LIMITLESS WORKER SURVEILLANCE

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

ABSTRACT

From the Pinkerton private detectives of the 1850s, to the closed-circuit cameras and email monitoring of the 1990s, to contemporary apps that quantify the productivity of workers, American employers have increasingly sought to track the activities of their employees. 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 – data analytics, communications capture, mobile device design, DNA testing, and biometrics – have dramatically expanded capacities for worker surveillance both on and off the job. At the same time, the cost of many forms of surveillance has dropped significantly, while new technologies make the surveillance of workers even more convenient and accessible. This raises the question of whether the law is a meaningful avenue to delineate boundaries for worker surveillance.

In this Article, we examine the effectiveness of the law as a check on 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 then propose three possible frameworks for worker privacy protections designed to withstand current and future trends in this arena.

[*] Assistant Professor of Law, University of the District of Columbia, David A. Clarke School of Law, Ph.D., Columbia University. Fellow, Berkman Klein Center at Harvard
[*] 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. The authors wish to thank the attendees of the 2016 Privacy Law Scholars Conference at George Washington University and those at the 2016 Law and Society Association Conference in New Orleans. Special thanks to Professors Frank Pasquale, Andrew G. Ferguson, and Alvaro Bedoya. We also thank Microsoft Research New York for funding Prof. Ajunwa's initial research on these topics.

TABLE OF CONTENTS

1. 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 labelled "OccupEye" attached to the underside of every desk.[1] Unannounced by management, the devices were part of a system of "automated workspace utilization analysis" designed to track the motion and heat of individual employees and provide detailed metrics on worker attendance.[2] Initially justified as an effort to gather data on energy efficiency and promote environmental sustainability, the 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] Yet while 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.

This failure is no mistake. 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 but not limited to massive efforts through warfare, slavery, globalization, and other forms of colonialism to control and exploit workers. Yet, less examined is the role of surveillance innovation itself on the workplace and the corresponding weakness of legal protections for those subjected to it.

Take for example what occurred in February of 1855, when Allan Pinkerton walked into a Chicago Masonic Hall to meet with attorney Edward Rucker. The two men sat down and discussed a problem that businesses were increasingly struggling with – the need for greater control over their employees, both inside and outside of work hours and locations. Pinkerton had consulted with numerous commercial interests, including six Midwestern railroad companies, and confirmed that a viable venture in this arena was possible. The two men decided then and there to form the

[1] http://www.buzzfeed.com/jimwaterson/telegraph-workplace-sensors#.qbW9zg7GG.
[2] *Id*.
[3] *Id*. (noting that once discovered, Telegraph employees immediately saw the monitoring devices as surveillance apparati, with one commenting: "Never before has taking a shit on company time felt so rebellious.").

North-Western Police Agency, later known as the Pinkerton National Detective Agency. 'The Pinkertons' (as the agents were called) served a variety of roles for employers – infiltrating and busting unions, enforcing rules, and effectuating the constant monitoring of workers that were deemed a threat to the interests of employers.[4] With the incorporation of the Agency, a new form of worker surveillance came into being, one that 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.

Today, despite the success of the Pinkertons and their antecedents, surveillance innovations are enabling employers to rely less and less on human agents to accomplish the surveillance[5] of their employees. Rather, technologies, both digital and otherwise, have become the primary tools of employee monitoring.[6] For example, earlier this year, 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.[7] In another recent case, characterized as "the mystery of the devious defecator" by US District Court judge Amy Totenberg, an employer was ordered to pay two employees $2.2 million in damages for demanding DNA samples from its employees for genetic testing after some fecal matter was discovered in the workplace.[8]

The technological monitoring of employees by employers has moved in lockstep with the advancement of technological capacities. Beginning

---

[4] Frank Morn, THE EYE THAT NEVER SLEEPS: A HISTORY OF THE PINKERTON NATIONAL DETECTIVE AGENCY at 18. Bloomington: Indiana University Press (1982).

[5] 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 and whether those actions are benign or not is both a matter of interpretation and of effect. Throughout the article, we use "monitoring" and "surveillance" interchangeably. *See*, PHILIP E. AGRE, SURVEILLANCE AND CAPTURE: TWO MODELS OF PRIVACY INFORMATION SOCIETY 10, NO. 2 (1994). *But see also*, JAMES BARKER & GRAHAM, SEWELL, COERCION VERSUS CARE: USING IRONY TO MAKE SENSE OF ORGANIZATIONAL SURVEILLANCE ACADEMY OF MANAGEMENT REVIEW 31, NO. 4 (2006).

[6] 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).

[7] David Kravets, *Worker Fired for Disabling GPS App that Tracked her 24 hours a Day*, ARSTECHNICA (May 11, 2015), http://arstechnica.com/tech-policy/2015/05/worker-fired-for-disabling-gps-app-that-tracked-her-24-hours-a-day/.

[8] 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.

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 the rapid technological advancements and diminishing costs now mean employee surveillance occurs both inside and outside the workplace – bleeding into the private lives of employees. Employers have also shifted their investments in certain technologies and practices in light of the legal frameworks that constrain them, or lack there of, resulting in a shift from the focus on collecting personally-identifying information and other protected data such as health records to the wholesale acquisition of unprotected and largely unregulated proxies and metadata such as wellness information, search queries, social media activity and the outputs of predictive 'big data' analytics.[9]

To capture the new privacy and discrimination issues arising in the context of workplace surveillance, this Article provides an overview of technological advancements in worker surveillance with a focused discussion on two arenas of recent expansion: 1) workplace wellness programs and 2) work productivity applications (apps). This Article then details the relevant extant spectrum of legal limitations on workplace surveillance and examines concerns about liminal spaces in the law. In the final section, we consider three possible solutions to address these concerns: (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 fall outside of HIPAA's jurisdiction, such as wellness and other data related to health and one's personhood.

[9] See Kate Crawford and Jason Schultz, *Big Data and Due Process: toward a Framework to redress Predictive Privacy Harms*, 55 BOSTON COLLEGE L. REV. 1 (2014) (noting 'predictive privacy harms').

I. WORKER SURVEILLANCE: A BRIEF HISTORY

In this section, we discuss some of the history and ethical debate of 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, and the effects of the changing nature of work on the employer's incentive and motivation to more closely surveil its workers.

A. Technological and Economic Limits on Worker Surveillance

The effects of electronic surveillance in the workplace has been debated for decades but that debate came to a significant crossroads in the 1980s, when the U.S. Office of Technology Assessment (OTA) published *The Electronic Supervisor: New Technologies, New Tensions*, a report which synthesized economic, political, sociological and psychological perspectives on workplace surveillance.[10] The report found that advances in computer monitoring have raised questions about fairness and privacy in regards to employer surveillance of employees. The report generally noted that because of declines in unionization, employees had little power to object to what they considered "unfair or abusive monitoring." Furthermore, although some employees reported feeling "stress" as a result of constant monitoring, the report noted that there is no legal requirement that employer monitoring be fair.[11]

While the OTA report found that unionization could provide some protections for workers against invasive worker surveillance, such protection was limited because the report found that "less than 20 percent of the office work force is unionized, and even where unions are involved, their effectiveness has been limited because technology choice and productivity measurement are often considered "management rights" under the contract."[12] By 2016, that number had fallen even further to just 11.1 percent of American workers belonging to a union.[13]

In the following subsections, we discuss the former technological and economic barriers to worker surveillance and how these have been eroded

[10] Kirstie Ball, *Workplace Surveillance: An Overview*, LABOR HISTORY, 51:1 (2010).
[11] OTA report summary: https://www.princeton.edu/~ota/disk2/1987/8708_n.html
[12] Id.
[13] United States Bureau of Labor and Statistics, http://www.bls.gov/news.release/pdf/union2.pdf

by technological advancements that make worker monitoring both more effortless and inexpensive.

1. Historic Technological and Economic Limits

As early monitoring of employees had to be conducted by human supervisors, this meant that there were both economic and technological limits to the monitoring of workers. In the early twentieth century, Henry Ford stalked the factory floor with a stopwatch, timing his workers' motions in a push for higher efficiency.[14] 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. 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."[15] Ford's Sociological Department was charged with surveilling the private lives of Ford's employees.[16] Inspectors were sent to their homes to interrogate them about their marital lives and their finances to see if they were worthy enough to work for Ford. As some have observer, "it seems amazing that people would tolerate such interrogation, but their jobs depended on it."[17] This genre of dictatorial worker surveillance is, however, not relegated to the history books. Similarly, Walmart, Inc. has been criticized for union-busting strategies that it has adopted since its inception in the 1960s, and workers fear for their jobs if they dare to dissent.[18]

Yet, neither Ford nor his investigators could be all places at once. It was not humanly possible to maintain 24/7 monitoring of workers without the aid of technologies that have become ubiquitous in the twenty-first century. 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 to remote technologies that could continue to surveil his workers after hours, and he did not have the highly accessible genetic testing that was developed in the 1990s which can now detect which worker has a higher than usual propensity for a particular disease.

---

[14] Richard Snow, I Invented the Modern Age: The Rise of Henry Ford 204-05 (Scribner 2013).
[15] Richard Snow, I Invented the Modern Age: The Rise of Henry Ford 204-05 (Scribner 2013).
[16] 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.
[17] Id.
[18] http://www.bloomberg.com/features/2015-walmart-union-surveillance/

Even for one of America's capitalist titans, the cost of such surveillance would have been insurmountable.

