ALGORITHMS AT WORK: PRODUCTIVITY MONITORING APPLICATIONS AND WEARABLE TECHNOLOGY AS THE NEW DATA-CENTRIC RESEARCH AGENDA FOR EMPLOYMENT AND LABOR LAW

Ifeoma Ajunwa*

ABSTRACT

Recent work technology advancements such as productivity monitoring software applications and wearable technology have given rise to new organizational behavior regarding the management of employees and also prompt new legal questions regarding the protection of workers’ privacy rights. In this Article, I argue that the proliferation of productivity monitoring applications and wearable technologies will lead to new legal controversies for employment and labor law. In Part I, I argue that productivity monitoring applications will prompt a reckoning regarding the balance between the employer’s pecuniary interests in monitoring productivity and the employees’ privacy interests. Ironically, such applications may also be both sword and shield in regard to preventing or creating hostile work environments. In Part II of this Article, I note the legal issues raised by the adoption of wearable technology in the workplace—notably, privacy concerns, the potential for wearable tech to be used for unlawful employment discrimination, and worker safety and workers’ compensation issues. Finally, in Part III, I chart a future research agenda for privacy law scholars, particularly in defining “a reasonable expectation of privacy” for employees and in deciding legal questions over employee data collection and use.

* Assistant Professor, Cornell ILR School; Associate Member, Cornell Law School, Faculty Associate Member, Berkman Klein Center at Harvard University.
# Table of Contents

**Introduction** .................................................................3

**I. Productivity Monitoring Applications** .........................4

   A. Weighing Privacy vs. Employers’ Interests ............5

   B. Harassment and Hostile Work Environment Issues*

**II. Wearable Technology**

   A. Privacy Concerns ...................................................... 28

   B. Potential for Discrimination ..................................... 31

   C. Worker Safety and Workers’ Compensation ...........33

**III. Employee Rights: Research Questions for Legal Scholars** 37

   A. A Reasonable Expectation of Privacy for Employees37

   B. The Battle over Employee Data .................................. 38

**Conclusion**...............................................................................42

Electronic copy available at: https://ssrn.com/abstract=3247286
INTRODUCTION

In the 18th Century, during the Qing Dynasty, Chinese merchants wore abacus rings which they operated with the use of a tiny pin—perhaps the first wearable technology. And since Frederik Winslow Taylor’s time-series experiments in factories in 1911, the notion that an employer’s economic interests are best achieved through the close monitoring of workers for efficiency in productivity has attained a firm foothold in American society. Today, recent work technology advancements, such as productivity monitoring software applications and wearable technology, have given rise to new organizational behavior regarding the management of employees and prompted new legal questions regarding the protection of workers’ rights. In this Article, I argue that the proliferation of productivity monitoring applications and wearable technologies will lead to new legal controversies for employment and labor law. In Part I, I argue that productivity monitoring applications will prompt a rethinking of the balance between the employer’s pecuniary interests in monitoring productivity and the employees’ privacy interests. Ironically, such applications may also be both sword and shield in regard to preventing or creating hostile work environments. In Part II of this Article, I note the legal issues raised by the adoption of wearable technology in the workplace—notably, privacy concerns, the potential for wearable tech to be used for unlawful employment discrimination, and worker safety and workers’ compensation issues. Finally, in Part III, I chart a future research agenda for privacy law scholars, particularly in defining “a reasonable expectation of privacy” for employees and in deciding legal questions over employee data collection and use.

1 See Ashely Feinberg, This Wearable Abacus is Basically the World’s Oldest Smart Ring, GIZMODO (Mar. 17, 2014, 3:40 PM), https://gizmodo.com/this-wearable-abacus-is-basically-the-worlds-oldest-sm-1545627562
2 FREDERICK WINSLOW TAYLOR, THE PRINCIPLES OF SCIENTIFIC MANAGEMENT 5 (1911).
I. PRODUCTIVITY MONITORING APPLICATIONS

Employers with an interest in monitoring worker productivity may request that employees install productivity applications on devices such as computers or mobile phones. Some productivity applications designed for installation on smartphones are Avaza, Boomr, Hubstaff, TSheets, GPS Phone Tracker, Track View, and Where’s My Droid. These applications on employees’ work smartphones allow employers to easily monitor employees’ activities even outside of work hours. According to a 2012 study by a technology research firm Aberdeen Group, 62 percent of companies with so-called “field employees” were using GPS to track them. This represents more than double the 30 percent figure estimated in 2008.

Tracking the physical location of employees as a means to ensuring productivity or monitoring against misconduct is a social phenomenon that traverses several occupational fields. At the University of California-San Francisco Medical Center, pediatric nurses wear electronic locators that monitor them wherever they go. Nurses at Wyckoff Hospital in Brooklyn are required to wear personal tracking devices, which even record the time they take a break or go to the bathroom, in order to improve care. The city of Aurora, Colorado, puts tracking devices inside its sweepers and snowplows to monitor the workers, and it has seen an overall 15 percent increase in productivity. Employers also monitor workers’ activities by installing spyware and GPS

---


4 See Chen, supra note 3.


6 Id.


8 Id.

9 Id.
trackers\textsuperscript{10} on desktops and company-issued laptops.\textsuperscript{11} GPS trackers especially record enough data to make detailed profiles of individual employees and to create “biometric CVs” that prove how well an employee is suited to a job.\textsuperscript{12}

Some have argued that such technological advances have contributed to the erosion of the demarcation between work and personal life\textsuperscript{13} and that these new technologies bring privacy concerns, particularly since such productivity applications are capable of tracking employees outside the workplace.\textsuperscript{14} Such persistent tracking is why, in the 1987 case of \textit{O’Connor v. Ortega}, Justice Blackmun noted that “the workplace has become another home for most working Americans. . . The tidy distinctions . . . between the workplace and professional affairs, on the one hand, and personal possessions and private activities, on the other, do not exist in reality.”\textsuperscript{15} In the sub-sections below, I discuss both the privacy concerns represented by productivity tracking, as well as how the power for pervasive tracking intersects with both harassment prevention and harassment claims.

\textit{A. Weighing Privacy vs. Employers’ Interests}

Although workplace surveillance in the name of productivity is not a new business concept,\textsuperscript{16} methods of surveillance, both more expansive and more discreet, have created unique


\textsuperscript{12} See Rutkin, \textit{supra} note 10.


\textsuperscript{14} See Rutkin, \textit{supra} note 10.

\textsuperscript{15} \textit{O’Connor v. Ortega}, 480 U.S. 709, 739 (1987); Sprague, \textit{supra} note 13, at 222.

legal challenges. As it has become possible for employers to collect personal data of their employees during and after work hours, scholars\textsuperscript{17} and workers have expressed their concerns about privacy\textsuperscript{18} and trust in the employment relationship and potential discrimination.\textsuperscript{19} In addition, the employer might be accused of spying on employee union activity if an employee with such device attends a union meeting during a break or the device tracks the employee’s precise locations.\textsuperscript{20}

\textit{Arias v. Intermex Wire Transfer, LLC}

Such concern was expressed through a number of lawsuits. In 2015, one employee brought a lawsuit against her employer in relation to this issue. Shortly after Myrna Arias, the employee and the plaintiff, was hired by her employer Intermex Wire Transfer, a company that provides money wire services, Intermex instructed its employees to download the Xora app to their company-issued smartphones.\textsuperscript{21} The Xora app is part of the StreetSmart workforce management software distributed by ClickSoftware, which provides the location of every mobile employee on a Google Map “with detailed information such as arrival times, break status, the route driven and more.”\textsuperscript{22} When the employees found out that the Xora app contained a GPS function, Arias and

\textsuperscript{17}See Patricia Sánchez Abril, Avner Levin & Alissa Del Riego, \textit{Blurred Boundaries: Social Media Privacy and the Twenty-First-Century Employee}, 29 AM. BUS. L.J. 63, 64, 100 (2012) (arguing that “‘boundary-crossing’ technologies blur the already elusive line between the private and the public, the home and the workplace.”); Ariana R. Levinson, \textit{Toward a Cohesive Interpretation of the Electronic Communications Privacy Act for the Electronic Monitoring of Employees}, 114 W. VA. L. Rev. 461, 469 (2012) (“Technology permits a ‘boundary-less’ workplace in which employees work during non-work hours and while at home. . . . As for employers, the technology provides more ability to monitor employees’ communications, made both at work and away from work.”); Sprague, supra note 13, at 244.

