CHIPPING AWAY AT WORKPLACE PRIVACY: THE IMPLANTATION OF RFID MICROCHIPS AND EROSION OF EMPLOYEE PRIVACY

Wes Turner*

INTRODUCTION

On August 1, 2017, a small technology firm in Wisconsin, Three Square Market, held a "chip party" where many employees were implanted with microchips.[1] The program was voluntary, and more than fifty of the firm's eighty employees opted in.[2] The chips replace key cards and passwords, allowing employees to enter the building, sign into their computers, and purchase food with the wave of a hand.[3] The microchip is a Radio Frequency Identification Device (RFID), which allows one device to communicate with another when in close proximity.[4] Over the past few decades, technological advancements have shifted the employee-employer relationship; implanting employees with a microchip represents a new peak in this trend.

---

*. J.D. (2019), Washington University in St. Louis.

1. Trent Gillies, *Why Most of Three Square Market's Employees Jumped at the Chance to Wear a Microchip*, CNBC (Aug. 13, 2017, 9:00 AM), https://www.cnbc.com/2017/08/11/three-square-market-ceo-explains-its-employee-microchip-implant.html [https://perma.cc/VF3K-M2QY].

2. Maggie Astor, *Microchip Implants for Employees? One Company Says Yes*, N.Y. TIMES (July 25, 2017), https://www.nytimes.com/2017/07/25/technology/microchips-wisconsin-company-employees.html [https://perma.cc/29BW-BHC2].

3. Gillies, *supra* note 1.

4. RFID Frequently Asked Question: What is RFID?, RFID JOURNAL, https://www.rfidjournal.com/faq/show?49 [https://perma.cc/HVG2-QCYR]. More specifically,

> RFID[] is a generic term for technologies that use radio waves to automatically identify people or objects. There are several methods of identification, but the most common is to store a serial number that identifies a person or object, and perhaps other information, on a microchip that is attached to an antenna (the chip and the antenna together are called an RFID transponder or an RFID tag). The antenna enables the chip to transmit the identification information to a reader. The reader converts the radio waves reflected back from the RFID tag into digital information that can then be passed on to computers that can make use of it.

Id.

Although these chips do not have GPS capabilities, Three Square Market is designing a chip that does.[5] Many companies already use some form of GPS and data tracking to monitor employee performance. United Parcel Service (UPS), for example, uses a system called "telematics."[6] UPS's telematics system tracks *everything*. A UPS delivery truck has two hundred sensors to track delivery information such as backup speed or seatbelt use. Each step along the delivery is tracked, with a supervisor receiving the information in real time: route, speed, parking, package retrieval, and even time spent buckling the seat belt.[7] UPS claims that in 2010 telematics saved 1.7 million driving miles, 15 million minutes of idling time, and 103,000 gallons of gas, while allowing the company to eliminate roughly ten percent of its vehicles.[8] Following this trend, Amazon recently patented a wristband to track warehouse employee hand movement and vibrate when an employee is reaching in the wrong bin.[9] Walmart, not to be outdone, recently patented audio surveillance technology to catalog noises at cash registers ranging from conversations to "rustling noises."[10] The employers' desire for efficiency gains from monitoring employees is clear: increase productivity while automating the supervision required to do so.

The legal protections for employee privacy concerns from excessive monitoring are based on 1980s workplaces and technology—GPS devices on company cars and video surveillance in the workplace.[11] Advances in technology have already pushed the limits of the usefulness of 1980s legal protections. Wearable technologies, such as Fitbits and smartwatches, leave employees vulnerable to "adverse employment decisions, discrimination,

5. Gillies, *supra* note 1.

6. Esther Kaplan, *The Spy Who Fired Me*, HARPER'S MAG. (Mar. 2015), https://harpers.org/archive/2015/03/the-spy-who-fired-me/ [https://perma.cc/CTJ8-NW5B].