2. The Rapid Evolution of Technological and Economic Limits

Technological advancements have made worker monitoring much more easily accomplished and also much less costly. In the 1980s, CCTV cameras, microphones and computer programs quickly displaced human managers and investigators. The rapid erosion of technological and economic constraints on employee surveillance magnified the invasiveness of these 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.

For example, punch clocks have given way to thumb scans,[19] key cards may soon give way to RFID tags, and internet browser histories are often scrutinized closely. Some employers log keystrokes and many are interested in capturing not only when their employees use private services like Gmail, Facebook, and Twitter, but what they publish there as well.[20] Employer-provided cellphones, an increasingly ubiquitous piece of worker equipment now offers employers the ability to pinpoint the worker's precise location through GPS**.** [21]

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.[22] Amazon, perhaps the largest retailer in America, requires their workers to carry electronic tablets that record both 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 are washing their hands.[23] As summed up by Ellen Bayer of the American Management Association: "Privacy in today's workplace is largely illusory."[24] Furthermore, many workers may be unaware of the extent to which their employer is tracking them; only two states, Delaware

[19] Esther Kaplan, *The Spy Who Fired Me*, HARPER'S MAGAZINE, March 2015, at 31.
[20] *The Rise Workplace Spying*, THE WEEK (July 15, 2015), http://theweek.com/articles/564263/rise-workplace-spying.
[21] *Id*.
[22] *Id*.
[23] *Id*.
[24] *Id*.

and Connecticut, mandate that employers must inform their employees of electronic tracking.[25]

It is important to note that these new privacy invasions are usually accompanied by the justification that such collection of data serves the employer's business interest of improving efficiency and innovation. For example, Boston-based analytics firm Sociometric Solutions has developed employee ID badges fitted with microphone, location sensor, and accelerometer and it is testing the badges in 20 companies. Sociometric Solutions claims that it doesn't record conversations or provide employers with individuals' data. Instead, Sociometric's stated goal is to discover how employee interactions affect the employee's performance.[26] 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 they wish.

Take as another example, UPS's surveillance program. In 2009, UPS fitted its delivery trucks with about 200 sensors that measure all sorts of activities from driving speeds to stop times. This allowed the firm to find out which drivers were taking unauthorized breaks, and to determine how many deliveries could be squeezed into one day. Within four years, the company was handling 1.4 million additional packages a day with 1,000 fewer drivers.[27]

But even as the higher efficiency gains of the surveillance of workers are touted, what is left unsaid is the cost to workers. The demand to meet electronically monitored goals means that workers take risks and push themselves physically in ways that result in more injuries.[28] While it is well established that lack of transparency and inadequate monitoring can result in organizational deviance and misconduct,[29] the converse is also true. Too much monitoring creates stress, fear and incentives to "beat the

---

[25] Esther Kaplan, *The Spy Who Fired Me*, HARPER'S MAGAZINE, March 2015, at 31.
[26] *The Rise Workplace Spying*, THE WEEK (July 15, 2015), http://theweek.com/articles/564263/rise-workplace-spying.
[27] Esther Kaplan, *The Spy Who Fired Me*, HARPER'S MAGAZINE, March 2015, at 31.
[28] 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." Esther Kaplan, *The Spy Who Fired Me*, HARPER'S MAGAZINE, March 2015, at 31.
[29] Ajunwa, Ifeoma, *'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).

system." In the case of UPS workers, the "mental whip" of the telematics system derived from the constant electronic monitoring of the trucks meant that many workers resorted to breaking safety rules that put themselves and others in danger.[30] The sociologist Karen Levy 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 not to take mandated breaks[31] and for the worker to continue working even when sleep was necessary.[32] There is also the question of whether invasive employee surveillance will ultimately lower employee morale and result in higher employee turnover.[33]

Although we have focused on the ways that electronic monitoring presents itself as a tool for increasing productivity, we must also remain cognizant of the fact that the definition of 'productivity' may blur the line between the employee's compensated time on the job and leisure time. Furthermore, we must also question whether the worker is being called upon to surrender more than her labor in exchange for a wage. The figure below shows that worker surveillance is now so pervasive that it goes beyond merely monitoring productivity in the workplace; rather, it now seeks to discover individual behavior and the personal characteristics of workers.

---

[30] "A UPS spokesperson told me that telematics has improved safety over- all 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." Esther Kaplan, *The Spy Who Fired Me*, HARPER'S MAGAZINE, March 2015, at 31.

[31] "Even when drivers are off-duty, employers can see where they are, and can contact them using systems' communication functions—which some- times 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,* 31:2, THE INFORMATION SOCIETY: AN INTERNATIONAL JOURNAL 160, 169 (2015).

[32] "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.*

[33] http://www.nytimes.com/2015/03/16/technology/managers-turn-to-computer-games-aiming-for-more-efficient-employees.html?_r=0.

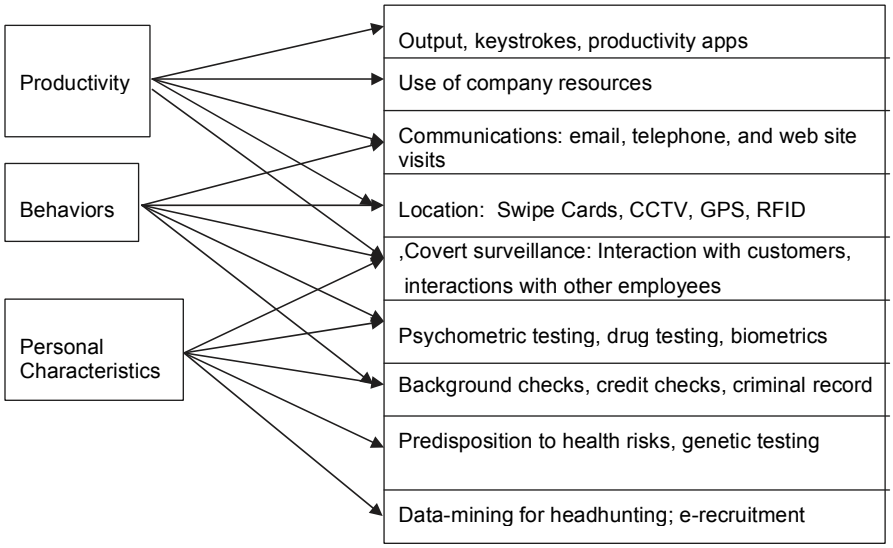

Figure 1: Adapted from Ball, K. (2010). Workplace Surveillance: An Overview

B. The Changing Nature of Work and Its Effects

The changing nature of work in America is a sociological seismic shift that has impacted both the employer and employee roles and as a consequence has influenced greater surveillance in the workplace. Statistics show that working remotely has risen 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.[34] But the percentage of telecommuters that make up the workforce would reveal itself to be even larger if you "include 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."[35]

[34] Alina Tugend, *It's Unclearly Defined, But Telecommuting on the Rise,* N.Y. TIMES (March 7, 2014), http://www.nytimes.com/2014/03/08/your-money/when-working-in-your-pajamas-is-more-productive.html?_r=0.
[35] *Id*.

With all those workers accounted for, the number of Americans who work remotely would reach as high as 30 percent.[36]

Furthermore, a larger number of workers are considered "contract" or "freelance" workers compared to the past. One study estimated that 1 in 3 American worker is a freelance worker.[37] A larger number of workers are also now expected to be on call 24/7.[38] As demand for worker accountability increases, incentives for greater and more intrusive surveillance will grow, particularly when the workers are not within a bounded physical workplace or when there is no opportunity to develop a relationship of trust within a traditional employer-employee relationship.

With the aim of surveilling 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." Some employers even go as far as deploying technology to "instantaneously detect anger, raised voices or children crying in the background on workers' home-office calls."[39]

Monitoring tools are built into freelance work websites like Upwork (formerly ODesk). 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."[40] 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 and check whether their contractors are working. The monitoring is not covert or unobtrusive; rather the clients are alerted by a small computer-screen icon pops up at the bottom of their screen each time a screen shot has been taken.[41] The workers are regularly made aware that they are being observed.

---

[36] *Id*.

[37] Laura Shin, *1 in 3 American Workers Freelances. But Is The Phenomenon Growing?* FORBES (Sept. 8, 2014), http://www.forbes.com/sites/laurashin/2014/09/08/1-in-3-american-workers-freelances-but-is-the-phenomenon-growing/. (citing Sara Horowitz, Freelancing in America, 2015 Report, https://blog.freelancersunion.org/2015/10/01/freelancing-america-2015/).

[38] Illya 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/, *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.

[39] http://www.wsj.com/articles/SB121737022605394845

[40] Id.

[41] Id.

The pressure to monitor workers who are increasingly seen as "independent" and thus further away from direct control also comes from increased fears of corporate and global espionage, especially from sophisticated nation-states. Recently, the U.S. government has stepped up efforts to address economic cybersecurity and federal trade secrecy law intended to specifically address foreign attempts to infiltrate and acquire domestic proprietary information from employers.[42] Many such security programs include ubiquitous worker surveillance mechanisms.

Thus, while there have been rapid technological innovations in scrutinizing and surveilling workers, and political frameworks that justify it, there has been little innovation when it comes to laws offering privacy protections for workers.

