corporation can constitute sufficient publication under right of privacy statute; (4) although no conditional privilege for legitimate business communications exists under right of privacy statute, employer's obtaining and disclosing personal information concerning an employee *may not amount to an unreasonable inference with employee's statutory right of privacy*; and (5) *when medical information is necessary reasonably to serve substantial and valid interest of employee, it is not an invasion of*

140. *Id.*
141. *Id.* at 134 (citations omitted).
142. *Id.*
143. *Id.*
144. 467 N.E.2d 126 (Mass. 1984).
145. *Id.* at 126–27.

employee's statutory right of privacy for physician to disclose such information to employer."[146]

Massachusetts' approach to worker privacy can be summed up as a balancing of interests in which the employer's legitimate business interest is accorded paramount importance over the worker's right to privacy. The court in *Bratt* noted, "We have concluded previously, however, that because § 1B proscribes only unreasonable interferences with a person's privacy, *legitimate countervailing business interests in certain situations may render the disclosure of personal information reasonable* and not actionable under the statute."[147]

Finally, as an illustration of which states afford workers the least privacy protections, we use smoker discrimination as a litmus test. The table below shows the states in which a worker may be fired for being a smoker, even if the smoking occurs solely outside the workplace.

States where an employee could be fired for being a smoker									
Alabama	Ye	Hawaii	No	Michigan	No*	North	No*	Utah	No*
Alaska	Ye	Idaho	No	Minnesota	No	North	No*	Vermont	No*
Arizona	No	Illinois	No*	Mississippi	No	Ohio	No*	Virginia	Yes
Arkansas	No	Indiana	No	Missouri	No	Oklahoma	No*	Washingto	Yes
Californi	No	Iowa	No	Montana	No*	Oregon	No*	West	No*
Colorado	No	Kansas	No	Nebraska	Yes	Pennsylvan	No*	Wisconsin	No*
Connecti	No	Kentucky	No*	Nevada	No	Rhode	No	Wyoming	No*
Delaware	No	Louisiana	No	New	No	South	No		
D.C.	No	Maine	No	New Jersey	No	South	No*		
Florida	Ye	Maryland	No*	New Mexico	No	Tennessee	No		
Georgia	Ye	Massachus	Yes	New York	No*	Texas	Yes		

146. *Id.* (emphasis added).
147. *Id.* at 135 (emphasis added).

*The protection is either not specific or not absolute, some contingencies may apply such as the business interest of the employer, etc. **It is lawful to have different insurance coverage or different insurance contribution rates for smokers versus non-smokers. *** Both contingencies above apply. Compiled from: *Workplace Smoking Laws in Your State*, NOLO, http://www.nolo.com/legal-encyclopedia/workplace-smoking-laws-your-state-46877.html [https://perma.cc/8J4L-Y4KW] (last visited Feb. 28, 2017).

Although most employment in the United States is "at-will," meaning that no cause is needed for a firing, the fact that the above-noted states allow employers to fire employees for their status as smokers is still relevant. Even when "at will" employment contract guarantees that the employee cannot be fired without cause, the law in those states allows the employer to claim smoking as "cause" for dismissal.[148]

3. The Pernicious Effects of Employment Contracts

Complicating the issue of worker surveillance is the fact that "at-will" employment contracts may provide conditions upon which the worker must accept employment and upon which the employment contract would be terminated.[149] Thus, employment contracts may be conditioned upon the worker acquiescing to surveillance by the employer.

These contractual complications suggest that the solution for preventing intrusive and unreasonable worker surveillance cannot lie in contractual law. In a global economy with a burgeoning labor force and the technological advances to harness the power of that labor force (in almost all the reaches of the world), there exists significant asymmetrical bargaining power between the employer and the employee such that the average employee may lack the bargaining power to protect her privacy interests on the basis of a contract.

148. *See, generally*, *Workplace Smoking Laws in Your State*, NOLO, http://www.nolo.com/legal-encyclopedia/workplace-smoking-laws-your-state-46877.html [https://perma.cc/8J4L-Y4KW] (last visited Feb. 28, 2017).

149. *See, e.g.*, William R. Corbett, *The Need for a Revitalized Common Law of the Workplace*, 69 BROOK. L. REV. 91, 125–27 (2004) ("Despite the dubious proposition that someone can do something for no reason at all, the now famous, or infamous, iteration of employment at will encapsulates the absolute power of employers to govern the workplace. Although employment at will expressly addresses employers' absolute right to terminate employees, it is about much more. One who has the power to terminate also has the power to do as she pleases with respect to all terms and conditions of employment. At its core, employment at will is about employer power and prerogative.").

III.
THE NEW ARENAS FOR WORKPLACE SURVEILLANCE

What are the new social and technological developments that are shaping workplace surveillance? In this Section we consider government-backed corporate wellness programs, the growing popularity of productivity apps that afford employers the opportunity to circumvent existing legal constraints on worker surveillance, and the ways that the breach of legal protections could harm the worker and the social good in general.