\textsuperscript{18}See Rutkin, supra note 10.

\textsuperscript{19}See Peterson, supra note 5.


other employees asked their employer whether they would be monitoring their movements even when they were off-duty. This was particularly concerning because the employees were required to keep their phones on “24/7 to answer phone calls from clients.” Arias’ supervisor at Intermex, Stubits, admitted that employees would be monitored while off duty and “ bragged that he knew how fast she was driving at specific moments ever since she had installed the app on her phone.”

Arias had no problem with turning on the app during her work hours, but she rejected having her location monitored during non-work hours and complained to her supervisor that this was an invasion of her privacy, arguing that the app was similar to a prisoner’s “ankle bracelet.” Afterwards, she was scolded for uninstalling the app, and within a few weeks of her objection to the use of the Xora app, Intermex fired her. After Intermex terminated Arias’ employment, the president and CEO of Intermex telephoned the vice president of NetSpend, the company Arias had been working for after being fired by Intermex, and she was promptly fired by NetSpend. Arias filed a lawsuit claiming wrongful termination, invasion of privacy, unfair business practices, retaliation and other claims, seeking over $500,000 in damages for lost wages. The suit was privately settled. The case is particularly important because employees are increasingly expected to be available at any time, and this leads to the mixing of business and personal activities during office hours where employers can easily “cross the line.”

23 Arias, supra note 21, at 17.
24 Id. at 18 (internal quotations omitted).
25 Id. at 17–18.
26 Id. at 18.
27 Id.
28 Arias, supra note 21, at 18.
29 Id. at 19.
A settled case not only invites discussion of how such a complaint would have played out in court, but also suggests another question: why, in the subsequent years, have there been no similar cases? The use of productivity apps is no isolated occurrence. The simplest answer comes from Gail Glick, the attorney who represented Arias, speaking to The Atlantic “that her argument, which relied in part on the section of the California penal code that restricts how GPS tracking can be used, may not have worked anywhere else.”\(^{32}\) That law creates criminal liability, with narrow exceptions, for the “use [of] an electronic tracking device to determine the location or movement of a person.”\(^{33}\) More broadly, scholars have pointed out that California is one of states with more comprehensive privacy laws, especially in relation to workers.\(^{34}\) Therefore, while a harm may exist in a real sense, its recognition in law varies. Without a legal theory on which to bring a case, employees facing situations like Arias’ may find themselves unable to sue—even if they could overcome other existing obstacles and disincentives to filing a suit against a former employer.

**GPS on Phones**

There are similar cases in which employees complained about their employers’ excessive surveillance using productivity and monitoring applications, especially ones with GPS tracking functions. In *Crabtree v. Angie’s List, Inc.*,\(^ {35}\) the employees sued their employer: They objected to being tracked via GPS data through their personal cell phones and alleged that they were wrongfully denied overtime compensation in violation of the Fair Labor Standards Act.\(^ {36}\) The defendant, Angie’s List, did not provide company-issued laptops or cell phones for use outside the office, so the workers often used their personal electronic devices for work purposes.\(^ {37}\) As the


\(^{33}\) CAL. PEN. CODE § 637.7 (West 2018).


\(^{36}\) *Id.*

\(^{37}\) *Id.*
employees spent approximately 10–12 hours per day working but were paid based on an eight-hour day and 40-hour workweek, the employer sought to obtain GPS data from the employees’ personal cell phones to construct a timeline of when they actually were or were not working. The employees rejected this attempt because they believed that it raised a significant privacy concern, since this means that workers’ movements were tracked even outside of their working time, and the GPS data would not accurately portray whether they were working at any particular time.

The employer asserted that the data would be relevant to demonstrating whether the employees “left for the day, left for lunch, or some other unpaid break” during the hours when they could log onto their computer software and still be inactive. The employer looked for support in other district court cases. One of them was Head v. Professional Transportation, Inc., in which the employer was permitted to obtain GPS data from trucks used in the business. However, Angie’s List overlooked the difference between that case and their own because the trucks in Head were owned by the employer and were driven during the workday. Also, in Baclawski v. Mountain Real Estate Capital LLC, another case cited by Angie’s List, the court denied the employer’s request to image the employee’s cell phone and computer, and allowed access to data only from a Time Recording app because the data were not as intrusive as GPS data. According to Rule 26(b)(2)(C)(i), discovery of information is limited if it can be obtained from another source that is “more convenient, less burdensome, or less expensive,” and the

38 Id.
39 Id.
40 Crabtree, 2017 WL 413242, at *2.
41 Id.
42 Id.
44 Id. at *2.
45 Crabtree, 2017 WL 413242, at *2.
47 Id. at *1–2.
employer allegedly had an alternative in Crabtree v. Angie’s List, Inc.\textsuperscript{49} Rule 26(b)(1) also requires that data collection be “proportional to the needs of the case,”\textsuperscript{50} but Angie’s List did not demonstrate that the GPS data from employees would be more probative of their working habits than data they already had—such as records of business-related calls.\textsuperscript{51} Therefore, the Court found that the employer’s demand was not proportional to the needs of the case because “any benefit the data might provide is outweighed by Plaintiffs’ significant privacy and confidentiality interests.”\textsuperscript{52} Consequently, the employer’s motion was denied.\textsuperscript{53}

In addition, Haggins v. Verizon New Eng., Inc.\textsuperscript{54} is related to the GPS monitoring of employees. Between November 2008 and February 2009, Verizon New England (VNE) required its field technicians to carry company-issued cell phones provided by Verizon Wireless during work because supervisors needed to stay in touch with the workers in order to assign installation projects.\textsuperscript{55} The cell phones contained a GPS function, which allowed the employer to determine the location of the employees and monitor them.\textsuperscript{56} The cell phones had a feature called Field Force Manager, which allowed employees to punch in and out of work remotely, receive driving instructions, and access customer contact information in addition to the GPS functionality.\textsuperscript{57} The employees were represented by a union, the International Brotherhood of Electrical Workers Local 2324, which had a collective bargaining agreement (CBA) with the employer.\textsuperscript{58} The employees sued the employer, asserting that carrying the phones violated their privacy rights under Article 14

\textsuperscript{49} Crabtree, 2017 WL 413242, at *1.
\textsuperscript{50} Fed. R. Civ. P. 26(b)(1).
\textsuperscript{51} Crabtree, 2017 WL 413242, at *3.
\textsuperscript{52} Id.; See also Hespe v. City of Chicago, 2016 WL 7240754, at *3 (N.D. Ill. Dec. 15, 2016).
\textsuperscript{53} Crabtree, 2017 U.S. Dist. LEXIS 12927, at *3.
\textsuperscript{54} Haggins v. Verizon New Eng., Inc., 648 F.3d 50, 51 (1st Cir. 2011).
\textsuperscript{55} Id.
\textsuperscript{56} Id.
\textsuperscript{57} Id. at 53.
\textsuperscript{58} Id. at 51.

In response, the company asserted that it had adopted the cell phone policy pursuant to the Management Rights clause of the CBA.\(^{60}\) Also, by switching from pagers to cell phones, VNE sought to improve their ability to respond quickly to emergencies and improve its communication with the employees, who worked as Central Office Equipment Installation Technicians.\(^{61}\) The company also asserted that the GPS function was important to transmit driving instructions, process employee work hours, and determine whether an employee was at the place he or she was supposed to be.\(^{62}\)

The court held that the union’s claim about privacy was preempted by section 301 of the Labor Management Relations Act\(^{63}\) because their resolution would require interpretation of the CBA’s Management Rights clause.\(^{64}\) It also granted summary judgment on the third-party beneficiary claim as the plaintiffs had not produced any evidence about the intent of the contracting parties.\(^{65}\) In the end, the employees’ claims were dismissed.\(^{66}\)

**GPS on Vehicles**

---

\(^{59}\) *See Haggins*, 648 F.3d at 51; Mass. Const. art. XIV, pt. 1.; Mass. Gen. Laws ch. 214, § 1B.

\(^{60}\) *Haggins*, 648 F.3d at 52. (The “Management Rights” in the agreement stated: “Subject only to the limitations contained in this Agreement the Company retains the exclusive right to manage its business including (but not limited to) the right to determine the methods and means by which its operations are to be carried on, to assign and direct the work force and to conduct its operations in a safe and effective manner.”)

\(^{61}\) *Id.* at 53.