II. EXTANT LEGAL PROTECTIONS

There are no general federal laws that expressly address the employer surveillance of workers and that sets limits on how intrusive to privacy such surveillance may become. Rather, the federal laws that have been created for the benefit of workers focus instead on protecting them from employment discrimination while disregarding privacy claims. It is generally understood, for example, that government employees have reduced expectations of privacy at work;[43] that the employee's office or work space is subject to search by the employer without permission,[44] and that any electronic device provided to the employee by the employer, generally remains the property of the employer,[45] meaning that it, too, could be subject to search without permission.[46] The same holds true for employees of private companies where the general principle of "at-will employment" entails that the private companies may demand acquiescence to surveillance as part of the employment bargain.[47] Generally, such private companies provide minimal notice to employees in order justify their surveillance regimes. In practice, what this means, is that most

[42] *See*, Laura K. Donohue, High Technology, Consumer Privacy, and U.S. National Security, 4 Am. U. Bus. L. Rev. 11-48 (2015). http://www.cbsnews.com/news/60-minutes-great-brain-robbery-china-cyber-espionage/. http://thehill.com/opinion/op-ed/267205-pass-the-defend-trade-secrets-act.

[43] *City of Ontario, Cal. v. Quon*, 560 U.S. 746, 756-57 (2010).

[44] *O'Connor v. Ortega,* 480 U.S. 709, 715-16 (1987).

[45] *City of Ontario, Cal. v. Quon*, 560 U.S. 746, 762 (2010).

[46] *Id*. at 761.

[47] Kirstie Ball, *Workplace Surveillance: An Overview*, LABOR HISTORY, 51:1 (2010).

employees should expect that their work mail (both paper and electronic) will be monitored, as well as company-associated social media accounts, company credit cards, company-provided phones, etc.[48] The real debates are now focused on whether personal email, social media, and even devices may be similarly monitored by employers.

In the following subsections, we discuss how some federal laws could be read to afford workers some protection against surveillance. With the illustrative example of laws that protect workers who smoke outside the workplace, we also discuss which states have stronger protections for the privacy of workers versus states with weaker protections.

A. Federal Law

As no federal laws directly address the employer surveillance of workers or sets limits on how intrusive to privacy such surveillance can be, it could be said that under federal law, worker surveillance is limitless. Some might believe that the Electronic Communications Privacy Act of 1986 (ECPA)[49] and the Computer Fraud and Abuse Act (CFAA)[50] would afford employees substantial protection but that belief is erroneous.

The Wiretap Act is Title I of the ECPA and it governs electronic communication in transit,[51] and expressly prohibits the interception of electronic communication without consent.[52] Title II of ECPA is the Stored Communications Act[53], which governs electronic communication

---

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

[49] 18 U.S.C. §§ 2510-22, 2701-12 (2006).

[50] 18 U.S.C. § 1030(A)-(H) (2006).

[51] *See* 18 U.S.C. § 2511 (2006).

[52] 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]. 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."[52] *Id.* at § 2510(1).

[53] *See* 18 U.S.C. § 2701 (2006).

that has already been sent and is in storage.[54] The ECPA's weaknesses to shield employees from employer surveillance derive from the fact that employee consent, even as a condition of employment, effectively waives all of ECPA's protections. As we discuss below, at-will employment makes such consent regimes risible as a protective measure.[55]

The Computer Fraud and Abuse Act (CFAA)[56] is a federal law that prohibits individuals or entities from "knowingly access[ing] a computer without authorization or exceeding authorized access" and thereby obtaining information.[57] 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 in which they are required, employers provide employees with computers, and this means that the employer owns the computer and there is no need for any sort of authorization to access the computer. For personal devices, the employer again could merely obtain access to those devices through the employment agreement.

1. Title VII

Some existing federal laws, designed to protect certain protected groups from discrimination, could potentially be read to also afford protection against certain types of employee surveillance; however as discussed below, we ultimately conclude that these protections are inadequate. Consider, as first example, Title VII, which prohibits

[54] The SCA states that: 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]

[55] *See, Infra,* subsection 3. Note also that at least one court has held that ECPA does not apply to physical monitoring of electronic workplace devices, even when the monitoring results in interception of electronic communications. US. v Ropp, https://scholar.google.com/scholar_case?case=5502061119220003016&hl=en&as_sdt=6&as_vis=1&oi=scholarr.

[56] 18 U.S.C. § 1030 (A)-(H) (2006).

[57] 18 U.S.C. § 1030(a) (2006). 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*. at § 1030(a)(5). Losses under the statute include "any reasonable cost to any victim, including the cost of responding to an offense, conducting any 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*. at § 1030(e)(11).

discrimination based on race, color, religion, sex or national origin.[58] Title VII makes it illegal for employers to discriminate based upon protected characteristics regarding terms, conditions, and privileges of employment. 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.[59]

Thus, for example, if an applicant choses not to identify their religion, Title VII could be read to protect that candidate from surveillance on the part of an employer to determine the candidate's religion. To illustrate, an employer could be lawfully prohibited from surveilling its employees to determine who was praying at break time, who was choosing not to eat pork, who did not drink caffeinated products, or who abstained from other religiously proscribed practices. The argument for this reading would be that 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 (hereinafter "ADA") was enacted to eliminate discriminatory barriers enacted against qualified individuals with disabilities, individuals with a record of a disability, or individuals who are perceived as having a disability.[60] It prohibits discrimination based on a physical or mental handicap and requires employers to make reasonable accommodations for disabled workers. The ADA was enacted by Congress and signed into law by President George H. Bush in 1990, in part, "to provide a clear and comprehensive national mandate for the elimination of discrimination against individuals with disabilities."[61] The term "disability" means, 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.[62] The Americans with Disabilities Act Amendment Act ("ADAAA") broadened the definition of the disabled individual under the ADA such that those

[58] Pub. L. No. 88-352, §703, 78 Stat. 241, 255-57 (1964) (codified at 42 U.S.C. § 2000 e-2 (2006).
[59] *Id*.
[60] *See* U.S. DEPT. OF JUSTICE CIVIL RIGHTS DIVISION, REHABILITATION ACT, http://www.ada.gov/cguide.htm#anchor65610 (last visited Oct. 26, 2015).
[61] 42 U.S.C. § 12101 (b)(1) (2012).
[62] 42 U.S.C. § 12102(1) (2012).

individuals with systemic or cellular level pathologies are covered.[63] 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.[64]

President Franklin Delano Roosevelt is famously known as a public figure that carefully guarded the fact of his disability arising from the poliovirus.[65] What FDR had that few employees do 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." 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 sunlight, or their plates smashed."[66] This stringent policy against photography was accepted as extra-legal, indulged as a *de facto* form of *lèse majesté*. As one correspondent mused: "By what right they do this I don't know," the correspondent wrote, "but I have never seen the right questioned."[67]

Yet, the ADA could potentially be read to afford protection against employee surveillance to discover disability. Much like pursuit of information relating to a protected category under Title VII could be presumed as serving the ends of unlawful employment discrimination, a quest to uncover an employee's private disability could be seen as the preparatory start to employment discrimination. Thus, an employee who finds himself under surveillance for purposes of discovering a disability may have recourse under the ADA.

3. Age Discrimination in Employment Act

Like Title VII, The Age Discrimination in Employment Act (hereinafter "ADEA")[68] was a remedial statute enacted to curb extant age discrimination in employment; therefore the language of the ADEA is

---

[63] Tasneem Dharamsi, *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).
[64] *Id*. at 254-55.
[65] Curtis Roosevelt, *FDR: A Giant Despite His Disability,* N.Y. TIMES (Aug. 5, 1998), http://www.nytimes.com/1998/08/05/opinion/05iht-edcurl.t.html.
[66] Matthew Pressman, *The Myths of FDR's Secret Disability*, TIME (July 12, 2013), http://ideas.time.com/2013/07/12/the-myth-of-fdrs-secret-disability/.
[67] *Id*.
[68] Pub. L. No. 90-202, 81 Stat. 602 (1967) (codified as amended at 29 U.S.C. §§ 621-634).

fairly similar to that of Title VII and the courts look to Title VII cases as authoritative for deciding ADEA cases.[69] The ADEA generally prohibits employment discrimination against individuals who are 40 years old or older.[70] The ADEA also applies to employment agencies[71] and labor organizations, [72] while making an exception for individuals hired or to be hired as firefighters and police officers.[73]

As the ACLU has reported, a growing number of employees are asking prospective employees to provide access to their social media passwords.[74] Access to individual's social media account, such as Facebook, often means gleaning enormous amounts of protected personal information including the individual's age. This could be directly gleaned from the section of the user's profile that allows the individual to list their birth date or it could be deduced from the individual's graduation date from high school, another feature available on Facebook. An argument could be made then, that the ADEA could provide recourse for individuals residing in those states which have not yet passed laws banning employers from requesting social media account passwords from their employees and applicants.[75]

4. The Employment Non-Discrimination Act

President Barack Obama signed an executive order on July 21, 2014 that made the Employment Non-Discrimination Act (ENDA) applicable

[69] *See E.E.O.C. v. Reno*, C.A.11 (Fla.) 1985, 758 F.2d 581, (holding that "because prohibitions of the Age Discrimination in Employment Act were derived in haec verba from Title VII, decisions under analogous section of Title VII were highly relevant to issue, in suit under ADEA, as to personal staff exemption).
[70] See 29 U.S.C. § 631(a)).
[71] 29 U.S.C. § 623 (b).
[72] 29 U.S.C. § 623 (c).
[73] 29 U.S.C. § 623 (j).
[74] *Employers, Schools, and Social Networking Privacy,* ACLU, https://www.aclu.org/employers-schools-and-social-networking-privacy (last visited Oct. 26, 2015).
[75] 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*, GOVTECH http://www.govtech.com/internet/Delaware-Governor-Signs-Internet-Privacy-Safety-Package-into-Law.html (Last Visited OCt. 26, 2015).