A. Workplace Wellness Program

Wellness programs are defined as "any [workplace] program designed to promote health or prevent disease,"[150] and have evolved to offer health risk assessment, weight reduction, and smoking cessation programs.[151] The most common objectives of these programs are smoking cessation and weight loss or the related behaviors of nutrition and fitness.[152] Currently, companies can work with employee wellness firms that mine employee data to gain deep insights about a company's employees—which prescription drugs they use, whether they vote, and when they stop filing their birth control prescriptions.[153] Walmart, for example, pays Castlight Health, Inc., to assess employee data and nudge employees toward weight loss programs or suggest physical therapy instead of expensive operations.[154] These programs raise serious questions about how much data employers should be able to use, when employers should be able to use such data, and how employers might use that data in discriminatory contexts. Additionally, while most of these programs are voluntary, some scholars have expressed concern about the fact that some employers are now making these programs mandatory and about the incentives and penalties tied to these programs.[155]

---

150. Ann Hendrix & Josh Buck, *Employer-Sponsored Wellness Programs: Should Your Employer Be the Boss of More Than Your Work*?, 38 SW. L. REV. 465, 468 (2009).

151. *Id.*

152. SOEREN MATTKE ET AL., RAND CORP., WORKPLACE WELLNESS PROGRAMS STUDY xv (2013).

153. *See* Rachel Emma Silverman, *Bosses Tap Outside Firms to Predict Which Workers Might Get Sick*, WALL ST. J. (Feb 17, 2016, 7:58 PM), https://www.wsj.com/articles/bosses-harness-big-data-to-predict-which-workers-might-get-sick-1455664940 [https://perma.cc/92UD-RVGA].

154. *Id.*

155. Mandatory wellness programs vary widely in terms of their application. For example, one program may require that employees undergo a "health risk assessment," including screening for risk factors such as high cholesterol and high blood pressure. Another program may require that employees collaborate with advisors who create and monitor fitness plans on the employee's behalf. Because of the varying nature of employee health statuses, the degree of employer financial expenditures and obligations, and the societal value placed on employee health within the workplace, the organization typically tailors its program to match the goals of the organization's workforce as a whole. Daniel Charles Rubenstein, *The Emergence of Mandatory Wellness Programs in the United States: Welcoming, or Worrisome?*, Note, 12 J. HEALTH CARE L. & POL'Y 99 (2009).

"Wellness" is generally used to mean a healthy balance of the mind, body, and spirit that results in an overall feeling of well-being. Halbert L. Dunn, M.D., introduced the concept to alternative medicine with his use of the phrase "high level wellness" in the 1950s.[156] The modern concept of wellness did not, however, become popular in corporate America until the 1970s.[157]

Since the 1970s, the government has actively promoted wellness within the workplace. Indeed, the idea of the government as a "residual guarantor" is one that has taken root in American society.[158] The government's role as a guarantor of health outcomes compels it to recruit the private sector to facilitate the achievement of the government's health goals.[159] This explains the Obama administration's support of wellness programs and the reinterpretation of protective federal laws to allow the surveillance endemic to wellness programs. Thus, employers now enjoy greater latitude to establish and administer wellness programs in the workplace.[160]

Currently, workplace wellness programs represent a $6 billion industry that includes an estimated five-hundred vendors selling programs either individually or as an optional component of healthcare insurance. When President Obama signed the Patient Protection and Affordable Care Act (ACA) into law in 2010, many rejoiced because it protected American individuals from denials of healthcare coverage based on pre-existing conditions. However, embedded within the ACA were other equally important provisions that were largely ignored. The ACA supports wellness programs through several of its provisions. "Notably, it provides start-up grants to small firms; establishes a '10-state demonstration program on rewards for wellness program participation in the individual market; and assigns a technical assistance role for the Centers for Disease Control and Prevention.'"[161]

"[A]pproximately half to two-thirds of U.S. employers offer some kind of" wellness program.[162] In 2013, 99 percent of large firms (those with two

156. *See* Halbert L. Dunn, *High-Level Wellness for Man and Society*, 49 AM. J. PUB. HEALTH 786 (1959).

157. Peter Conrad, *Wellness in the Work Place: Potentials and Pitfalls of Work-Site Health Promotion,* 65 MILBANK Q. 255, 257 (1987).

158. The government is a "residual guarantor" of health services, whether it provides these services directly or through community agencies. Every locale and population should be served by a unit of government which takes a leadership role in assuring the public's health. AM. PUB. HEALTH ASS'N, HEALTHY COMMUNITIES 2000: MODEL STANDARDS 443 (1991).

159. "Many of the activities . . . go beyond the activities customarily carried out by State and local governmental entities. Even in those areas where health agencies are extensively involved, prevention is a shared responsibility of the public and private sector." *Id.*

160. Lindsay F. Wiley, *Access to Health Care as an Incentive for Healthy Behavior? An Assessment of the Affordable Care Act's Personal Responsibility for Wellness Reforms*, 11 IND. HEALTH L. REV. 635, 655 (2014).

161. Lisa Klautzer et al., *Can We Legally Pay People for Being Good? A Review of Current Federal and State Law on Wellness Program Incentives*, 49 INQUIRY 268, 268 (2012).