\(^{62}\) *Id.*


\(^{64}\) *Haggins*, 648 F.3d at 54.

\(^{65}\) *Id.*

\(^{66}\) *Id.* at 57.
There are laws and cases related to GPS tracking of vehicles as well. As an example of such law, an Illinois statute enacted in 2014 prohibits the utilization of GPS tracking to monitor the location of vehicle without the consent of the vehicle owner, unless the tracking is lawfully conducted by a law enforcement agency.\(^{67}\) It is therefore not illegal for employers to track the location of a company-owned vehicle used by its employees because the employer, the owner of the vehicle, consents to the tracking. Also, California Penal Code §637.7 prohibits the use of “an electronic tracking device to determine the location or movement of a person” via a “vehicle or other moveable thing,” unless “the registered owner, lessor, or lessee of a vehicle has consented to the use of the electronic tracking device with respect to that vehicle.”\(^{68}\)

Several courts have supported this idea by holding that an employee driving an employer-owned vehicle is not able to claim invasion of privacy when the employer tracks his or her whereabouts. Some example lawsuits are *Elgin v. Coca-Cola Bottling Co.*\(^{69}\) and *Tubbs v. Wynne Transp. Servs.*.\(^{70}\) In *Elgin v. Coca-Cola Bottling Co.*, the employer investigated the employee, an African-American employee, and other Caucasian employees when it had cash shortages from vending machines with no sign of forced entry.\(^{71}\) After the investigation, the employee was informed that a GPS tracker had been placed on his vehicle and that he had been cleared of wrongdoing.\(^{72}\) The employee did not experience any adverse employment action.\(^{73}\) The employee

\(^{67}\) 720 ILL. COMP. STAT. 5/21-2.5(c) (West 2012).

\(^{68}\) CAL. PEN. CODE § 637.7 (West 2018); Holly, *supra* note 30 (regarding the legal restriction and employee GPS monitoring).


\(^{71}\) Elgin, 2005 WL 3050633 at *1.

\(^{72}\) Id.

\(^{73}\) Id.
sued the employer, asserting that it violated the Missouri Human Rights Act and intruded upon his seclusion by performing a racially motivated investigation.\textsuperscript{74}

As part of the reasoning for the decision in favor of the employer, the court stated that the use of the tracking device on the company car, even though it was used by the employee, did not constitute a great intrusion because it revealed only highly public information of the van’s location and it should not be highly offensive to the employee because the van was the employer’s property.\textsuperscript{75} Similarly, in \textit{Tubbs v. Wynne Transp. Servs.}, no invasion of privacy for the employee was found when the employer had its trucks outfitted with GPS devices.\textsuperscript{76}

Also, in \textit{Gerardi v. City of Bridgeport},\textsuperscript{77} an employee hired as a fire inspector for the city’s fire department, sued the city and its fire chief, alleging violations of Conn. Gen. Stat. sections 31-48b\textsuperscript{78} and 31-48d.\textsuperscript{79} The city equipped fire inspectors’ vehicles with GPS without informing the inspectors and brought a disciplinary proceeding against the employee, claiming that he was not performing his job well based on the GPS data.\textsuperscript{80} Because the Connecticut Electronic Monitoring Act defines electronic monitoring as “the collection of information on an employer’s premises,” the court held that an employer’s off-site GPS monitoring of its own vehicles would not be prohibited by the Act.\textsuperscript{81} The court found that the statutes the plaintiff claimed were violated did

\textsuperscript{74} \textit{Id.}
\textsuperscript{75} \textit{Id.} at *4.
\textsuperscript{78} \textsc{conn. gen. stat. ann.} § 31-48b (west 2012) (limiting use of electronic surveillance devices by employers limited and prohibiting recording negotiations between employers and employees).
\textsuperscript{79} \textsc{conn. gen. stat. ann.} § 31-48d (west 2012) (requiring employers engaged in electronic monitoring required to give prior notice to employees).
\textsuperscript{80} \textit{Gerardi}, 2007 WL 4755007, at *1; \textsc{conn. gen. stat. ann.} § 31-48d (west 2012).
not apply and that plaintiff had not exhausted his administrative remedies as provided in the CBA. 82

“Many courts have found that employees do not have a reasonable expectation of privacy when employer-owned equipment or technology is involved, the employer has a legitimate business interest, and the intrusion occurs during normal work hours.”83 However, the law is less clear when an employer tries to track employees who use their personal vehicles for company business. For example, in Cunningham v. New York State Dept. of Labor, installing a GPS device on a vehicle owned by a state employee was found to be an unreasonable search.84 The New York State Department of Labor (DOL) suspected that the employee submitted false time reports and attached a GPS device to his car.85 Later, the GPS data substantiated the DOL’s suspicions, and the employee was terminated after a hearing.86 Because the employer search was within the workplace, the court concluded that the employer did not violate the New York or United States Constitution by not seeking a warrant first.87 However, the search was considered unreasonable because it was extremely intrusive as the GPS tracked the employee even on evenings, weekends, and vacation.88 The search as a whole was regarded as unreasonable because the employer did not make a

---

82 Gerardi, 2007 WL 4755007, at *8.
83 Clement L. Tsao, Kevin J. Haskins & Brian D. Hall, The Rise of Wearable and Smart Technology in the Workplace, A.B.A. NAT’L SYMP. ON TECH. IN LAB. & EMP. L. 1, 3 (2017); see also Garrity v. John Hancock Mutual Life Ins. Co., No. CIV.A. 00–12143–RWZ, 2002 WL 974676, at*2 (D. Mass. May 7, 2002) (finding no reasonable expectation of privacy for emails sent on computer system owned by employer and when the employer has a legitimate business interest); Thygeson v. U.S. Bancorp., No, CV–03–467–ST, 2004 WL 2066746, at *21 (D. Or. Sept. 15, 2004) (no reasonable expectation of privacy when the employee used his employer’s computer and network for personal use, saved personal information in a location that was accessible by his employer, and the employee handbook prohibited personal use of the employer’s computer).
84 Cunningham v. N.Y. State Dept. of Labor, 997 N.E.2d 468, 470 (N.Y. 2013); see also Tsao, Haskins & Hall, supra note 83, at 3.
85 Cunningham, 997 N.E.2d at 470–71.
86 Id. at 471.
87 Id. at 472.
88 Id. at 473.
reasonable effort to avoid tracking the worker outside of the worker’s working hours. The GPS evidence was thus suppressed.

On the other hand, other courts have reached different conclusions. In *El-Nahal v. Yassky*, a taxi driver Hassan El-Nahal filed a complaint against David Yassky, Commissioner Matthew Daus, Michael Bloomberg, and the City of New York, claiming that the New York City Taxi and Limousine Commission (TLC) violated 42 U.S.C. § 1983, the Fourth Amendment, and Article I, § 12 of the New York State Constitution by using GPS to track his whereabouts without probable cause or a search warrant. In this case, the court found that taxi drivers in New York City did not have an expectation of privacy in GPS data even though the drivers personally owned their vehicles because the state regulatory authorities required GPS tracking system to be installed in all cabs. Furthermore, regulations mandated use of the technology system and required taxi drivers to create handwritten trip records if the system was not working to keep records of the drivers’ activity.

When considering invasion of privacy claims, “courts generally weigh the employee’s expectation of privacy against the employer’s asserted business purposes for monitoring its employees.” *Katz v. United States* brought the term “reasonable expectations” into privacy issues and protections. “A reasonable expectation of privacy is an objective entitlement founded on broadly based and

---

89 Id.
90 *Cunningham*, 997 N.E.2d at 473.
92 Id.
94 *El-Nahal*, 993 F. Supp.2d at 466.
widely accepted community norms, and courts have recognized that lack of notice and consent typically support employees’ invasion of privacy claims.

### A. Harassment and Hostile Work Environment Issues

Beyond the concerns over privacy, electronic monitoring, as effectuated by productivity tracking applications, has the potential both for employer harassment of employees as well as for employer’s obligation to prevent harassment in the workplace. Consider that the previously mentioned Arias case essentially represents a supervisor’s abuse of the power to monitor. Notably, Arias’ supervisor at Intermex, Stubits, admitted that employees would be monitored while off duty and bragged that he knew Arias’ driving speed at any given moment. When the Plaintiff, Arias, uninstalled the app after expressing concern that the app was similar to a “prisoner’s ankle bracelet,” she was scolded for uninstalling the app, and was fired. Furthermore, after Intermex terminated Arias’ employment, the president and CEO of Intermex telephoned the vice president of another company, NetSpend, where Arias had been working in order to obtain medical benefits, and Arias was then fired by NetSpend. It is no surprise then, that Arias’s lawsuit included a claim for “retaliation” among other claims.