law for federal contractors.[76] The president also amended a separate executive order to extend workplace protections to federal government employees. The current version of the bill, which is still under consideration in Congress, prohibits private employers with more than 15 employees from discriminating against applicants or employees on the basis of sexual orientation or gender identity. Religious organizations are provided an exception, broader than that found in the Civil Rights Act of 1964. Non-profit membership-only clubs, except labor unions, are similarly exempt. The president's executive order does not include a religious exemption for federal employees.[77]

The president's executive order could be read to mean that employees of federal contractors could not legally be subjected to surveillance meant to detect either homosexual orientation or biological sex. Contrast this to the case of Castor Semenya. Ms. Semenya is a world champion track runner from South Africa, who was forced to undergo a medical evaluation to determine her biological sex.[78] These tests were prompted by allegations from co-runners that Ms. Semenya was biologically male and thus had an unfair advantage over her female competitors. While there remain debates over whether the increased testosterone bestowed by male sex organs provide an edge to competitors in sporting events, in the context of a white collar office, this law would mean that a federal employee could not be subject to surveillance meant to uncover what gender she was assigned at birth or her sexual orientation. It could also mean, for example, that an employee asserting a right to use a sex-segregated bathroom would not have to submit to surveillance to prove that he had reproductive organs corresponding to the requisite sex.

5. Pregnancy Discrimination Act

The Pregnancy Discrimination Act could similarly afford women some protection against certain types of surveillance in the workplace. The Pregnancy Discrimination Act (PDA) is an amendment to Title VII of the Civil Rights Act of 1964. Discrimination on the basis of pregnancy, childbirth, or related medical conditions constitutes unlawful sex

---

[76] Steve Benen, *Obama Advances Anti-Discrimination Policy with Executive Order,* MSNBC (July 21, 2014), http://www.msnbc.com/rachel-maddow-show/obama-advances-anti-discrimination-policy-executive-order.
[77] *Id*.
[78] *Semenya Told to Take Gender* Test, BBC, (Aug. 19, 2009) http://news.bbc.co.uk/sport2/hi/athletics/8210471.stm.

discrimination under Title VII.[79] 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.[80] Notwithstanding the law, the instances of pregnancy discrimination seem to be on the rise. In 2006, the Equal Employment Opportunity Commission (EEOC) saw nearly 5,000 complaints of pregnancy-based discrimination which represented a 30 percent jump from the previous decade and there were more than 6,000 complaints in 2010.[81]

In recent years several high profile businesswomen have come forward to reveal that they took steps to hide their pregnancies in the workplace. Talia Goldstein, the CEO of a matchmaking startup chose to hide her first pregnancy after an informal survey she took of colleagues in her industry indicated that they would be reluctant to fund a start-up headed by a pregnant CEO. She also described the negative reactions she got from colleagues once she revealed her pregnancy, with several making comments to suggest that she would stop working now that she was pregnant. While Ms. Goldstein eventually told her colleagues about her pregnancy, the PDA could be read to provide an employee protection from surveillance meant to determine her pregnancy status.

6. The Genetic Information Non-Discrimination Act

The Genetic Information Non-Discrimination Act (hereinafter, "GINA") was signed into law by President George Bush in 2008. The law took effect in 2009 and its purpose is to protect Americans from genetic discrimination in healthcare insurance coverage and in employment. GINA remains a primarily administrative law meaning that the Equal

---

[79] THE PREGNANCY DISCRIMINATION ACT, http://www.eeoc.gov/eeoc/publications/fs-preg.cfm (Last Visited Oct. 26, 2015).
[80] *Id*.
[81] Darlena Cuhna, *When Bosses Discriminate Against Pregnant Women*, THE ATLANTIC (Sept. 24, 2014), http://www.theatlantic.com/business/archive/2014/09/when-bosses-discriminate-against-pregnant-women/380623/.

Employment Opportunity Commission (hereinafter "the EEOC") is charged with enforcing it and that administrative procedures with the EEOC must be exhausted before a private plaintiff may bring suit under the auspices of GINA.

The first case to allege a GINA violation was that of Pamela Fink, a resident of Connecticut who was fired from her job allegedly because her choice of a prophylactic double mastectomy had revealed to her employers that she was the carrier of a mutated gene linked to breast cancer (BRCA2).[82] According to Fink, she had been an exemplary employee and she had received her first negative review after her double mastectomy and the day before her reconstructive surgery. The case was later settled out of court for an undisclosed amount.

The "devious defecator" case was a GINA case in which 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 to discover the defecator who was leaving feces around the perimeter of the workplace. The employees alleged that the employer's actions were a violation of GINA. Although that case does not squarely fit into what GINA as an anti-discrimination law was designed to do – which is prevent the non-hiring or dismissal of those discovered to carry a genetic disease, privacy advocates were heartened by the outcome of the case as, not only was this the first GINA case to be brought to trial, it also resulted in a $2.25 million money award. As of this writing, the case has yet to be overturned on appeal.

While GINA ordinarily prohibits employers from collecting genetic information, such as family medical history, through a wellness program, a recent EEOC guideline has reconciled GINA's prohibitions with the government's backing of wellness programs, and has established that the collection of family medical histories as a part of wellness programs will not constitute a violation.[83] This recent ruling is in conflict with the recent pending lawsuits that the EEOC has brought against wellness programs,

---

[82] Emily Friedman, *Pamela Fink Says she was Fired after Getting a Double Mastectomy to Prevent Breast Cancer*, ABC (April 30, 2010), http://abcnews.go.com/Health/OnCallPlusBreastCancerNews/pamela-fink-fired-testing-positive-breast-cancer-gene/story?id=10510163.

[83] "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 USC § 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*, HEALTHAFFAIRSBLOG (May 13, 2015), http://healthaffairs.org/blog/2015/05/13/the-aca-the-ada-and-wellness-program-incentives/.

which it believes has violated both the ADA and GINA Health Information Portability and Accountability Act.[84]

Like GINA, the Health Information Portability and Accountability Act (hereinafter "HIPAA") has been called upon to protect interests that the Act was not necessarily designed to protect. The primary reason for this occurrence is that the general public is under the erroneous impression that HIPAA was designed to protect the privacy interests of patients.[85] The secondary reason being that there is no other federal law that comprehensively protects health information. Yet, we cannot overlook that HIPAA's protection of employer health information is limited.

The most prominent cases brought under HIPAA have involved a disclosure of protected health information by a healthcare provider. Consider that, although HIPAA does not provide a private tort cause of action,[86] the case of *Acosta v. Byrum,*[87] employed HIPAA to establish a tort cause of action for a suit brought in state court regarding the disclosure of electronic medical information.[88] In *Acosta v. Byrum*, the plaintiff, a patient, sued her psychiatrist, among other defendants, for negligent infliction of emotional distress.[89] The patient alleged that the doctor wrongfully allowed an office manager to access her medical records using his medical record access number, and that she suffered severe emotional distress, humiliation, and anguish when the office manager then disclosed her medical records to other parties.[90] In her complaint, the plaintiff asserted that when the psychiatrist provided his medical access code to the office manager, the doctor violated the rules and regulations established by HIPAA.[91] Although she did not assert a HIPAA claim, the plaintiff cited to HIPAA as establishing the appropriate

---

[84] *See, Infra*_____

[85] Many wrongly assume that the "P" in HIPAA stands for "privacy."

[86] *See generally* Jack Brill, *Giving HIPAA Enforcement Room to Grow: Why There Should Not (Yet) Be a Private Cause of Action*, 83 NOTRE DAME L. REV. 2105, 2124–39 (2008) (recommending that no cause of action be added to HIPAA at this time).

[87] 638 S.E.2d 246, 250–52, 254 (N.C. Ct. App. 2006).

[88] *Acosta v. Byrum,* 638 S.E.2d 246, 250–52, 254 (N.C. Ct. App. 2006) (holding 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 and 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).

[89] *Id.* at 249.

[90] *Id.*

[91] *Id.* at 253.

standard of care in her case.[92] The case was dismissed on the grounds that HIPAA does not grant an individual a private cause of action, but on appeal, the court reversed and agreed with the plaintiff that HIPAA's provisions may be referred to for the appropriate standard of care in the case, albeit that this was a suit based on a negligence cause of action and no HIPAA violation was being alleged in the case.[93] Similarly then, both GINA and HIPA could potentially be called upon to protect an employee who is subjected to surveillance meant to discover genetic condition. It is worth noting, however, that the case that allowed that HIPAA may serve as a standard for a duty of care alleged an actual harm, i.e., emotional distress. A significant problem with reading a protecting based on existing federal law 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

Moving beyond federal law, it is important to underscore the uneven nature of worker privacy protections offered by the different states. We employ the issue of smoker discrimination as a litmus test to gauge how protected employee privacy is in a particular state. But first, it is important to understand that there is a public/private divide when it comes to employee surveillance at the state level. While the Constitution could protect workers from government surveillance, workers who work for a private employer cannot rely on the Constitution as recourse since "State action" is required to invoke a constitutional right – with the result that public-sector employees enjoy far greater privacy rights than private-sector employees.[94] 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.[95] Even, then, "the protection provided by these remedies varies widely from jurisdiction to jurisdiction and in some cases has not protected against even the most outrageous forms of employer intrusions."[96]

---

[92] *Id.*
[93] *Id.* at 253–54.
[94] S. Elizabeth Wilborn, *Revisiting the Public/Private Distinction: Employee Monitoring in the Workplace,* 32 Ga. L. Rev. 825, 828-829 (1998).
[95] *Id*.
[96] *Id*.