162. Marcie Pitt-Catsouphes et. al., *Workplace-Based Health and Wellness Programs: The Intersection of Aging, Work, and Health*, 55 GERONTOLOGIST 262, 263 (2015).

hundred or more workers) offered at least one wellness program. Specifically, 69 percent offered gym membership discounts or on-site gyms, 71 percent offered smoking cessation programs, and 58 percent offered weight-loss programs.[163] Among those firms, 51 percent offered some financial incentive to participate in wellness programs.[164] Employers use incentives more often to encourage completion of a health risk assessment or participation in a wellness program than to reward behavior change. In 2013, incentives ranged from 3 to 11 percent of the total cost of individual coverage.[165] The use of incentives is likely to expand; 29 percent of employers reported that one of the top areas of focus for their health care strategy was adopting or expanding the "use of financial incentives to encourage healthy activities."[166]

By granting employers leeway to recruit employees into wellness programs, the ACA, "raises the maximum incentive to employees for achieving health related standards, such as reaching a target weight, to 30% of the cost of their insurance coverage."[167] This new maximum, effective January 1, 2014, "can—with approval from the Secretaries of Health and Human Services, Labor, and the Treasury—be increased to 50% of the cost of coverage."[168] The ACA already allows up to 50 percent of the cost of the insurance coverage to be offered to individuals as an incentive for smoking cessation.[169]

Wellness programs are poised to become ubiquitous in the corporate space, particularly given that group health insurers now have many choices in designing incentives and more than 60 percent of Americans now receive their health insurance coverage through an employment-based plan.[170] The incentives "can be carrots (rewards) or sticks (penalties), and can take the form of modified premiums, smaller copays or deductibles, cash, gift cards, or merchandise."[171] Financial incentives have increased "to a record $693 per employee, on average, this year from $594 in 2014 and $430 five years ago."[172]

---

163. KAISER FAMILY FOUND., EMPLOYER HEALTH BENEFITS SURVEY (2014), http://kff.org/report-section/ehbs-2014-summary-of-findings [https://perma.cc/42N7-DZUY].

164. *Id.*

165. Incentives for Nondiscriminatory Wellness Programs in Group Health Plans, 45 Fed. Reg. 33,158, 33,168 (June 3, 2013) (to be codified at 45 C.F.R. pts. 146–47).

166. TOWER WATSON/NAT'L BUS. GRP. ON HEALTH, THE NEW HEALTH CARE IMPERATIVE: DRIVING PERFORMANCE, CONNECTING VALUES 6 (2014), https://www.towerswatson.com/en-US/Insights/IC-Types/Survey-Research-Results/2014/05/full-report-towers-watson-nbgh-2013-2014-employer-survey-on-purchasing-value-in-health-care [https://perma.cc/M73X-W4AM].

167. *Id.*

168. *Id.*

169. REDBRICK HEALTH, PATIENT PROTECTION AND AFFORDABLE CARE ACT OF 2010 (ACA) WELLNESS RULES 6 (2013).

170. David Blumenthal, *Employer-Sponsored Health Insurance in the United States—Origins and Implications*, 355 NEW ENG. J. MED. 82, 82 (2006).

171. John Cawley, *The Affordable Care Act Permits Greater Financial Rewards for Weight Loss: A Good Idea in Principle, But Many Practical Concerns Remain*, 33 J. OF POL'Y ANALYSIS & MGMT. 810, 811 (2014).

172. Sharon Begley, *Employer Incentives for U.S. Worker Wellness Set Record*, REUTERS (Mar. 26, 2015 4:13 AM), http://uk.reuters.com/article/2015/03/26/us-usa-healthcare-wellness-

"Companies with more than 20,000 employees are offering an average of $878 this year to induce workers to participate. Companies with 5,000 to 20,000 workers are offering $661, up from $493 in 2014."[173] It is unclear, however, whether these incentives cloud the asymmetrical power relationship between the employer and the employee. Another question exists as to whether wellness programs coerce employees to relinquish valuable and sensitive health information for a mere pittance in the form of premium reductions.

1. Issues with Electronic Data Collection

Many workplace wellness programs employ wearable electronic fitness trackers such as Fitbit or Jawbone. As previous research demonstrates, the data from fitness trackers can be irregular and unreliable.[174] Furthermore, the data from trackers requires interpretation. Data analytic companies that interpret the data using "industry and public research"[175] define the standards that measure a worker's health status and health risks. One problem with this, as scholars have noted, is that medical and health research rapidly changes, such that standards as to what is "healthy" are not the same as they were in the past.[176] Yet, the companies interpreting the data from wearables lawfully operate as black boxes, concealing their data sets and the algorithms they use for interpretation.[177]

Another overlooked problem is that of access to the data collected by employer-provided wearables. Legally, when an employer provides an employee with a device, whether it be a laptop, a mobile phone, or a fitness tracker, that device remains the property of the employer. This means that the

---

idUKKBN0MM0BB20150326 [https://perma.cc/N3A8-RZ7Q]; *see also* Kate Crawford et al., *Our Metrics, Ourselves: A Hundred Years of Self-Tracking from the Weight Scale to the Wrist Wearable Device*, 18 EUR. J. CULTURAL STUD. 479, 486 (2015).