On the other hand, the prevalence of electronic monitoring at work finds justifications where the law may require, or at least encourage, it. Robert Sprague explains:

Hostile work environment jurisprudence is one [area in which law may compel surveillance]. *Burlington Industries, Inc. v. Ellerth*, and its companion case

---

98 Swaya & Eisenstein, supra note 9, at 13.
99 See Arias, supra note 21, at 17; Fort, Raymond & Shackelford, supra note 21, at 146; Sprague, supra note 13, at 223.
100 Arias, supra note 21, at 39.
101 Id.
102 Id. at 40.
103 Id.
104 Id. at 42.
Faragher v. City of Boca Raton, offers employers a defense against a hostile environment created by a supervisor (when no tangible employment action is taken) if it exercised reasonable care to prevent and correct promptly any sexually harassing behavior. This places greater pressure on employers to monitor employee behavior.105

Also, scholars like Harvey L. Fiser and Patrick D. Hopkins have considered how new technologies change what is reasonable in the context of negligent hiring liability and how that can create pressure, or even an obligation, to take certain data points.106 Although not perfectly aligned with monitoring productivity—given that this monitoring takes place pre-employment—the concept that employers may find themselves increasingly liable for things which they could have prevented by tracking might amplify the body of law facilitating surveillance. Moreover, because hiring technologies rely on patterns,107 an increasing obligation to monitor and screen before employment means there could be a rise in tracking productivity during employment, as the data created by employees will validate or challenge the factors considered in pre-employment screening. In other words, if employers are required to use technology in hiring then they will, in essence, be required to use technology to then evaluate those hiring decisions, which inevitably leads to workplace monitoring as a matter of mere compliance.

II. WEARABLE TECHNOLOGY

As wearable technology enters—and is sometimes specifically invented for—the workplace, it will be important to determine what legal protections are left for workers in the use of such devices in the workplace. Consider the haptic feedback wristband invented by Amazon, which

105 Sprague, supra note 13, at 224.
107 Id. at 61–62.
would use ultrasonic tracking to interact with inventory. The full name for the patent is the Ultrasonic Bracelet and Receiver for Detecting Position in 2D Plane, and the goal of the system is to save time locating items in warehouses and increase productivity. The system would monitor whether the worker has engaged with the correct inventory bins and reflect its analysis through haptic feedback. Amazon’s invention also has the ability to track workers beyond their performance, as it would know exactly what their hands were doing at any time.

According to a number of articles, magazines, and the US patent file, the system includes ultrasonic devices installed around the warehouse, the actual wristbands that warehouse workers wear, and a management module that oversees the activity. With an ultrasonic unit, the system tracks where the worker is in relation to a particular inventory bin they are seeking, and the bracelet buzzes when he or she is heading the wrong direction. By using the device, supervisors would also be able to identify when the workers pause, fidget, or take a bathroom break.

Amazon already holds the reputation for a management style that some allege results in the treatment of workers, especially low-paid laborers, like “human robots,” by having them conduct repetitive tasks as fast as possible. By allegedly timing their toilet breaks and using packing timers, the wristband, with its haptic feedback system, has raised further concerns about poorer

---

109 See Id.
110 Id.
113 Yeginsu, supra note 111.
114 Id.
115 Solon, supra note 112.
working conditions and the possibility of harsher workplace surveillance. In response to this, Amazon released a statement about its patents for wristband tracking systems in which it characterized concerns as misguided and asserted that the wristbands would improve the process of product retrieval from bins by “free[ing] up [workers’] hands from scanners and their eyes from computer screens.”

While Amazon has not yet used the device, the company uses wearable GPS tags to optimize warehouse routes. Moreover, Amazon is not the only inventor to contemplate wearable monitoring in the inventory context, with Intermec Technologies Corporation (Intermec) having twice applied for patents on an inventory assistance glove or wristband. While Intermec has not been awarded a patent, its invention would use wireless communication to provide feedback based on proximity to inventory bins, much like Amazon’s.

Other patents, granted or pending, may be relevant to wearable technology at work, even if unintentionally. MAD Apparel, Inc. (MAD), for example, has patented a vest that can monitor, provide feedback, and even make adjustments on its own in real time. While MAD mostly depicts its vest for exercise or other personal purposes, such technology could easily find its way into the workplace, especially in arenas of physical labor. Likewise, Stephan Heath’s (Heath)
application for electromagnetic frequency identification devices envisions multiple uses, from health care to law enforcement, for its technology in wearable form. Because Heath mentions that the technology would be applicable wherever predictive analytics are employed, its proposed use in wristbands, apparel, or “electronic skin tattoos” could be relevant to workers if the invention becomes reality. Also on the horizon could be the adaptation of virtual reality technologies, commonly thought of in a gaming context, to industrial purposes. Immersion Corporation’s patent application for a haptic feedback bodysuit discusses the ability to set permission profiles in different settings, thereby determining how haptic feedback is received (e.g., by controlling the type or the intensity). The application specifically references “work colleagues,” and the technology could certainly be used by work superiors who would downplay employee concerns by emphasizing the programmability of permission settings. Patent applications in health care contexts have similar crossover potential. One application by IBM describes a method to detect and correct poor posture, while smart exoskeletons that adjust via algorithm could go beyond correcting gait or preventing falls to instead correct deviations in path or transmit other data.

Hyundai’s proposed exoskeleton already has a workplace-intended variant.

125 Id.
127 Id.
While patents and patent applications may aid in predicting the future of wearable technology at work, other devices are already in use, and Amazon is not the only company that utilizes such technology to improve worker productivity and efficiency. For example, Mike Glenn, the executive vice president of market development and corporate communications at FedEx Corporation (FedEx), notes that wearable technology is already having a significant impact on FedEx employees, especially those involved in package sorting, pickup, and delivery, who wear ring scanners. In addition, United Parcel Service, Inc. (UPS) adopted a wearable scanning system in 2012 for its employees handling packages. The workers wear hands-free imagers on a finger and a small terminal on the wrist or hip so that they can quickly image barcodes and improve data entry. UPS also has sensors on its delivery trucks to collect data and “track the opening and closing of doors, the engine of the vehicle, and whether a seat belt is buckled.” Also, a Canadian startup, Thalmic Labs, invented an armband that lets a wearer control movements on a screen with a flick of the wrist. Moving beyond the consumer space, the company targets workers in industries like construction, field service, and healthcare where integration with smart glasses, like Google Glass, can be helpful. The XOEye glasses use HD video to entirely avoid

133 See Fort, Raymond & Shackelford, supra note 21 at 145; Couret, supra note 132.
136 Id.

Fitbit has become a particularly popular wearable technology for the workplace. Holding the top spot in the wearable market, it includes “a GPS monitor, a heart rate monitor, and an alarm and can even compile exercise summaries.”\footnote{Alexandra Troiano, Note, *Wearables and Personal Health Data: Putting a Premium on Your Privacy*, 82 Brook. L. Rev. 1715, 1716 (2017).} These days, employees are encouraged and many times rewarded for providing their information through such devices. For example, “[a]bout 90\% of companies now offer wellness programs, some of which encourage employees to use Fitbit and other devices that measure the quantity and intensity of their workouts and to employ simple visual and motivational tools to track their progress and help sustain their engagement.”\footnote{H. James Wilson, *Wearables in the Workplace*, Harv. Bus. Rev. (Sept. 2013), https://hbr.org/2013/09/wearables-in-the-workplace; See Fort, Raymond & Shackelford, supra note 21, at 153; Troiano, supra note 138, at 1717, 1722 (stating that wellness programs and wearable devices are implemented to increase productivity and health-related costs can be reduced).} Appirio, an information technology consulting company, distributed 400 Fitbits to employees as a part of its corporate wellness program.\footnote{Id.}