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. They are: Alaska, California, Florida, Hawaii, Illinois, Louisiana, Montana, New York, South Carolina and Washington. California was the first state to grant privacy rights to private sector workers.[97] The California Constitution also protects data privacy.[98] Of the states that do not have explicit protections for the privacy of workers employed by a private employer, some state courts, including New Jersey and Alaska, have found that the state constitution's privacy protection could be extended to support a private employee's public policy claim of privacy infringement."[99]

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 fall into three broad categories: A first category that mimics the Wiretapping Act and allows for video but no audio and therefore no explicit protection from video only monitoring. The second category is even narrower and protects only the most intimately private employee actions from video and audio surveillance, and the third category of law, which is the least protective, demands only a notice requirement to alert employees to the fact that they are being surveilled.[100] The criticism of these laws are that they do not do enough to protect the worker, rather some have argued that the laws merely gives employers a legal safety net to avoid litigation simply by posting a notice of surveillance, and that this ignores employees' dignity rights."[101]

---

[97] Cal. Const. Art. I, § 1.

[98] Cal. Const. Art. I, § 13.

[99] Joanne Deschenaux, *Legal Protections for Employees' Workplace Privacy Rights Arise from Many Sources*,SHRM.ORG (May 25, 2010) http://www.shrm.org/legalissues/stateandlocalresources/pages/workplaceprivacysources.aspx.

[100] 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).

[101] 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).

Since 2012, some states have gone further in their bid to protect worker privacy by also instituting laws that afford workers protection in regards to 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.[102]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.[103] New Mexico also enacted a law in 2013 that affects only job applicants and doesn't mention current employees."[104] The Delaware governor recently signed a law that prohibits employers from invading their employees' or job applicants' social media accounts. The Delaware Employee/Applicant Protection for Social Media Act prevents employers from demanding access to an employee's 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."[105]

Some states have also passed laws to address the location tracking of workers. For example, in the State of 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.[106] And in Connecticut, the state legislature statutorily prohibits any employer from electronically monitoring an employee's activities without prior notice to all employees who may be affected.[107]

The state of California seems to have particularly strong protections for worker privacy. In the case of *Mintz v. Mark Bartelstein & Associates Inc.,*[108] in which an Agent filed a complaint against his employer and its principal, alleging violation of Computer Fraud and Abuse Act (CFAA)

---

[102] Bryan Knedler & William Welkowitz, *States Continue to Protect Workers' Social Media Privacy in 2014*, BNA.COM (Feb.10,2015) http://www.bna.com/states-continue-protect-n17179922967/.
[103] *Id*.
[104] *Id*.
[105] *Delaware Governor Signs Internet Privacy, Safety Package into Law*, GOVTECH http://www.govtech.com/internet/Delaware-Governor-Signs-Internet-Privacy-Safety-Package-into-Law.html (Last Visited OCt. 26, 2015).
[106] Kendra Rosenberg, *Location Surveillance by Gps: Balancing an Employer's Business Interest with Employee Privacy,* 6 WASH. J.L. TECH. & ARTS 143, 149 (2010).
[107] *Id*.
[108] 906 F. Supp. 2d 1017 (C.D. Cal. 2012).

and California Data Access and Fraud Act (CDAFA), and various state law claims, the court found that the undisputed allegation that "Priority Sports used Plaintiff's Gmail account to view information about the terms of Plaintiff's employment with CAA, including his compensation" was an act that "clearly implicated Plaintiff's legally protected interest in the privacy of his employment and financial affairs."[109] Further, the court remarked that although the California Supreme Court has recognized 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 reinforces the premise that individuals have a legitimate privacy interest with respect to income earned in the private sector.[110] California courts have similarly recognized an individual's protected privacy interest in his employment personnel file.[111]

2. States with Weaker Protections

In contrast to California, the state of Massachusetts seems to have particularly weak protections in place for workers. The 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.[112] However, even before the court may proceed with the "balancing test," the plaintiff must first establish that he has a protected privacy interest in the information.[113] Massachusetts courts, however, have not found an employee privacy interest even in acts committed outside the workplace. The case of *Rodrigues v. EG Sys., Inc.,*[114] provides a representative snapshot of how an employee's acts outside of the workplace may be deemed not private information. In

[109] *Mintz v. Mark Bartelstein & Associates Inc.*, 906 F. Supp. 2d 1017, 1033 (C.D. Cal. 2012).
[110] *Id.*
[111] *Id. See also*, *El Dorado Sav. & Loan Ass'n v. Super. Ct.*, 190 Cal.App.3d 342, 235 (Ct.App.1987).
[112] *See Webster v. Motorola, Inc.*, 418 Mass. 425, 637 N.E.2d 203, 207 (1994); *Folmsbee v. Tech Tool Grinding & Supply Inc.*, 417 Mass. 388, 630 N.E.2d 586, 588 (1994); *Bratt v. Int'l Bus. Machines Corp.*, 392 Mass. 508 (1984).
[113] *See, eg., Rodrigues v. EG Sys., Inc.*, 639 F. Supp. 2d 131 (D. Mass. 2009), *See also, Schlesinger v. Merrill Lynch, Pierce, Fenner & Smith, Inc.*, 409 Mass. 514, 567 N.E.2d 912, 915 (1991).
[114] *See*, 639 F. Supp. 2d 131 (D. Mass. 2009).

Rodrigues, a conditional employee, who was dismissed from consideration from permanent employment after test results showed nicotine use, indicating that he was a smoker, 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 claim under Employee Retirement Income Security Act (ERISA).[115]

The Massachusetts court found that Rodrigues did not have a protected privacy interest in the fact that he is a smoker because Rodrigues did not keep that fact private. As rationale for this ruling, the court noted that, in his deposition, Rodrigues admitted to smoking openly in public; 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."[116] The court also saw as pertinent to whether Rodrigues act of smoking outside of his workplace was a private or not 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."[117] The Massachusetts court found that because of these admissions, Rodrigues had no cause of action to contest his dismissal under the Massachusetts privacy statute.[118]

Of special interest to our arguments for this Article, however, are the Massachusetts court's rulings on medical information. In the case of *Bratt v. Int'l Bus. Machines Corp.,*[119] an employee brought action against employer, its agent, and another employee alleging libel and invasion of privacy.[120] The United States District Court, District of Massachusetts, granted defendants' motion for summary judgment on all counts of employee's amended complaint, and the employee appealed. Following oral argument, the United States Court of Appeals for the First Circuit certified questions of law. The Supreme Judicial Court, Liacos, J., held 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

---

[115] *Rodrigues v. EG Sys., Inc.,* 639 F. Supp. 2d 131 (D. Mass. 2009).
[116] *Id*. at 134.
[117] *Id*.
[118] *Id*.
[119] *Bratt v. Int'l Bus. Machines Corp.*, 392 Mass. 508 (1984).
[120] *Id*.

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 employer, it is not an invasion of employee's statutory right of privacy for physician to disclose such information to employer."[121]

Massachusetts approach to worker privacy may be summed up as a balancing of interests -- frequently resulting in the employer's legitimate business interest being 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."[122]

3. The Pernicious Effects of Employment Contracts

Complicating the issue of worker surveillance is the fact that most states allow for "at-will" employment which means that employment contracts may provide conditions upon which the worker may accept employment and upon which the employment contract would be terminated.[123] Thus, employers may condition employment contracts upon the worker acquiescing to intrusive surveillance by the employer.

What the additional factor of "at-will" employment means is that the solution for preventing intrusive and unreasonable worker surveillance

---

121 *Id*. at 134-35.

122 *Bratt v. Int'l Bus. Machines Corp*., 392 Mass. 508, 519-20 (1984).

123 See e.g., William R. Corbett, *The Need for a Revitalized Common Law of the Workplace*, 69 BROOKLYN L. REV. 91, 125-27 (2003), (declaring: "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.").

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 simply lacks the bargaining power to protect her privacy interests in the employment exchange.