173. Begley, *supra* note 172.

174. Most users wear fitness trackers on their wrist, and the trackers use accelerometers to measure motion. Some inherent flaws are that the accelerometers measure only motion, not exertion, and that some of "today's wrist-worn accelerometers are still calibrated for steps." Albert Sun & Alastair Dant, *What Your Activity Tracker Sees and Doesn't See*, N.Y. TIMES (Mar. 11, 2014), https://www.nytimes.com/interactive/projects/well/2014/03/accelerometers.html [https://perma.cc/2ZZF-EEGG]. This means that the trackers cannot tell when an individual is cycling and thus will not count that as physical activity. *See id.*

175. *See* Hannah Augur, *The Physician and the Fitbit: Why Doctors and Administrators Don't Love Wearables*, DATACONOMY (Mar. 29, 2016), http://dataconomy.com/the-physician-and-the-fitbit-why-doctors-and-administrators-dont-love-wearables-2 [https://perma.cc/5QMB-TUTN].

176. Many wellness programs use body mass index (BMI) as a metric to determine obesity. However, current medical research shows that this is an inaccurate metric since BMI does not distinguish between fat mass and muscle mass. *See* Alban De Schutter, et al., *Body Composition and Mortality in a Large Cohort with Preserved Ejection Fraction: Untangling the Obesity Paradox*, 89 MAYO CLINIC PROC. 1072, 1077 (2014). *See also* Albert Sun, *Same B.M.I., Very Different Beach Body*, N.Y. TIMES (Sept. 3, 2015), http://www.nytimes.com/interactive/projects/cp/summer-of-science-2015/latest/bmi?smid=tw-nytimes [https://perma.cc/8JT3-77C6].

177. *See* Kate Crawford, *When Fitbit is the Expert Witness*, ATLANTIC (Nov. 19, 2014), http://www.theatlantic.com/technology/archive/2014/11/when-fitbit-is-the-expert-witness/382936 [https://perma.cc/283Z-LEZE].

employer may access the data from such devices at any time without permission from the employee.[178] This raises concerns about the privacy of the electronic data collected from employees who choose to participate in wellness programs.

2. Issues of Employment Discrimination

In addition to the potential for invasion of privacy, the collection of personal health information for wellness programs implicates the potential for employment discrimination. However, traditional anti-discrimination laws such as Title VII of the Civil Rights Act of 1964 or the ADA typically do not address issues of discrimination arising from wellness programs. Instead, the issues go beyond race, gender, pregnancy, age, or even genetic discrimination. The two most significant categories of discrimination implicated in wellness programs are weight and smoking.

In the United States, more than two-thirds of adults are considered overweight, and of that group, more than one-third of adults are considered obese.[179] The law is not well-settled on whether obesity is a "disability" for purposes of the ADA, such that obese people would be a special class protected from losing their jobs because of their weight. Some jurisdictions do not consider obesity as a disability, while others define obesity as a disability only when its severity impacts activities of daily living.[180] The practical effect of the latter definition is that protective federal law generally only includes the morbidly obese and excludes the moderately obese,[181] who nonetheless have increased risks of certain chronic disease and whom an employer might view as an increased healthcare cost. Given the uncertain legal landscape, obese workers may be wary of joining a wellness program for fear of losing their jobs.

Smokers also lack legal protections against discrimination. There is no federal law protecting a smoker from employment discrimination. In nine states, an employer may legally fire an employee for smoking, even if the smoking occurs outside of the workplace.[182] Given this lack of protection and

178. According to Marc Smith, a sociologist with the Social Media Research Foundation, "Anything you do with a piece of hardware that's provided to you by the employer, every keystroke, is the property of the employer. Personal calls, private photos—if you put it on the company laptop, your company owns it. They may analyze any electronic record at any time for any purpose. It's not your data." Kaplan, *supra* note 27, at 32.

179. *See* NAT'L INSTS. OF HEALTH, NAT'L INST. OF DIABETES & DIGESTIVE & KIDNEY DISEASES, OVERWEIGHT AND OBESITY STATISTICS (2012), https://www.niddk.nih.gov/health-information/health-statistics/Pages/overweight-obesity-statistics.aspx [https://perma.cc/R9Q4-YTVY].

180. *See* Jessica L. Roberts, *Healthism and the Law of Employment Discrimination*, 99 IOWA L. REV. 571, 594–600 (2014) (providing a detailed explanation of jurisdiction splits and shifts in the interpretation of such laws like the ADA when it comes to coverage of the obese).

181. *Id.*

182. *See supra* Part II(B)(2) (chart titled: "States where an employee could be fired for being a smoker").

risk of dismissal, smokers may be hesitant to join the smoking cessation programs offered by many corporations.

The EEOC recently brought three cases based on its suspicions that employers used corporate wellness programs as backdoors to employment discrimination. First, in *E.E.O.C. v. Orion Energy Systems*, after an employee objected to and declined to participate in the Orion's wellness program, "she was required to pay the entire premium cost for single coverage for her health benefit."[183] Orion otherwise paid the entire amount of the health insurance premiums for employees who participated in the wellness program.[184]The case is currently pending.