Also, smart watches that share many capabilities of fitness bands have pedometer technology or GPS functionality that can measure efficiency and improve employee safety.\footnote{See Patrick Van den Bossche, et al., *Wearable Technology in the Warehouse*, Supply Chain 24/7 (Feb. 1, 2016), http://www.supplychain247.com/article/wearable_technology_in_the_warehouse (last visited Aug. 22, 2018).} These devices optimize the storage locations of tools and aim to minimize workers’ movement—similar to Amazon’s haptic wristband—by tracking the steps required to execute particular operations and automatically shutting down machines when employees are in danger.\footnote{Id.} Employees could also
use their smart watches to easily update locations and quantities of inventories, and conduct transactional operations.\textsuperscript{143}

**Cap and Helmet**

SmartCap, invented by an Australian company called EdanSafe, detects the wearer’s brain activity and delivers data to workers about fatigue levels in real time by reading their brain waves.\textsuperscript{144} Once per second, an algorithm analyzes the data collected by the Cap to determine the wearer’s level of alertness, and transmits this information by Bluetooth to the user.\textsuperscript{145} Audial and visual alarms are activated when the user’s fatigue level drops, and the sensors can tell when the Cap is removed.\textsuperscript{146} Supervisors can monitor the output and fatigue levels of numerous, cap-wearing employees during past shifts using the SmartCap and its Fatigue Manager Server.\textsuperscript{147} The Cap was initially developed for use in the mining industry and is currently used by many truck drivers to increase their productive output and physical safety.\textsuperscript{148} “A headband version is also in production.”\textsuperscript{149}

The DAQRI helmet is a similar product that allows workers to see GPS-guided blueprints via augmented reality vision in real time and spot welds by seeing through walls.\textsuperscript{150} In addition to a visor that presents visual overlays of information, like instruction and warnings, the helmet has

\textsuperscript{143} Id.
\textsuperscript{145} Id., supra note 144.
\textsuperscript{146} Id.
\textsuperscript{147} Id.
\textsuperscript{148} See Turner, supra note 119.
\textsuperscript{149} See Coxworth, supra note 144.
\textsuperscript{150} See Turner, supra note 119.
“cameras and sensors that can measure, record, and track information about the wearer’s surroundings.” The helmet is used by companies like California-based Hyperloop.

**High-Tech Vests**

Similar to how the Amazon wristband tracks workers’ location, high-visibility vests are fitted with GPS to enhance workplace safety by alerting workers when they are entering a hazardous zone on a construction site. This high-tech vest not only reduces danger by tracking workers throughout a geo-fenced jobsite, but it also optimizes workflow by allowing managers to track workers’ movements.

Another example of wearable technology is the implantation of radio-frequency identification (RFID) microchip under workers’ skin to facilitate services. In July 2017, more than 50 out of 80 employees at a River Falls, Wisconsin technology company called Three Square Market volunteered to implant the device under their skin between the thumb and pointer finger. One employee at the company said he readily agreed to embed a microchip into his hand and was satisfied with the experience, as the chip allowed him to easily swipe into secure rooms, log into his computer, and use vending machines. The RFID technology was approved by the Food and Drug Administration in 2004.

Lastly, Hitachi created a device affixed to a lanyard called the Business Microscope. Acting as an advanced employee security badge, the Business Microscope is embedded with “infrared

---

153 See Holmes, *supra* note 144.
154 Brummond & Thornton, *supra* note 151.
155 See Miller, *supra* note 134; Yeginsu, *supra* note 111.
156 See Miller, *supra* note 134.
157 Id.
sensors, a microphone sensor, and a wireless communication device,” which allows for monitoring of how and when office workers interact with each other by recognizing when two employees wearing the badges within a certain distance of each other and recording face time and behavioral data. The device tracks everything by sending information to management about how often an employee walks around the office, when he or she stops to talk to other co-workers, and whether he or she contributes at meetings. Regarding the device’s capability to detect “who talks to whom, how often, where, and how energetically,” which can provide a better understanding of how frequently different departments interact and improves organizational communication and quantitative evaluation of efficacy, but it has not offered examples of how the device is actually used. Since the Business Microscope was first developed in 2007, Hitachi has collected “over one million days of human behavior and big data.”

Exoskeletons

In addition to these relatively small, wearable devices, exoskeletons, or wearable robotics, are “bionic suits that use springs and counterweights to enhance human power and protect from injuries associated with heavy lifting and repetitive movements.” They comprise of robotics and computers, or “more specifically, motors and sensors and software and novel algorithms that

161 Id.
162 Turner, supra note 119.
163 See Greene, supra note 160.
164 Turner, supra note 119.
165 See Greene, supra note 160.
166 Dov Greenbaum, Ethical, Legal and Social Concerns Relating to Exoskeletons, 45 SIGCAS COMPUTERS & SOC’Y 234, 234 (2015).
167 Holmes, supra note 144.
combine the former.” Because the most experienced construction workers are in their forties and fifties, and construction work can be strenuous, the use of exoskeletons can benefit both workers and the industry by reducing the physical impact of such work. Ekso Bionics created the Ekso Works Industrial Exoskeleton, which lets a person lift heavy tools as if they weighed nothing at all. Also, exoskeletons are also suited to help those who have with restricted mobility because of paralysis or weakened limbs by allowing people to move in a more sustained way or walk despite spinal injuries. Exoskeletons in the workplace can thus prevent work-related musculoskeletal ailments and improve productivity by reducing absences due to illness and disability, even though they may cause some ethical concerns about dehumanization.

Exoskeletons may also collect user data, such as “location information, usage information, neural input information, vitals data and other private information relating to the user,” so that it can be used for product feedback or medical necessity. For example, DARPA’s exoskeleton, which is designed to be strong and pro-active, helps the wearer know the precise location and movements of his or her colleagues, detect and interpret sounds, communicate wirelessly, and monitor his or her mood as well as mental and physical conditions.

168 Greenbaum, supra note 166, at 234.
169 Holmes, supra note 144.
170 See Adam Rogers, We Try a new Exoskeleton for Construction Workers, WIRED (Apr. 28, 2015, 7:00 AM), https://www.wired.com/2015/04/try-new-exoskeleton-construction-workers/.
171 Greenbaum, supra note 166, at 234.
172 Isabelle Wildhaber, The Robots are Coming: Legalities in the Workplace, HR MAGAZINE (June 20, 2016), http://www.hrmagazine.co.uk/article-details/the-robots-are-coming-legalities-in-the-workplace.
173 Id.
174 See Greenbaum, supra note 166, at 236.
175 Id. at 239.
International Examples of Workplace Wearable Technology

The expansion of wearable technology at the workplace is not limited to the United States. For instance, similar to Amazon’s patents for haptic wristbands, Tesco, a British multinational groceries and merchandise retailer, has adopted location tracking wrist computers. It required its workers at a distribution center in Ireland to wear the armbands, officially named the Motorola arm-mounted terminals. The band tracked the goods workers gathered, reduced the time spent marking clipboards, and allowed the employers to measure employee productivity by providing data points on the workers’ loading, unloading, and scanning speeds. It also allocated tasks to the wearer, forecasted their completion time, and quantified the worker’s movements through the facility to provide analytical feedback, verifying the correct order or alerting a worker who performs below expectations. Except for the workers’ lunch breaks, any distribution center workers’ activity, including time using the toilet or spent at the water fountain, was tracked and marked as decreasing the workers’ productivity score.

Moreover, companies are expected to adopt more of these types of wearable devices that improve efficiency by reducing the sequence of movements. According to Wearables in the Workplace by H. James Wilson, emerging wearables, most notably Google Glass, will replace the process required to check smartphones for work with simple gestures that take much less time. In addition, Microsoft is developing armbands that project keyboards and displays onto

---

177 See Rutkin, supra note 10.
180 See Wilson, supra note 139.
181 See Wilson, supra note 139.
182 See Wilson, supra note 139.
wearers’ wrists.\textsuperscript{183} Other early prototypes are based on predictive feedback system of wearer’s movements.\textsuperscript{184} Of particular interest to labor scholars is the implication that XOEye, Daqri, and other such wearable workplace technologies) may allow employers to shift dangerous jobs to untrained, inexperienced, or unskilled workers.