III. THE NEW ARENAS FOR WORKPLACE SURVEILLANCE

It is important to examine, at a granular level, the emerging social and technological developments that are shaping workplace surveillance. In this section we consider governmentally backed corporate wellness programs, and the growing popularity of productivity apps that afford opportunities 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

Currently, private firms may employ wellness firms to mine employee data to gain deep insights about which prescription drugs employees use, whether they vote, and when they stop filing their birth control prescriptions.[124] Wal-Mart, for example, pays Castlight Healthcare Inc to assess employee data and nudge them toward weight-loss programs or suggest physical therapy instead of expensive operations.[125] But these programs raise serious questions about when and how much data employers should be able to use, and how that data might be used in discriminatory contexts. Wellness Programs have been defined as "any program designed to promote health or prevent disease."[126] Early workplace wellness programs were known as Employee Assistance Programs, and employees could receive assistance for issues regarding mental health, substance abuse, and stress.[127] Wellness Programs have

[124] See Rachel Emma Silverman, "Bosses Harness Big Data to Predict Which Workers Might Get Sick," *The Wall Street Journal,* Feb 16, 2016.
[125] Ibid.
[126] Ann Hendrix & Josh Buck, *Employer-Sponsored Wellness Programs: Should Your Employer Be the Boss of More Than Your Work*?, 38 SW. L. REV. 465, 468-69 (2009).
[127] *Id*.

since evolved to offer health risk assessment, weight reduction and smoking cessation programs, and to promote healthful behavior in the workplace.[128] While most of those programs are voluntary, some scholars have expressed some concern about the incentives offered by the program (which may also be re-framed as penalties) and about the fact that some employers are now making some of these programs mandatory.[129]

Workplace wellness programs now represent a $6 billion annual industry and includes an estimated 500 vendors selling programs either individually or as an optional component of healthcare insurance. When the ACA was signed into law in 2010, many saw it as a victory for workers, because, for one, it represented the protection of American individuals from denials of healthcare coverage based on pre-existing conditions, thus ostensibly freeing workers from employer sponsored group insurance. However, included as part of the Act were significant provisions that largely escaped notice. The ACA includes several provisions designed to promote wellness programs. 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."[130]

"The ACA also gives employers more latitude to reward employees for program uptake, which is increasingly regarded as critical to engaging employees and thus realizing the full value of the programs."[131] "It 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."[132] The new limit,

---

[128] *Id*.

[129] Mandatory wellness programs may 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, B.S.E., *The Emergence of Mandatory Wellness Programs in the United States: Welcoming, or Worrisome?*, 12 J. HEALTH CARE L. & POL'Y 99 (2009).

[130] 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 J. 268, 268 (2012).

[131] *Id*.

[132] *Id*.

which takes effect 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.[133] The ACA already allows up to 50% of the cost of the insurance coverage to be offered to individuals as an incentive for smoking cessation.[134]

More than 60 percent of Americans get their health insurance coverage through an employment-based plan.[135] 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., first used it in the context of alternative medicine-- he began using the phrase "high level wellness" in the 1950s. The concept of wellness was introduced to corporate America in the 1970s.[136]

Since the 1970s, the government has taken on an active role in promoting wellness within the workplace. The President's Committee on Health Education was established in 1973 and, in addition to other acts, this committee legitimized an emphasis on health and health education and a more hands-on role for government in developing model programs and providing seed money for their implementation. It recommended, for example, creation of a National Center for Health Education, which occurred in 1975. The Center successfully pushed for expanded worksite programming as well as nation-wide programming, professional credentialing, and comprehensive school health education programs.

Important governmental writings that influenced the profession were the 1979 Surgeon General's report on health promotion entitled Healthy People, and the 1980 report entitled Promoting Health, Preventing Disease: Objectives for the Nation. In 1980, the U.S. Government also created a separate Department of Education in the Department of Health and Human Services and gave it responsibility for supporting health education, health promotion, and wellness programming. In 1981, Objectives for the Nation in Disease Prevention and Health Promotion was adopted as policy in the United States and again in 2001 with new goals established. The following year, 1991, saw the publication of Healthy People 2000: National Health Promotion and Disease Prevention Objectives and Healthy Communities 2000: Model Standards. The subsequent publication of healthy People 2010 is also helping to shift

---

[133] *Id*.

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

[135] David Blumenthal, *Employer-Sponsored Health Insurance in the United States—Origins and Implications*. 355:1 NEW ENG. J. MED. 82, 83 (2006).

[136] Peter Conrad, *Wellness in the Work Place: Potentials and Pitfalls of Work-Site Health Promotion,* 65 THE MILBANK QUARTERLY 255, 257 (1987).

public policy toward prevention through health education and health promotion programming in communities.

The idea of the government as a "residual guarantor" is one that has taken root in American society. This concept is found in literature written by the government to explain its stance on health promotion in communities.[137] As a guarantor of health outcomes, the government also feels compelled to recruit the private sector to facilitate the achievement of the government's health goals.[138] This explains the Obama administration's support of the Wellness programs and the ways that protective federal laws which might have been read to contradict the surveillance endemic to wellness programs has been reinterpreted to allow employers greater latitude in establishing and administering wellness programs in the workplace.[139]

Approximately half to two-thirds of U.S. employers offer some kind of wellness program.[140] Ninety-nine percent of large firms (with 200 or more workers) in 2013 offered at least one wellness program. Specifically, 69 percent offer gym membership discounts or on-site gyms, 71 percent offer smoking cessation programs, and 58 percent offer weight-loss programs. Among these firms, 36 percent offer some financial incentive to participate in wellness programs.[141] Incentives are used more often to incentivize completion of a health risk assessment or participation in a wellness program than to reward behavior change. The most common objectives of lifestyle modification programs are smoking cessation and weight loss or the related behaviors of nutrition and fitness.[142] The amount of the incentives ranges from 3 to 11 percent of the total cost of individual

---

[137] The government is a "residual guarantor" of health services, whether they are provided directly or through community agencies. Every locale and population should be served by a unit of government that takes a leadership role in assuring the public's health. HEALTHY COMMUNITIES 2000: MODEL STANDARDS WASHINGTON, DC, 26 (American Public Health Association, xvii 1991).

[138] "Many of the activities . . . go beyond the activities customarily carried out by state and local governmental agencies. Even in those areas where health agencies are extensively involved, prevention is a shared responsibility of the public and private sector." *Id*. at 443.

[139] 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).

[140] Marcie Pitt-Catsouphes, et. al., *Workplace-Based Health and Wellness Programs: The intersection of Aging, Work, and Health,* 55 THE GERONTOLOGIST 262, 263 (2015).

[141] *2014 Employer Health Benefits Survey*, KFF.ORG (Sept. 10, 2014), http://kff.org/report-section/ehbs-2014-summary-of-findings/

[142] SOEREN MATTKE, ET AL., WORKPLACE WELLNESS PROGRAMS STUDY, xv, (RAND Corp., 2013).

coverage.[143] The use of these programs is likely to expand; 25 percent of employers report 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 behaviors."[144]

Wellness programs are poised to become ubiquitous in the corporate space, particularly given that group health insurers now have many choices in designing incentives. The incentives may take the form of modified premiums, smaller copays or deductibles, cash, gift cards, or merchandise.[145] Employers have increased the financial incentives they offer workers to participate in wellness programs to a record $693 per employee, on average, this year from $594 in 2014 and $430 five years ago.[146] 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.[147]The question is whether these incentives cloud the asymmetrical power relationship between the employer and the employee and whether in reality the employee is being called upon 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, etc. As previous research has shown, the data from fitness trackers can be irregular and unreliable.[148]

---

[143] Incentives for Nondiscriminatory Wellness Programs in Group Health Plans , 45 Fed. Reg. 33158, 33168 (June 3, 2013) (to be codified at C.F.R. 146-147).

[144] THE NEW HEALTH CARE IMPERATIVE: DRIVING PERFORMANCE, CONNECTING VALUES, 10, (Tower Watson/Nat'l Bus. Group on Health, 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.

[145] John Cawley, *The Affordable Care Act Permits Greater Financial Rewards For Weight Loss: A Good Idea In Principle, But Many Practical Concerns Remain.* 33(3) JOURNAL OF POLICY ANALYSIS AND MANAGEMENT 810 (2014).

[146] Crawford, K., Lingel, J. and Karppi, T. 2015 'Our Metrics, Ourselves: A Hundred Years of Self-Tracking From The Weight Scale to The Wrist Wearable Device', *European Journal of Cultural Studies* Vol. 18(4-5) 479 –496; *see also* 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-idUKKBN0MM0BB20150326?feedType=RSS&feedName=healthNewsMolt.

[147] *Id*.

[148] Most fitness trackers are worn on the wrist and use accelerometers to measure motion; some inherent flaws are that the accelerometer measures only motion, not exertion and

Furthermore, the data from Fitbits and other such devices require interpretation. Data analytic companies which interpret the data using "industry and public research" are defining the standards that measure a worker's health status and health risks. One problem, as scholars have noted is that medical and health research is rapidly changing, such that current standards as to what is "healthy" are not the same as they were in the past.[149] Yet, companies that interpret the data from wearables lawfully operate as black boxes, revealing nothing about their data sets and the algorithms used for interpretation.[150]

Another overlooked problem lies in the question of access to the data collected by employer-provided wearables. Legally, when an employer provides a device for an employee, whether it be a laptop, a mobile phone, or a fitness tracker, that device remains the property of the employer, meaning that the employer could access the data from such devices at any time without permission from the employee.[151] This raises concerns about the privacy of the electronic health data collected from employees who choose to participate in wellness programs.

---

also, some of today's wrist-worn accelerometers are still calibrated for steps, they cannot tell when an individual is cycling and thus won't count that as physical activity. *See*, Albert Sun & Alastair Dant, *What Your Activity Tracker Sees and Doesn't See,* N.Y. TIMES (Last Updated Mar. 11, 2014) http://well.blogs.nytimes.com/projects/2014/03/accelerometers.html.

[149] Many wellness programs use "body mass index" (BMI) as a metric to determine obesity. However, current medical research has shown 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 PROCEEDINGS 1072 (2014). *See also*, *Summer of Science*, N.Y. TIMES (Sept. 3, 2015), http://www.nytimes.com/interactive/projects/cp/summer-of-science-2015/latest/bmi?smid=tw-nytimes.