Second, in *E.E.O.C. v. Flambeau*, *Inc.*, the EEOC alleged that Flambeau's requirement that employees participate in its wellness program or face termination of their health insurance violated the ADA.[185] According to the complaint, Flambeau cancelled an employee's health insurance because he did not complete the biometric testing and health risk assessment mandated by Flambeau's wellness program, leaving him only with the option of fully paying for his own health insurance.[186] If the employee had completed the biometric testing and health risk assessment, Flambeau would have covered about 75 percent of his health insurance premiums.[187]

The EEOC's contention that the Orion and Flambeau wellness programs violated the ADA stems from the ADA's prohibition on asking employees disability-related questions or requiring employees to submit to medical examinations, unless those questions or examinations are job-related and consistent with business necessity.[188] Wellness programs may include disability-related inquiries and medical examinations if the program is "voluntary," and if employee medical information is kept confidential.[189] The question arising from the Orion and Flambeau cases is whether the penalty exacted on employees—paying the full health insurance premium—belies the "voluntariness" of the wellness program. The EEOC has defined a "voluntary" wellness program as one in which the employer neither requires participation nor penalizes employees for declining participation in the program.[190] But, the EEOC has not yet taken a formal position on what amounts to a penalty.

---

183. *See* Complaint ¶ 16, EEOC v. Orion Energy Sys. (E.D. Wis. 2016) (No. 1:14-cv-01019-WCG), 2014 WL 4180675, at *1.

184. *See id.*

185. EEOC Opening Brief at 4–7, 9–10, EEOC v. Flambeau, Inc., 131 F.Supp.3d 849 (W.D. Wis. 2014) (No. 16-1402).

186. *Id.*

187. *Id.*

188. *Id.*

189. *See id.*; Complaint ¶ 11, EEOC v. Flambeau, Inc., 131 F.Supp.3d 849 (W.D. Wis. 2014) (No. 3:14-cv-00638-bbc).

190. *See* EEOC Regulations Under the Americans with Disabilities Act, 29 C.F.R. § 1630 (2016) (final rule on employer wellness programs and Title I of the ADA).

In the third case, *E.E.O.C. v. Honeywell Int'l, Inc.*, the EEOC asserted that penalties levied against employees for not participating in wellness programs contravene the mandated voluntary nature of wellness programs:

> "The EEOC seeks to immediately enjoin Honeywell from levying all penalties and costs—including withholding Health Savings Account ("HSA") contributions—against any Honeywell employee who refuses to undergo biomedical testing in conjunction with Honeywell's corporate wellness program. The EEOC does not allege that Honeywell's wellness program violates employees' right to privacy in their medical information, nor does the EEOC request that the Court order Honeywell to cease the biometric testing associated with its wellness program."[191]

B. Productivity Apps

Productivity apps have been touted as workplace technology that will revolutionize management and lead to greater efficiency in the workplace. The "gamification of performance management" in today's workforce is represented by an $11 billion industry that "includes workforce-management systems such as" CornerStone, OnDemand, BetterWorks, and Kronos "and 'enterprise social' platforms such as Microsoft's Yammer, Sales-force's Chatter, and, soon, Facebook at Work."[192]

However, it is important to consider that the very nature of apps—as electronic programs that can tirelessly monitor an employee, twenty-four hours a day, seven days a week (an impossible feat for a human supervisor)—makes these programs well-suited for limitless worker surveillance. Consider the case of the Xora app. A mid-level executive in California brought suit against her employer who, she alleged, dismissed her for uninstalling an app from her company-issued iPhone that tracked her outside of work and even when she turned the phone off. The plaintiff analogized the app to a prisoner's anklet electronic monitoring device. She also alleged that her employer admitted that he used the device to monitor her driving speed even during non-work hours.[193]

Even with the convenience and perceived accuracy that productivity apps could afford human managers, issues remain as to whether an information asymmetry concomitant with such apps exists, such that users may not actually be consenting to the apps even though they give permission. In addition, it is unclear whether the invasive nature of productivity apps might permanently erode worker privacy. In the era of Big Data,[194] most aspects of human life are

---

191. *See* EEOC v. Honeywell Int'l, Inc., No. 0:14-cv-04517-ADM-TNL, 2014 WL 5795481, at *1 (D. Minn. Nov. 6, 2014).

192. Kaplan, *supra* note 27, at 31; *see also* Dougherty & Hardy, *supra* note 47.

193. Kravets, *supra* note 10.

194. danah boyd and Kate Crawford define Big Data as: "a cultural, technological, and scholarly phenomenon that rests on the interplay of: (1) *Technology*: maximizing computation power and algorithmic accuracy to gather, analyze, link, and compare large data sets. (2) *Analysis*: drawing

deemed quantifiable. The friction arises from Big Data's voracious appetite for data that feeds a surveillance and self-monitoring imperative. The workplace has not escaped this trend toward quantification.

Employer surveillance of workers was borne out of necessity. With increased focus on division of labor, oversight and monitoring became necessary to ensure that employees completed work not only in a timely fashion but also in a manner that met quality standards.[195] Based on time and quality restraints, employers have a clear economic interest in monitoring their employees. Less clear, however, is the permissibility and desirability of employer surveillance on facets of workers' lives previously recognized as personal, autonomous, and private. Advances in technology have enabled and facilitated such encroachment by allowing for even greater electronic monitoring and data gathering.

Start-up companies are continually developing and perfecting new technologies for employer surveillance. For example, BetterWorks makes management software that "blends aspects of social media, fitness tracking and video games" into a program designed to encourage productivity among workers.[196] The software obliges employees to track their progress toward a measurable goal "on a digital dashboard that everyone in their company can see."[197] An employee's progress is represented by a tree that "grows with accomplishments and shrivels with poor productivity."[198] As each employee's quantified productivity is visible to his fellow workers, the program affords co-workers the ability to encourage or shame each other to conform to the desired productivity metrics.