\textbf{B. Privacy Concerns}

Although wearable devices can contribute to business productivity, these devices also raise new legal issues.\textsuperscript{185} The privacy of the worker is a primary concern, given that these devices are worn in close proximity to the body.\textsuperscript{186} In addition, wearable technology may pose challenges to traditional privacy practices and principles like the Fair Information Practice Principles (FIPPs), which are guidelines concerning fair information practice in an electronic marketplace and for the Internet of Things.\textsuperscript{187} The basic privacy principles include: collection limitation, purpose specification, use limitation, accountability, security, notice, choice, and data minimization.\textsuperscript{188} As many wearable devices lack input mechanisms and extensively collect, store, and transmit personal data on a cloud, they are at a high risk of challenging basic privacy principles. For

\begin{footnotesize}
\footnote{\textsuperscript{183} See id.}
\footnote{\textsuperscript{184} See id.}
\footnote{\textsuperscript{185} See id.; Suddath, \textit{supra} note 178 (explaining that from 2007 to 2012, the average number of full-time employees in a Tesco superstore fell nearly 18 percent); Turner, \textit{supra} note 119 (explaining that, according to a Rackspace study, workers who integrate wearable technology are 8.5 percent more productive and 3.5 percent more satisfied, and management can get insight about human labor through worker data.).}
\footnote{\textsuperscript{188} See OECD Guidelines, \textit{supra} note 187, at 70–71; Phaik Lin Goh, \textit{supra} note 186, at 31; Wolf, Polonetsky & Finch, \textit{supra} note 187, at 4.}
\end{footnotesize}
example, screenless devices may generate a great amount of invisible data, thus straining the limits of notice and consent.\textsuperscript{189}

Moreover, because of the greater potential for employer surveillance posed by wearables, there is a possibility that the National Labor Relations Act (NLRA) is challenged. The National Labor Relations Board holds that an employer engages in unlawful surveillance “when it surveils employees engaged in Section 7 activity by observing them in a way that is ‘out of the ordinary’ and therefore coercive.”\textsuperscript{190} Since it is difficult for employees to reject using wearable devices in the employment relationship\textsuperscript{191} and employers have the ability to track each employee’s precise location and physiological activity, wearable technology could have a chilling effect on protected concerted activity under the NLRA.\textsuperscript{192}

However, despite these concerns about privacy for employees’ personal information, case law has demonstrated that the law is unlikely to effectively protect employees from privacy intrusions via wearable technology.\textsuperscript{193} The Electronic Communications Privacy Act (ECPA) and the Stored Communications Act (SCA) prohibit the “intentional interception, access and disclosure of wire, oral or electronic communications and data,” but contain employer-centric exceptions.\textsuperscript{194} Also, legal protection of privacy is weak. While some laws may aim to protect unsuspecting employees or unauthorized gathering of information, case law has shown that few

\textsuperscript{189} See Peppet, supra note 179, at 117; Phaik Lin Goh, supra note 186, at 32.
\textsuperscript{190} Aladdin Gaming, LLC, 345 N.L.R.B. 585, 585–86 (2005), petition for review denied, 515 F.3d 942, 947 (9th Cir. 2008); Tsao, Haskins & Hall, supra note 83, at 1; Section 7 of the Act provides: “Employees shall have the right to self-organization, to form, join, or assist labor organizations, to bargain collectively through representatives of their own choosing, and to engage in other concerted activities for the purpose of collective bargaining or other mutual aid or protection.” National Labor Relations Act, 29 U.S.C. §157 (2012).
\textsuperscript{191} Adam D. Moore explains that the consent takes the following form: if an employment is to continue, then an employee must agree to such-and-so kinds of surveillance. Moore calls this “thin consent” because it is assumed that jobs are hard to find and the employee needs the job. See Adam D. Moore, Employee Monitoring and Computer Technology: Evaluative Surveillance v. Privacy, 10 BUS. ETHICS Q. 697, 701 (2000).
\textsuperscript{192} See Tsao, Haskins & Hall, supra note 83, at 1.
\textsuperscript{193} Phaik Lin Goh, supra note 186, at 32.
\textsuperscript{194} Brummond & Thornton, supra note 151.
protections exist when an employee consents to information gathering and use within the scope of her employment. The law “generally does not protect employees . . . from information that is willingly shared and/or information that is gathered after consent is provided.” Regarding this, some states, including California and Texas, have laws protecting employees from equipment tracking without express consent, and the proposal of the Location Privacy Protection Act and other similar bills like the Geolocation Privacy and Surveillance Act (GPS Act) demonstrate that lawmakers are increasingly concerned about location information.

In United States v. Simons, the court held that an employee does not have a reasonable expectation of privacy regarding his use of the Internet when the employer has policies about Internet use. Because the employer’s privacy policy in this case stated that it would “audit, inspect, and/or monitor” employees’ use of the Internet, the employee was found not to have an objectively reasonable expectation of privacy. This conclusion was based on the Supreme Court case of O’Connor v. Ortega, in which the Court found that the employee’s reasonable expectation of privacy should be analyzed in the employment relationship context. Also, Seff v. Broward County shows that the Americans with Disabilities Act will not limit employers from requiring employees to submit health and fitness data as part of establishing a “bonafide benefit plan.”

195 See Fort, Raymond & Shackelford, supra note 21, at 166.
196 Id. at 145.
197 Phaik Lin Goh, supra note 186, at 33.
198 206 F.3d 392, 398 (4th Cir. 2000).
199 Id.
201 691 F.3d 1221, 1224 (11th Cir. 2012) (In this case, the employer’s wellness program was a term of the county’s benefit plan); Brown, supra note 159, at 28.
C. Potential for Discrimination

Another legal issue concerning wearable technology is the potential for discriminatory employer actions in contravention of the Americans with Disabilities Act (ADA) and the guidelines of the Equal Employment Opportunity Commission. The ADA prohibits discrimination against a qualified individual in regard to employment on the basis of disability and also prohibits employers from administering medical examinations and other disability-inquiries to employees unless the examination or inquiry is job-related and consistent with business necessity.

Wearable devices present cause for concern because they are very adept at tracking health data and providing a picture of an employee’s health. Managers prohibited from conducting medical examinations on employees can have access to physical data, including health and disability information, about the workers, regardless of the employer’s intentions. For example, devices that read heart rates reveal potential medical information. Also, employees who might not be reaching productivity standards due to a medical condition or disability could be discriminated against, bosses could potentially abuse the power to monitor by targeting employees.

---

203 The EEOC’s enforcement guidance states that a “medical examination” is any procedure or test “that seeks information about an individual’s physical or mental impairments or health.” See U.S. EQUAL EMP’T. OPPORTUNITY COMM’N, Notice 915.002, ENFORCEMENT GUIDANCE: DISABILITY-RELATED INQUIRIES AND MEDICAL EXAMINATIONS OF EMPLOYEES UNDER THE AMERICANS WITH DISABILITIES ACT (2000), https://www.eeoc.gov/policy/docs/guidance-inquiries.html.
204 Id. (The EEOC’s enforcement guidance states that a “disability-related inquiry” is a question that “is likely to elicit information about a disability.”)
206 Id.
207 See Haggin, supra note 20 (“[I]f a warehouse employee does poorly on tracked activity measures on the job, the employer might need to consider whether the data could indicate a physical disability that would require the employer to make a reasonable accommodation”)
208 See Turner, supra note 119.
209 See Haskins, supra note 205, at 74; Turner, supra note 119; Haggin, supra note 20.
populations of a certain gender, race, or age disproportionally, and it would be very easy for employers to gain access to the personal data of employees and use that data without consent in promotion and retention decisions. Furthermore, as some scholars have noted, corporate wellness programs may lead employers to consider data outside work hours, such as sleep patterns or dietary habits, when determining employee benefits or compensation, potentially discriminating against employees in reliance on data entirely outside of the conventional workplace.