[150] *See*, Kate Crawford, *When Fitbit is the Expert Witness*, THE ATLANTIC (Nov.19, 2014) http://www.theatlantic.com/technology/archive/2014/11/when-fitbit-is-the-expert-witness/382936/.

[151] 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." Harper's Magazine, Esther Kaplan, The Spy Who Fired Me, http://www.populardemocracy.org/sites/default/files/HarpersMagazine-2015-03-0085373.pdf

2. Issues of employment discrimination

Other than the potential for invasion of privacy, the collection of personal and sensitive health information by wellness programs invites questions as to employment discrimination. Many of the issues of discrimination arising from wellness programs are not, however, ones that are clearly addressed by traditional anti-discrimination laws such as Title VII of the Civil Rights Act, or the Americans with Disabilities Act. The issues of discrimination arising from wellness programs go beyond race, gender, pregnancy and 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 more than one-third of adults are considered obese. The law is not well settled on whether obesity is a disability such that obese people would be a special class protected from losing their jobs because of their weight.[152] For some jurisdictions, obesity is never a disability and for others, obesity only becomes a disability when it is so severe as to impact daily life activities -- such a definition would really only include the morbidly obese and not the moderately obese who nonetheless have increased risks of certain chronic disease and whom an employer might view as an increased healthcare cost.[153] As a result of these uncertain legal protections, workers should be wary about losing their jobs as a result of joining a wellness program.

Another area of where the worker is unprotected by the law is when it comes to smoking.[154] There is no federal law protecting a smoker from employment discrimination. In nine states, an employer may legally fire an employee for smoking outside of the workplace.

The EEOC has recently brought three cases based on its suspicions that corporate wellness programs are being employed as a backdoor for employment discrimination. In the case of *EEOC v. Orion Energy Systems*, an employee objected to participation in the wellness program. Specifically, she questioned whether the health risk assessment was voluntary and whether medical information obtained in connection with the assessment would be kept confidential. After the employee raised her

[152] Lindsay F. Wiley, *Shame, Blame, and the Emerging Law of Obesity Control*, 47 UC Davis L. Rev. 121 (2013)
[153] Lindsay F. Wiley, *Shame, Blame, and the Emerging Law of Obesity Control*, 47 UC Davis L. Rev. 121 (2013)
[154] Jessica Roberts, *Healthism & The Law of Employment Discrimination*, 99 Iowa L. Rev.571 (2014)

objections, she was called into a meeting with Orion's personnel director and her supervisor. During that meeting, the employee was ordered not to express any opinions about the wellness program to her coworkers. After the employee declined to participate in the wellness, she was required to pay the entire premium cost for her health benefit. The case is currently pending.

In a second case, *EEOC v. Flambeau*, *Inc.* (No. 3:14-00638) (W.D. Wis. 2014), the EEOC alleges that Flambeau's requirement that employees participate in its wellness program or face termination of their health insurance violates the ADA. According to the complaint, Flambeau cancelled employee Dale Arnold's health insurance because he did not complete the biometric testing and health risk assessment conducted under Flambeau's wellness program, leaving him only with the option of applying for COBRA at his own cost. If Mr. Arnold had completed the biometric testing and health risk assessment, Flambeau would have covered about 75 percent of his health insurance premiums. Similarly, Orion Energy covered the entire amount of the health insurance premiums for employees who participated in its wellness program, while employees who did not participate had to cover the entirety of their premium costs.

The EEOC's contention that the Flambeau and Orion Energy wellness programs violate 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. However, the ACA allows that disability-related inquiries and medical examinations are permitted in the context of a wellness program if the program is "voluntary," and if employee medical information is kept confidential. The question arising from the Orion Energy and Flambeau cases is whether the penalty of paying the full premium exacted on the employee belies the "voluntariness" of wellness program. The EEOC has defined a voluntary wellness program as one in which the employer neither requires participation nor penalizes employees for not participating in the program. But, the EEOC has not yet taken a formal position on what would amount to a penalty.

In the third case, *E.E.O.C. v. Honeywell Int'l, Inc.,* No. CIV. 14-4517 ADM/TNL, 2014 WL 5795481, at *1 (D. Minn. Nov. 6, 2014). 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. It is important to note once again that the EEOC does not allege that Honeywell's wellness program violates employees' right to privacy in

their medical information, and that the EEOC does not request that the Court order Honeywell to cease the biometric testing associated with its wellness program; the EEOC is merely asserting that the penalties levied in this case contravene the mandated voluntary nature of wellness programs.

While the extant cases against wellness programs have focused on the biomedical testing that accompanies such programs, it is important to understand that many corporate wellness programs also include smoking cessation offerings, and that, in several states, workers may be fired for admitting to being a smoker, even if they do not smoke in the workplace. Thus, such smoking cessation programs solicit and collect information from employees that may be wielded by the employer for the employees' dismissal.

B. Productivity Apps

Productivity Apps have been touted as a workplace technology that will revolutionize management and that will 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, Kronos and "enterprise social" platforms such as Microsoft's Yammer, Sales-force's Chatter, and, soon, Facebook at Work.[155]

However, it is important to consider that the very nature of apps, as electronic programs which can tirelessly monitor an employee, 24 hours a day, 7 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 Central Californian woman brought suit against her employer who, she alleges, fired her for uninstalling a program on her company-issued iPhone that tracked her every move, 24-hours-per-day and seven-days-per-week, which invariably included times when she was not working. The plaintiff argued that termination for uninstalling the app was unlawful and analogized the employer's demand to maintain the program to electronic monitoring

[155] Esther Kaplan, *The Spy Who Fired Me*, HARPER'S MAGAZINE, March 2015, at 31, *see also*, Conor Dougherty & Quentin Hardy, *Managers Turn to Computer Games, Aiming for More Efficient Employees,* N.Y. TIMES (March 15, 2015) http://www.nytimes.com/2015/03/16/technology/managers-turn-to-computer-games-aiming-for-more-efficient-employees.html?_r=0.

anklets for prisoners. In addition, she alleged that the app was used inappropriately, such as when her employer admitted that he used it to monitor her driving speed during non-work hours.[156]

Even with all the convenience and perceived accuracy that productivity apps could afford human managers, there remains the issue of whether there is an information asymmetry about such apps that negate consent, and whether the invasive nature of such apps could permanently erode worker privacy. Employers' surveillance of workers was borne out of necessity. With division of labor came the need for overseeing and monitoring to insure that the work was completed not just in a timely fashion but also in a manner that met quality standards. Thus it is undeniable that employers have an economic interest in monitoring their employees. What is contested is the expanding encroachment of employer surveillance on facets of a worker's life that were previously deemed personal, autonomous, or private, a creep that is enabled and facilitated by advances in technology that allow for even greater electronic monitoring and data gathering. These new technologies are increasingly being perfected and made available to managers by start-up companies.

For example, BetterWorks is a company that makes management software which "blends aspects of social media, fitness tracking, and video games" into a program designed to encourage productivity among workers.[157] Employees are obliged to track their progress towards a measurable goal on a digital dashboard that everyone in their company can see. Co-workers have the ability to give encouragement or shame each other. An employee's progress is represented by a tree that "grows with accomplishments or shrivels with poor productivity."[158]

BetterWorks, and apps like it, are prime examples of what Julie Cohen has termed the "the surveillance-innovation complex"[159] and Shoshana

---

[156] David Kravets, *Worker Fired for Disabling GPS App that Tracked her 24 hours a Day*, ARSTECHNICA (May 11, 2015), http://arstechnica.com/tech-policy/2015/05/worker-fired-for-disabling-gps-app-that-tracked-her-24-hours-a-day/.

[157] Conor Dougherty & Quentin Hardy, *Managers Turn to Computer Games, Aiming for More Efficient Employees,* N.Y. TIMES (March 15, 2015) http://www.nytimes.com/2015/03/16/technology/managers-turn-to-computer-games-aiming-for-more-efficient-employees.html?_r=0.

[158] *Id*.

[159] JULIE E. COHEN, THE SURVEILLANCE-INNOVATION COMPLEX: THE IRONY OF THE PARTICIPATORY TURN (June 19, 2014). DARIN BARNEY, ET AL., THE PARTICIPATORY CONDITION (University of Minnesota Press, Forthcoming 2015) (on file http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2466708).

Zuboff designates, "surveillance capitalism."[160] With such apps, "commercial surveillance environments use techniques of gamification to motivate user participation" and furthermore, surveillance is recast "in an unambiguously progressive light" with the conceit that such greater monitoring drives innovation and economic growth.[161] In turn, the surveillance-innovation complex insidiously finds justification as academic inquiry as to how workers should be managed, a 'discipline' that is referred to as "workplace science." This emerging field is comprised of data analysis injected into the field of human resource management and eschews "gut feel and established practice" in favor of Big Data to "guide hiring, promotion and career planning."[162]

Proponents of this workplace science couch the heightened surveillance it requires as unremarkable apart from the capacity for such surveillance to obtain information of immense utility for the greater good of the company. As one proponent of the field 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."[163] Such discourse, while failing to consider privacy implications, also promotes the ideology that Big Data mined from workers invariably leads to innovation and efficiency. In turn, as Julie Cohen has observed, such rhetoric also "advance[s] the instrumental goal of holding the regulatory state at arm's length." If the only remarkable consequence of the data mining of worker's daily lives is economic growth, then there is nothing left for the political economy to concern itself about, apart from encouraging and enabling such data mining.