BetterWorks, and apps like it, are prime examples of what Julie Cohen has termed "the surveillance-innovation complex" and what Shoshana Zuboff refers to as "surveillance capitalism."[199] With such apps, "[c]ommercial surveillance environments use techniques of 'gamification' to motivate user participation." The apps recast surveillance "in an unambiguously progressive light" with the conceit that greater monitoring drives innovation and economic growth.[200] This "surveillance-innovation" complex has created "workplace

---

on large data sets to identify patterns in order to make economic, social, technical, and legal claims. (3) *Mythology*: the widespread belief that large data sets offer a higher form of intelligence and knowledge that can generate insights that were previously impossible, with the aura of truth, objectivity, and accuracy." *See* danah boyd & Kate Crawford, *Critical Questions for Big Data*, 15 INFO. COMM. & SOC'Y 662, 663 (2012).

195. *See, generally*, Émile DURKHEIM, THE DIVISION OF LABOUR IN SOCIETY (1893).

196. Dougherty & Hardy, *supra* note 47.

197. *Id.*

198. *Id.*

199. Shoshana Zuboff, *Big Other: Surveillance Capitalism and the Prospects of an Information Civilization*, 30 J. INFO. TECH. 75, 89 (2015).

200. Cohen, *supra* note 13, at 207.

science," an academic inquiry into how workers should be managed.[201] This emerging field is comprised of data analysis injected into the field of human resource management. It eschews "gut feel and established practice" in favor of Big Data to "guide hiring, promotion and career planning."[202]

Proponents of workplace science couch the heightened surveillance it requires as unremarkable apart from its capacity to obtain information of immense utility for the greater good of the company. One industry insider notes: "Today, every e-mail, instant message, phone call, line of written code and mouse-click leaves a digital signal. These patterns can now be inexpensively collected and mined for insights into how people work and communicate, potentially opening doors to more efficiency and innovation within companies."[203] Such discourse fails to consider privacy implications, and also promotes the ideology that Big Data mined from workers invariably leads to innovation and efficiency. This rhetoric also "advance[s] the instrumental goal of holding the regulatory state at arm's length."[204] If the only remarkable consequence of this data mining of workers' daily lives is economic growth, then there is nothing left for the political economy to concern itself with, apart from encouraging and enabling such data mining.

While some may claim that work science is merely another iteration in a long history of academic study with the unabashed goal of promoting worker efficiency and productivity, work science differs in paradigm and practice from its antecedents in ways that hold disconcerting implications for worker privacy and employability. Louis Brandeis popularized the term "scientific management" in 1910.[205] Frederick Winslow Taylor adopted the term in the 1880s and 1890s. Taylor's theory of management analyzed workflows with the primary goal of improving economic efficiency and labor productivity. This combination came to be known as a subset of scientific management.[206] Taylorism (also known as "scientific management") focused on mastering the job or task by breaking it down into discrete components that could be studied for efficiency. By contrast, the focus of workforce science has shifted to the individual worker. As a result, management is now more concerned with physically mastering the individual worker or, better yet, inducing the worker to self-mastery in a manner that benefits the company.[207]

---

201. Steve Lohr, *Big Data, Trying to Build Better Workers*, N.Y. TIMES (April 20, 2013), http://www.nytimes.com/2013/04/21/technology/big-data-trying-to-build-better-workers.html [https://perma.cc/J5PA-XD9W].

202. *Id.*

203. *Id.*

204. Cohen, *supra* note 13, at 207.

205. HORACE BOOKWALTER DRURY, SCIENTIFIC MANAGEMENT: A HISTORY AND CRITICISM 15–21 (Colum. Univ. 2d ed. 1918) (1915).

206. *Id.*

207. *See* FREDERICK WINSLOW TAYLOR, THE PRINCIPLES OF SCIENTIFIC MANAGEMENT 11–13 (1911).

1. Issues of Privacy and 24/7 monitoring

Not content with merely inducing self-mastery, firms seek to be omnipresent in workers' lives. Unlike other forms of surveillance, productivity apps possess the potential for uninterrupted monitoring of workers' lives. As the Xora case demonstrates, productivity apps may be switched on without a worker's knowledge. Thus, productivity apps could represent entry points for the employer to violate the privacy of workers by tracking their movements outside of work.

2. Monitoring as Pretext for Employment Discrimination

Because the data from electronic wearables have proven unreliable and irregular, we do not trust that the data from productivity apps will always provide a true picture of productivity. We also do not trust that the chain of custody for such data is adequate to maintain fairness. Rather, there is a worry that the data from productivity apps could be manipulated or interpreted in such a way as to serve the ends of discrimination against individuals that are members of protected classes.