Wearable devices such as exoskeletons also have implications for the ADA. The ADA requires employers to provide reasonable accommodations, including acquisition or modification of equipment or devices, to qualified employees with disabilities, unless doing so would pose an undue hardship to the business. Because exoskeletons, unlike other wearable devices above, can be considered a mitigating measure, which is an element that “eliminates or reduces the symptoms or impact of an impairment,” employees using exoskeletons may not be regarded as having a disability. Therefore there is a concern about defining an employee as disabled and providing reasonable accommodation, because while employers cannot ignore the fact that a person is disabled because he or she uses an exoskeleton, they cannot force an

210 See Turner, supra note 119.
211 See Fort, Raymond & Shackelford, supra note 21 at 158.
216 See Greenbaum, supra note 166, at 237–38.
employee to use an exoskeleton.\footnote{Id.} It is also unclear whether compensation may be different for employees who use exoskeletons and for those who do not.\footnote{Id. at 239.}

Moreover, wearable technology that collects health-related information of employees can also implicate the Health Insurance Portability and Accountability Act (HIPAA), which establishes national standards for protecting individually identifiable health information, or protected health information (PHI).\footnote{See 45 C.F.R. §160.103 (2014); 45 C.F.R. §162.923 (2012); 45 C.F.R. §164.306 (2013).} However, HIPAA applies to the PHI of “covered entities” and their business associates,\footnote{See 45 C.F.R. §160.103 (2014); 45 C.F.R. §162.923 (2012); 45 C.F.R. §164.306 (2013).} and since employees with wearable devices and their employers are not considered “covered entities,” such employees are not subject to HIPAA.\footnote{See 45 C.F.R. §160.103 (2014); Haskins, supra note 205, at 76; Phaik Lin Goh, supra note 186, at 32–33.}

\textbf{D. \textit{Worker Safety and Workers’ Compensation}}

Wearable technology such as bionic suits, exoskeletons, and helmets can improve worker performance and safety while also allowing employers to promote biometric analysis beyond merely health and wellness.\footnote{See Michael B. Stack, \textit{Wearable Technology in Workers’ Compensation}, AMAXX (Jul. 27, 2017), http://blog.reduceyourworkerscomp.com/2017/07/wearable-technology-workers-compensation/.} Better safety and employee performance also lead to reductions in workers’ compensation program costs for employers and higher profit margins.\footnote{See Garry Mathiason et al., \textit{LITTLER ON LEGAL COMPLIANCE SOLUTIONS FOR THE TRANSFORMATION OF THE WORKPLACE THROUGH ROBOTIC ARTIFICIAL INTELLIGENCE, AND AUTOMATION} § 3.1 (2017) (“For example, employers with thousands of employees report that reducing the lost-time period by only a few days can result in saving millions of dollars, both in terms of reductions in wage-loss benefits (i.e., ‘indemnity’ benefits) and medical costs.”); Greenbaum, supra note 166, at 239 (contending that workers’ compensation for employees may be limited in part due to the use of exoskeletons in the workforce); John Rehm, \textit{Exoskeletons and the Workplace}, WORKER’S COMPENSATION WATCH (Dec. 7, 2015), https://workerscompensationwatch.com/2015/12/07/exoskeletons-and-the-workplace/ (positing that the use of exoskeletons could result in fewer workers’ compensation claims); see also Stack, supra note 222; Turner, supra note 119.} Mathiason et al., in Littler Reports, describe that this is realized in two ways: first, as robots replace works that
are dangerous, strenuous, or repetitive, workers are likely to suffer less work-related injuries, and second, applications that are designed to assist workers in performing physical requirements of their jobs will improve the ability of injured workers to return to work.\textsuperscript{224}

Michael B. Stack, an expert in workers’ compensation, also explains that reduction in workers’ compensation cost for employers is made possible through real-time reporting of an employee’s location, immediate reporting of an employee in distress, which allows summoning emergency assistance, and measuring of the force of impact for diagnosis and treatment of workplace injury.\textsuperscript{225} As an example of real-time reporting, wearable technology can caution employees regarding their posture, therefore assisting employees performing sedentary work to make adjustments to reduce injury at the workstation.\textsuperscript{226} One major corporation, Target, is using activity and sleep-tracking devices to promote health habits for employees, and employers are showing greater interest in using wearable technology to prevent occupational injuries.\textsuperscript{227} In addition, assistive wearable devices that help employees suffering from severe spinal cord injuries and information they can provide in relation to post-injury care, progress, and return-to-work issues contribute to the change in workers’ compensation.\textsuperscript{228}

Furthermore, employers can use data from wearable devices to defend themselves against an employee’s workers’ compensation claim. For example, since Fitbit “monitors sleep patterns, decides how many hours a user sleeps, and determines the quality and efficiency of that sleep”

\textsuperscript{224} See Mathiason et al., \textit{supra} note 223, at § 3.1.
\textsuperscript{225} Stack, \textit{supra} note 222; \textit{see also} Van den Bossche, et al., \textit{supra} note 141 (“Employee biometrics could be monitored to identify which operations or situations cause excessive exertion on an operator that could result in future injury.”).
\textsuperscript{226} Stack, \textit{supra} note 222.
\textsuperscript{228} Stack, \textit{supra} note 222.
and a wearer can be compared to the “average” sleeper, such that an employer could use that information as evidence of the sleep-deprivation of the employee at the time of the accident.\textsuperscript{229}

Although no specific lawsuit was found regarding workers’ compensation for workplace injury caused by wearable technology, there have been reports of a Canadian law firm—cited by many law reviews and news articles—which used evidence collected by a wearable device in a personal injury case.\textsuperscript{230} It is the first known personal injury case in which the plaintiff used activity data from a Fitbit to show the effects of an accident in a legal proceeding.\textsuperscript{231} The plaintiff was apparently injured in 2010 and sought to use the Fitbit data in November 2014.\textsuperscript{232} The plaintiff was injured when she was working as a personal fitness trainer, and she attempted to use her Fitbit data as evidence of her diminished physical activity resulting from a work-related injury.\textsuperscript{233} With the help of a analytic company called Vivametrica that prepared analytical reports from aggregated Fitbit data and a law firm in Calgary, she aimed to show that her “post-injury activity levels were lower than the baseline for someone of the same age and profession.”\textsuperscript{234} Although not an employment law case, this shows that information from wearable devices could be used as evidence in litigation\textsuperscript{235} and could also help to support or disprove workers’

\begin{thebibliography}{9}
\bibitem{peyton2016c} See Peyton, \textit{supra} note 230, at 391; CLM, \textit{supra} note 229, at 6.
\bibitem{peyton2016d} CLM, \textit{supra} note 229, at 6.
\bibitem{peyton2016e} Peyton, \textit{supra} note 230, at 391.
\bibitem{peyton2016f} \textit{Id.; see} Crawford, \textit{supra} note 230; Olson, \textit{supra} note 230.
\bibitem{chauriyecomm2016} See Nicole Chauriye, Note, \textit{Wearable Devices as Admissible Evidence: Technology Is Killing Our Opportunities to Lie}, 24 \textit{CATH. U. J.L. & TECH.} 495, 507 (2016); Peyton, \textit{supra} note 230, at 391; CLM, \textit{supra} note 229, at 6; \textit{see also} Chauriye, \textit{supra} note 235, at 509–11 (discussing \textit{Commonwealth v. Risley}, a non-employment case in which Fitbit data was used in the courtroom, and the Fitbit data contradicted the statements of an alleged victim).
\end{thebibliography}
compensation, and harassment claims.\textsuperscript{236} It is important to note that prior to the Americans with Disabilities Act Amendments Act (“the ADAA”) becoming law, employers could “account for the ameliorative effects of efforts that employees have undertaken to lessen the negative effect of their conditions when determining whether they were substantially limited in a major life activity…” But passage of the ADAA “changed this paradigm by [defining] an individual’s disability without reference to any but the most rudimentary ameliorative measures.”\textsuperscript{237}

Although wearable devices could reduce workers’ compensation costs with the data they collect, employers must also consider the injuries that wearable devices may cause. Wearable products with a heads-up display, such as the DAQRI helmet or Google Glass are of particular concern because employees may be distracted by images on the displays while operating or driving heavy equipment at workplaces like construction sites.\textsuperscript{238} In addition, robots, or exoskeletons, that are incompatible with the human body or poorly designed or implemented could damage muscles, tendons, and nerves, especially when performing repetitive tasks.\textsuperscript{239} Also, exoskeletons could negatively impact workers, particularly those with pre-existing conditions, such as chronic obstructive pulmonary disease (COPD), because wearing such a device may increase chest pressure.\textsuperscript{240} Lawyers explain that workers’ compensation and other claims could be brought against employers in the event of an accident involving such devices

\begin{footnotes}
\footnotetext[237]{Gregory A. Hearing & Marquis W. Heilig, \textit{Recent Developments in Employment Law and Litigation}, 2 Tort Trial \& Insurance Practice Law Journal 45, 322 (2010). “Specifically, the ADAA notes that a vision impairment, properly remedied by eyeglasses or contact lenses, is not a disability.” \textit{Id}.
\footnotetext[238]{Brummond & Thornton, \textit{supra} note 151.
\footnotetext[239]{See Mathiason et al., \textit{supra} note 223, at § 3.1.
and advise that employers who intend to implement these wearable devices should consider adjusting their policies and protocols to limit their liability.241

II. EMPLOYEE RIGHTS: RESEARCH QUESTIONS FOR LEGAL SCHOLARS

In this section, I detail unanswered questions regarding the governance of these new emerging technologies in the workplace.