Although work science is merely an iteration in a long history of academic study with the unabashed goal of promoting worker efficiency and productivity, the new work science differs in paradigm and practice from its predecessors in ways that hold disconcerting implications for worker privacy and employability. Louis Brandeis is credited with

---

[160] Shoshana Zuboff, "Big Other: Surveillance Capitalim and the Prospects of an Information Civilization*," Journal of Information Technology*, 2015 (30) pp 75-89.

[161] JULIE E. COHEN, THE SURVEILLANCE-INNOVATION COMPLEX: THE IRONY OF THE PARTICIPATORY TURN (June 19, 2014). DARIN BARNEY, ET AL., THE PARTICIPATORY CONDITION (University of Minnesota Press, Forthcoming 2015) (on file http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2466708).

[162] 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.

[163] *Id*.

popularizing the term "scientific management" in 1910.[164] Frederick Winslow Taylor adopted the term in the 1880s and 1890s and his theory of management that analyzed workflows with the primary goal of improving economic efficiency and labor productivity came to be known as a subset of scientific management.[165] Unlike Taylorism when the focus was on the job/task and mastering it by breaking it down into discrete components that could be studied for efficiency, now with workforce science, the spotlight is on the individual worker and 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 firm.

1. Issues of Privacy and 24/7 monitoring

Unlike other forms of surveillance, productivity apps have the potential to be omnipresent in the workers' lives. As the Xora case has demonstrated, productivity apps may be switched on without the 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

Given that the data from electronic wearables have been proven to be 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 easily designed. However, they are possible. The challenge for their design lies in reestablishing the power balance between the information domain of

[164] HORACE BOOKWALTER DRURY, SCIENTIFIC MANAGMENT: A HISTORY AND CRITICISM 15-21 (Columbia Univ. 1918).
[165] HORACE BOOKWALTER DRURY, SCIENTIFIC MANAGMENT: A HISTORY AND CRITICISM 15-21 (Columbia Univ. 1918).

employers and the information domains of the worker. As long as work-related information remains 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 place of technological advances in work-related sensors and surveillance. Instead, we must think of information about workers as multi-dimensional, touching many contexts and domains of an individual's life at the same time, such as their time, their location, their privacy, and their physicality. And when those domains contain sensitive categories of data, such as health, the law must recognize that and intervene to prevent workplace justifications from overriding those protections. In many ways, this is what GINA sought to accomplish for the narrow domain of genetic information.[166]

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 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 fall outside of HIPAA's jurisdiction,[167] 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.[168] The European Union's Data Directive has long served as a model

---

[166] *See*, Ifeoma Ajunwa, *Genetic Data and Civil Rights*, 51 Harv. C.R.-C.L. L. Rev. __ (forthcoming 2016).(arguing that GINA should 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).

[167] HIPAA has jurisdiction over health information handled by health care providers. The law is not settled on whether wellness program vendors fall under that category.

[168] See Sam Han and Scot Ganow, *Model Omnibus Privacy Statute*, 35 UNIV. OF DAYTON L. REV. 303 (2010); ." S. Elizabeth Wilborn, *Revisiting the Public/Private Distinction: Employee Monitoring in the Workplace*, 32 GA. L. REV. 825 (1998) ("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); http://articles.latimes.com/1991-03-27/news/mn-938_1_constitutional-amendment

for this approach, empowering 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.[169] Recently, the European Commission announced it is considering an even stronger General Data Protection Regulation which would place more power in the hands of NDPAs to enforce general privacy violations.[170]

While there is much appeal to this approach as a general panacea for privacy concerns writ large, it still 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 accede power to standard notice-and-consent mechanisms whereby data collectors and processors seek consent for specific uses of data. In the United States, such an omnibus protection would represent a pyrrhic victory; as we noted earlier, in the context of at-will employment laws, wherein 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 with no real chance for dispute by the employee.

Arguably, in the consumer context, individuals have some power to forego granting consent to particular requests and can seek marketplace alternatives in data collectors or processors who offer different data practices. However, in the worker context, such consent is essentially a fiction. The occasional 'OccupEye' public incident aside, the notion that most employees could parse each employer surveillance practice and technology and then negotiate consent both individually and collectively pits those with the least power in worker context against those with the most. The requirement that the information collector or processor limit her use to a specific purpose does not help mitigate the dangers of limitless worker surveillance either; employers will simply continue to redefine the purposes of their surveillance in light of the employer-employee context and the information domain as work-related information, much as *The Daily Telegraph* defined the OccupEye installation as related to workplace environmental and climate control purposes. Thus, the employer could potentially offer the pretext of improving worker productivity as justification of *any* surveillance; thus enabling limitless worker surveillance.

[169] See http://ec.europa.eu/justice/data-protection/.
[170] See http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf.

Moreover, as Paul Schwartz has pointed out, omnibus privacy approaches tend to define privacy at a "lowest common denominator" level because the definition must work for all individuals and for all kinds of data.[171] As we note above, the particular context of employee data, especially data concerning wellness, health, and one's personhood, and which could be wielded to remove one's access to making a livelihood, demands specific attention and thus is more appropriately considered under a regime with a narrower and more robust approach.[172]

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

More promising 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. If one were to imagine such an approach, say a law entitled the "Employee Privacy Protection Act" (EPPA), one could envision it specifically limiting 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. Much like other worker protection laws, such as minimum wage, overtime, and safe working conditions, this would serve as a general protection for all workers that could not be waived. It would 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 are antithetical to "freedom to contract" principles and would limit the opportunity for technological innovation to benefit work and the labor economy. But those innovations would still be available to the worker through third party products and services – just not at the insistence and under the undue influence of the employer. Thus, the context of the use of such data would shift to one that was more autonomous for the worker. Data autonomy would no longer be seen as a condition of employment or as part of an employer's capital to be capriciously withheld or magnanimously granted to the employee, rather data autonomy would be recognized as an essential human right, part and parcel of the guarantee of an individual's right to make a livelihood. That

---

[171] Paul M. Schwartz, *Preemption and Privacy*, 118 Yale L.J. 902 (2009) (arguing there are benefits from a sectoral approach to privacy over an omnibus approach).

[172] See also Helen Nissenbaum, PRIVACY IN CONTEXT, Stanford Law Books (2009).

shift moves the data from the domain and context of "workplace" to one of personhood.

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

An even narrower approach would be to further limit the protections to specific types of sensitive data, such as data related to autonomy and physicality.[173] Much as the OccupEye device installed in *The Daily Telegraph*'s offices was jokingly seen as a constraint on bathroom breaks, worker surveillance often does focus on the physicality of workers, placing them in extremely vulnerable positions vis-à-vis their employers. This is particularly true in the context of health and wellness programs as proxies for worker surveillance, wherein physical monitoring is all but mandated. 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) which would clarify that health information generated through any program (including third party wellness programs) or device connected to one's employment is considered protected health information under other health privacy laws, such as the Health Insurance Portability and Accountability Act (HIPAA). It would also mandate strong rules for employer access to health data collected from fitness devices (even when employer owned) and for vendors as to what happens to data collected from employees as part of a wellness program, such data should not be sold without the permission of the employee, and the employee has the right to request the destruction of the data record once the employment has been 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.[174] It would also take advantage of the fact that HIPAA laws and regulations are extremely well developed and most employers have experience working with the restrictions HIPAA imposes. Such a law would also allow that innovations in physical sensors, such as the Apple Watch, Microsoft Band, or Fitbit, will continue to evolve without the need to revisit privacy rules each and

[173] See generally Paul Ohm, Sensitive Data, 88 S. Cal. L. Rev. ___ (2015), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2501002.

[174] Nicolas Terry, Big Data Proxies and Health Privacy Exceptionalism, 24 Health Matrix 65-108 (2014), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2320088.

every time those innovations touch on a new context or domain related to the sensitive information discoverable about workers by their employers.

2. CONCLUSION

While accelerations in worker surveillance innovation and technological advancements in worker monitoring have been accepted as auguring well for worker productivity and the efficacy of remote management, they have decimated worker privacy. For one, the innovative technology of wearable technology has in reality 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 privacy invasions are considered only in terms of the harms that accompany them, this belies the fact that diminished privacy for workers represents harm in 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 productivity of their workers 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 as separate from work and the workplace.

Appendix A

States where an employee could be fired for being a smoker									
Alabama	Yes	Hawaii	No	Michigan	No*	North Carolina	No**	Utah	No*
Alaska	Yes	Idaho	No	Minnesota	No	North Dakota	No*	Vermont	No*
Arizona	No*	Illinois	No**	Mississippi	No	Ohio	No*	Virginia	Yes
Arkansas	No*	Indiana	No	Missouri	No	Oklahoma	No*	Washington	Yes
California	No	Iowa	No	Montana	No**	Oregon	No*	West Virginia	No**
Colorado	No	Kansas	No	Nebraska	Yes	Pennsylvania	No*	Wisconsin	No**
Connecticut	No	Kentucky	No**	Nevada	No	Rhode Island	No	Wyoming	No**
Delaware	No*	Louisiana	No	New Hampshire	No	South Carolina	No		
D.C.	No	Maine	No	New Jersey	No	South Dakota	No***		

Florida	Yes	Maryland	No*	New Mexico	No	Tennessee	No		
Georgia	Yes	Massachusetts	Yes	New York	No**	Texas	Yes		

*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: http://www.nolo.com/legal-encyclopedia/workplace-smoking-laws-your-state-46877.html