IV.
SOLUTIONS TO PROTECT WORKER PRIVACY

Solutions to limitless worker surveillance are not easy to design; however, they are possible. The challenge for their design lies in reestablishing the power balance between the information domains of employers and workers. As long as work-related information remains in the domain of the employer—be it one's wellness, location, or conduct away from the office—few laws or regulations will survive the accelerating technological advances in sensors and surveillance. Instead, we must think of information about workers as multi-dimensional, touching many contexts and domains of an individual's life simultaneously, including time, location, privacy, and physicality. When those domains contain sensitive categories of data, such as health, the law must intervene to prevent workplace justifications from overriding individual privacy protections. In many ways, this is what GINA sought to accomplish for the narrow domain of genetic information.[208]

With these conditions in mind, we consider three possible approaches: (1) a comprehensive omnibus federal information privacy law, similar to approaches taken in the European Union, which would protect all individual privacy to various degrees regardless of whether or not one is at work or elsewhere and without regard to the sensitivity of the data at issue; (2) a narrower, sector-specific Employee Privacy Protection Act (EPPA), which

208. *See* Ifeoma Ajunwa, *Genetic Data and Civil Rights*, 51 HARV. C.R.-C.L. L. REV. 75, 100–07 (2016) (arguing that GINA be strengthened with a disparate impact clause as GINA represents a civil rights legislative scheme to prevent all manner of genetic discrimination in the workplace).

would focus on prohibiting specific workplace surveillance practices that extend outside of work-related locations or activities; and (3) an even narrower sector and sensitivity-specific Employee Health Information Privacy Act (EHIPA), which would protect the most sensitive type of employee data, especially those that could arguably fall outside of HIPAA's jurisdiction,[209] such as wellness and other data related to health and one's personhood. We discuss each in turn below.

A. A Comprehensive Approach: Omnibus Federal Information Privacy

Proposals for omnibus federal information privacy laws are nothing new.[210] The European Union's Data Directive has long served as a model for this approach; it empowers the European Data Protection Supervisor, individual National Data Protection Authorities (NDPAs), and various citizens and civil society groups to enforce violations of personal data protection.[211] Recently, the European Commission announced it is considering an even stronger General Data Protection Regulation[212] that would place more power in the hands of NDPAs to enforce general privacy violations.[213]

While there is much appeal to this approach as a general panacea for privacy concerns writ large, it suffers from several weaknesses as a solution to the limitless worker surveillance problem. First, because omnibus approaches intentionally provide broad coverage for all data in all situations, they cede power to standard notice-and-consent mechanisms whereby data collectors and

---

209. HIPAA has jurisdiction over health information handled by health care providers. The law is not settled on whether wellness program vendors fall within that category. The U.S. Department of Health and Human Services provides an explanation regarding which entities are covered under HIPAA and that list does not explicitly include wellness programs: "The HIPAA Privacy Rule establishes national standards to protect individuals' medical records and other personal health information and applies to *health plans, health care clearinghouses*, and those *health care providers* that conduct certain health care transactions electronically." *See* The HIPPA Privacy Rule, U.S. DEP'T OF HEALTH AND HUMAN SERVS., (emphasis added) https://www.hhs.gov/hipaa/for-professionals/privacy/index.html?language=es [https://perma.cc/9BQ4-E3RW].

210. *See* Scot Ganow & Sam S. Han, *Model Omnibus Privacy Statute*, 35 U. DAYTON L. REV. 345 (2010); *see also* Wilborn, *supra* note 123, at 862 ("One of the more extreme proposals suggested to solve the problem of employee privacy, at least with respect to electronic monitoring and surveillance, has been Professor Laurence Tribe's proposal of a Twenty-Seventh Amendment to the United States Constitution"); Henry Weinstein, *Amendment on Computer Privacy Urged*, L.A. TIMES (Mar. 27, 1991), http://articles.latimes.com/1991-03-27/news/mn-938_1_constitutional-amendment [https://perma.cc/PYT6-JDRG].

211. *See, e.g.*, *Protection of Personal Data*, EUR. COMM'N (July 24, 2016), http://ec.europa.eu/justice/data-protection [https://perma.cc/3Q7V-Z3AU].

212. *See* Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, 2016 O.J. (L 119) 1.

213. *See* European Council Doc. No. 9565/15, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data—Preparation of a general approach, at 8 (June 11, 2015), http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf [https://perma.cc/HAJ9-ZLZ3].

processors seek consent for specific uses of data.[214] In the United States, such an omnibus protection would represent a pyrrhic victory. In the context of at-will employment—where there is asymmetrical bargaining power between the worker and the employer—standard notice and consent mechanisms would merely serve as a sanitizing seal of approval for employer surveillance; there would be no real chance for dispute by the employee. The occasional "OccupEye" public incident aside, most employees cannot parse each employer surveillance and technology in order to negotiate consent. Omnibus protection both individually and collectively pits those with the least power (employees) against those with the most (employers). Therefore, such employee consent is essentially ceremonial with no space for true negotiation.

Second, limiting data collection to work-related purposes "will not mitigate the dangers of limitless worker surveillance. Employers could simply continue to define the purpose of their surveillance in the context of the employer-employee relationship, and define the information domain as "work-related."[215] Thus, the employer could potentially offer the pretext of improving worker productivity as justification for *any* surveillance, thereby enabling limitless worker surveillance.