A. A Reasonable Expectation of Privacy for Employees

A reasonable expectation of privacy is the fulcrum on which employee-monitoring cases turn. One problem is that while a reasonable expectation of privacy is well defined for Fourth Amendment cases, it is not as defined within the employment context, and some scholars have argued that workplaces operate as “private governments” with employers exercising near dictatorial power over what privacy rights may be granted to workers.242 While *Katz v. United States* was the case that introduced the term “reasonable expectation,”243 that term has been defined as “an objective entitlement founded on broadly based and widely accepted community norms;”244 and courts have recognized that, in the private sphere, lack of notice and consent typically support employees’ invasion of privacy claims.245 Yet, courts have also found that employees do not have a reasonable expectation of privacy when employer-owned equipment or

241 See Mathiason et al., supra note 223, at § 3.1 (stating that when determining eligibility for workers’ compensation, injuries caused by robots will be treated the same as injuries caused by using other tools used in the workplace like hammers or computer keyboards); Brummond & Thornton, supra note 151 (suggesting that employers consider revising their safety policies and protocols).
243 389 U.S. 347, 360 (1967) (Harlan, J., concurring) (note that this case involved government action, and non-governmental employers are not subject to Fourth Amendment restrictions that would be afforded to government employees).
245 Swaya & Eisenstein, supra note 95, at 13.
technology is involved, the employer has a legitimate business interest, and the intrusion occurs during normal work hours.\textsuperscript{246}

Emerging technologies and their advanced data collection functions challenge the notion that a “reasonable expectation of privacy” continues to hold any well-settled definition. This is especially true for devices, such as wearable technologies that continue to collect data even during off-work hours. Consider the recent Supreme Court case, \textit{Carpenter v. United States},\textsuperscript{247} in which the Court held that accessing cell phone location data without a warrant was a violation of the Fourth Amendment.\textsuperscript{248} Although some might argue that any precedents from the \textit{Carpenter} case should be constrained to the Fourth Amendment, the Ninth Circuit reasoned, in \textit{O’Connor v. Ortega},\textsuperscript{249} that the employee’s reasonable expectation of privacy should be analyzed in the employment-relationship context.\textsuperscript{250} This means that as employees are obliged to interact with emerging technologies in the workplace, which by their operation collect employee data—sometimes without affirmative consent—the question of what constitutes or should constitute a reasonable expectation of privacy for employees will remain an important one for legal scholars.

\textbf{B. The Battle over Employee Data}

The emerging technologies of productivity applications and wearable technology also raise legal questions about the collection and control of employee data. Compounding the problems with data generated by wearable technology at work is the fact that there are no real federal laws to limit the collection of data that is not facially-related to a protected category. As my coauthors

\textsuperscript{246} Tsao, Haskins & Hall, \textit{supra} note 83, at 3; \textit{see also} Thygeson v. U.S. Bancorp., No. CV--03--467--ST, 2004 WL 2066746, at *21 (D. Or. Sept. 15, 2004) (no reasonable expectation of privacy when the employee used his employer’s computer and network for personal use, saved personal information in a location that was accessible by his employer, and the employee handbook prohibited personal use of the employer’s computer).

\textsuperscript{247} 138 S. Ct. 2206, 2206 (2018).

\textsuperscript{248} \textit{Id.} at 2221, 2223.

\textsuperscript{249} 280 U.S. 709, 717 (1987).

\textsuperscript{250} \textit{Id.}
and I explained in a previous article, the applicability of various federal statutes in the context of surveillance is extremely narrow. This gives employers broad license to monitor employees. Furthermore, the sheer volume of data that can legally be obtained from and about employees could make data-generated evidence seem especially persuasive, enhancing biases that may already exist.

Federal policy has also promoted workplace wellness programs, which can be a vehicle for justifying the use of wearable technology and its monitoring functions in the workplace. That surveillance could prove critical to workers’ compensation decisions, as companies seek to reduce costs related to worker injuries. With data obtained through wellness programs, employers could use predictive analytics to determine which employees are more at risk of getting injured. Such preventative monitoring means that data will influence not just how workers’ compensation determinations are made, but also which workers will remain employed. Factors like weight or whether a worker smokes could be included in those calculations, and there would be no federal law to protect workers from that genre of discrimination. By connecting a governmental push for wellness programs to opportunities to save costs from workers’ compensation, employers can (absent relevant state law) discriminate against workers using data that has been collected under the guise of helping employees achieve their personal health goals. Past research has also revealed that employee data collected as part of workplace wellness programs are frequently sold to third parties without the employee’s knowledge or consent.

---

252 Id. at 764–67.
253 Id. at 767.
The battle over employee data, however, will not only be about limits on what data can be collected and who controls that data. Instead, at least through the lens of workers’ compensation claims and on the assumption that such claims go to trial, the real fight will be over how the data get interpreted. Some legal scholars like Scott R. Peppet have already posed the question of whether consumers will accept “the possible use of [wearable technology data] by an adversary in court [or] an insurance company when denying a claim.” Just as Vivametrica was called upon in the Canadian case to compare personal Fitbit data to some baseline, an employer could compare data from the wearable device against a larger population. As one legal scholar notes, this creates two problems: (1) a comparison not specific to the person or their circumstances; and (2) variance among data analysis methods (whether from an outside firm or engineered into the device itself). Even where there is agreement on which data is admissible, methods of interpretation will be contested. This could lead to wildly divergent results whereby someone differently situated from the general population is deemed responsible for their own injury because their patterns stray from a median, or where the same case could just as easily go the other way because a different algorithm analyzed the samples. Therefore, setting standards, not just for which data are admissible for workers’ compensation claims, but for how the data will be interpreted seems critical.

Accuracy of the data from wearable technology, however, remains an issue. Fitbit, in particular, has been subject to class action lawsuits challenging the accuracy of features like sleep or heart rate monitoring. These raise concerns for Fitbit data being introduced in court as

---

255 Peppet, supra note 179, at 89.
256 Peyton, supra note 230, at 392.
257 Id. at 392–93.
evidence for or against workers’ compensation claims. Data from wearable technologies may be made even less accurate if device users try to “game” their design flaws. Furthermore, data quality cannot be separated from the overarching impact of surveillance on workers. One study found that monitoring could inherently make an individual nervous, which could then skew the health data being collected.259 Thus, those with the “worst” results on metrics generated by wearable technology could simply be those most concerned about being watched. As such, the data wearable technology produces might be biased towards those who are comfortable being surveilled. Device-generated data as part of court testimony poses an extra challenge when the analytical processes that produce the data are themselves secret, as they would be with commercial devices.260 As a result, bias for the data, or a belief that data cannot “lie,” goes unchecked, because understanding the way in which data operate requires information that is unavailable, even if the decision-maker has the requisite technological knowledge.

Despite the flaws of electronic data as a witness, keeping data from wearable devices out of litigation will be nearly impossible in the current legal landscape. With practically no expectation of privacy at work,261 it will be difficult for employees to keep data collected from work devices out of court. Wearable technology, like other surveillance methods, is presented as beneficial to workers.262 Yet, potential harms caused by steep economic incentives or a lack of information, as well as the asymmetrical power relationship between workers and employers, call into question the voluntary use of such devices.263

259 Solon, supra note 137.
261 Ajunwa, Crawford & Schultz, supra note 16, at 748.

Electronic copy available at: https://ssrn.com/abstract=3247286
CONCLUSION

It is no accident that one of the corporate leaders in workplace management technology is Kronos, named after the Greek God of Time.²⁶⁴ Even before Taylor’s time series experiments in the early 20ᵗʰ century, employers have been preoccupied with maximizing employee productivity in order to achieve a surplus. The twenty-first century has ushered in new technologies uniquely designed to attend to the employers’ interests in profit-maximization, but those new technologies also bring with them new concerns about employee privacy and the potential to effectuate employment discrimination. In sum, the future of productivity applications and wearable technology will see more devices that will generate more data. There will be legal controversies as to who owns the data, who controls the data, what data should be introduced in legal proceedings and how they should be interpreted. These issues should, however, not overshadow the greater socio-legal question of whether employers should collect such data in the first place.