Third, as Paul Schwartz notes, omnibus privacy approaches tend to define privacy at the lowest common denominator level because the definition must work for all individuals and for all kinds of data.[216] In the particular context of employee data, especially data involving wellness, health, and personhood, there are unique concerns which require specific attention in order for employees to retain their privacy rights. Such concerns are better addressed by a regime with a narrower and more robust approach.[217]

B. A Sector-Specific Approach: The Employee Privacy Protection Act

More promising than an omnibus law would be a sector-specific approach that narrows the context and focus of the law to the particular employer-employee relationship, recognizing the power differential between the parties and the problematic frame of employment/workplace data. A hypothetical "Employee Privacy Protection Act" (EPPA) could specifically limit workplace surveillance to its appropriate context—actual workplaces and actual work tasks. It would explicitly prohibit surveillance outside the workplace both in terms of physical location privacy and activity privacy. Such a boundary could not be breached simply through notice-and-consent mechanisms. Much like other worker protection laws, such as those providing for minimum wage,

214. *See, e.g.*, *id.*

215. Much as *The Daily Telegraph* defined the OccupEye installation as related to workplace environmental and climate control purposes.

216. Paul M. Schwartz, *Preemption and Privacy*, 118 YALE L.J. 902 (2009) (arguing that there are benefits to a sector-specific approach to privacy over an omnibus approach).

217. *See* HELEN NISSENBAUM, PRIVACY IN CONTEXT (2010).

overtime pay, and safe working conditions, the EPPA would serve as a general protection for all workers that could not be waived. The EPPA would also prohibit productivity apps from monitoring employees when they are off-duty, notwithstanding any insistence on monitoring as a condition of employment.

Critics of such a proposal may argue, of course, that prohibitions on notice-and-consent mechanisms are antithetical to "freedom to contract" principles and would limit the opportunity for technological innovation to benefit work and the labor economy. However, a bedrock contract principle provides that undue influence negates the required intent to contract. And technological innovations would still be available to the worker through third party products and services, but not at the insistence or undue influence of the employer. The use of such data would therefore shift from favoring the employer to favoring the employee and allow for employee autonomy over his or her own data. Data autonomy would no longer suffer vulnerability as a condition of employment, nor as part of an employer's capital to be capriciously withheld or magnanimously granted to the employee. Instead, this narrower approach recognizes data autonomy as an essential human right, and one that is part and parcel of the guarantee of an individual's right to make a livelihood. Such a shift moves the data from the domain and context of the "workplace" to one of personhood.

C. A Sector and Sensitivity-Specific Approach: The Employee Health Information Privacy Act

An even narrower approach would be to further limit worker privacy protections to specific types of sensitive data, such as data related to autonomy and physicality.[218] Although employees at *The Daily Telegraph* jocularly referred to the OccupEye device as a monitor for bathroom breaks, worker surveillance does often focus on the physicality of workers, placing them in extremely vulnerable positions vis-à-vis their employers. This is particularly true when employers use health and wellness programs as proxies for worker surveillance. To guard against such efforts to undermine worker autonomy and privacy, a third approach would be to enact the Employee Health Information Privacy Act (EHIPA). The Act would clarify that health information generated through any program, including third party wellness programs, or device connected to one's employment is protected information under existing health privacy laws, such as HIPAA.

The EHIPA would also mandate strong rules regarding both employer and vendor access to health data collected from fitness devices distributed as part of wellness programs. Pursuant to the EHIPA, such data could not be sold without the permission of the employee, and the employee would have the right to

218. *See generally* Paul Ohm, *Sensitive Information*, 88 S. CAL. L. REV. 1125 (2015) (theorizing that certain types of information should be considered sensitive information because they represent significant risk of privacy harm).

request the destruction of the data record once her employment terminated. This would bring all information relating to the physicality of workers (with the exception of genetic information, which enjoys even greater protection under GINA) under the same standard and would not allow proxies or end-runs such as those in wellness programs to proliferate.[219] A system such as EHIPA would also benefit from the experience that employers have with well-developed laws such as HIPAA. Such a law would also anticipate innovations in physical sensors—like the Apple Watch, Microsoft Band, or Fitbit—and allow for their evolution without the need to revisit privacy rules as relating to potentially sensitive worker information.

CONCLUSION

While many view accelerations in worker surveillance innovation and technological advancements as auguring well for worker productivity and the efficacy of remote management,[220] those same innovations have decimated worker privacy. Innovations in wearable technology, for instance, have created an all-seeing Argos Panoptes, albeit one that seduces us with its novelty and distracts us from its surveillance aspects with a user-friendly interface. When we consider privacy invasions only in terms of the harms that accompany them, we neglect the fact that diminished privacy for workers represents a harm in and of itself. The freedom to safeguard one's private time and personal life should not be deemed an economic good that may be exchanged for the benefit of employment. While employers have a reasonable interest in ensuring the worker productivity and in dissuading misconduct in the workplace, that interest does not outweigh the human right to privacy and personal liberty in domains that have been traditionally considered separate from work and the workplace.

219. Nicolas Terry, *Big Data Proxies and Health Privacy Exceptionalism*, 24 HEALTH MATRIX 65–108 (2014).

220. *But see generally* Ethan Bernstein, *Making Transparency Transparent: The Evolution of Observation in Management Theory*, 11 ACAD. MGMT. ANNALS 217 (2017) (concluding that more surveillance may actually lead to less knowledge and control).