7. *Id.*

8. *Id.*

9. Matt Novak, *Amazon Patents Wristband to Track Hand Movements of Warehouse Employees*, GIZMODO (Jan. 31, 2018, 1:30 PM), https://gizmodo.com/amazon-patents-wristband-to-track-hand-movements-of-war-1822590549 [https://perma.cc/6GZW-8P7X].

10. Caroline O'Donovan, *Walmart's Newly Patented Technology for Eavesdropping on Workers Presents Privacy Concerns*, BUZZFEED NEWS (July 11, 2018, 6:05 PM), https://www.buzzfeednews.com/article/carolineodonovan/walmart-just-patented-audio-surveillance-technology-for#.gia8Mn4Vg [https://perma.cc/7NX5-U7GW].

11. *See infra* Sections I.A. and I.C.

and invasions of privacy rights."[12] Personal smartphones used for work, coupled with workplace productivity and security apps, likely give rise to similar problems.[13] But an implanted and immovable microchip may take these problems to a new extreme.

Part I of this Note tracks the development of employee privacy rights and how these rights have responded to recent changes in technology and work. Part II analyzes how microchip implants will likely be treated and makes additional policy recommendations.

I. HISTORY

A. Privacy, the Constitution, and the Common Law

The Fourth Amendment to the United States Constitution provides privacy protection from government searches.[14] Often, an individual's expectation of privacy determines the degree of protection accorded by the Fourth Amendment.[15] For example, in *Smith v. Maryland*, the Supreme Court used a two-part inquiry to determine whether the Fourth Amendment protected the defendant's privacy interest.[16] The first question is "whether the individual, by his conduct, has 'exhibited an actual (subjective) expectation of privacy.'"[17] "The second question is whether the individual's

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

13. *See, e.g.*, Arias v. Intermex Wire Transfer, L.L.C., No. 1:15-cv-01101-JLT, at *1 (E.D. Cal. 2017) (discussed *infra* Section I.D); Kamika S. Shaw, *GPS Tracking of Employee Devices: How Much is Too Much?*, ONLABOR (May 8, 2017), https://onlabor.org/gps-tracking-of-employee-devices-how-much-is-too-much/ [https://perma.cc/7ARB-EUCQ] (applying the privacy-based car GPS framework to smartphone tracking) .

14. The Fourth Amendment states that

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized

U.S. CONST. amend. IV.

15. *See* Smith v. Maryland, 442 U.S. 735, 740 (1979); *see also* Katz v. United States, 389 U.S. 347, 353 (1967) (holding that the government's activities in electronically listening to and recording the defendant's words in a public telephone booth violated the privacy upon which the defendant "justifiably relied" and thus constituted a search and seizure within the meaning of the Fourth Amendment).

16. 442 U.S. 735, 740.

17. *Id.* (quoting *Katz*, 389 U.S. at 361).

subjective expectation of privacy is 'one that society is prepared to recognize as reasonable,'" that is, whether the individual's expectation is objectively reasonable.[18] In order to receive the protections of the Fourth Amendment, there must be an objectively reasonable subjective expectation of privacy.[19] Accordingly, in *Smith*, the Court held that individuals have no expectation of privacy in the telephone numbers they voluntarily surrender to third parties, establishing what is now known as the third-party doctrine.[20]

The Supreme Court introduced the reasonable-expectation-of-privacy analysis into the public employment context in *O'Connor v. Ortega*.[21] In *O'Connor*, the Court held that even where the government is acting as an employer, the Fourth Amendment may protect government employees from searches by their government employer.[22] In *O'Connor*, an employee at a public hospital was being investigated for sexually harassing two other employees.[23] The public employer searched the employee's office without his permission.[24] The Court held that the governmental interest in the "efficient and proper operation of the workplace" must be balanced against the privacy interests of employees in their place of work.[25] Thus, the Court found that employees have a protectable privacy interest recognized by the Fourth Amendment at the workplace, although it provides less protection than at home.[26] Because Ortega did not share his desk or file cabinet, and

18. *Id.* (quoting *Katz*, 389 U.S. at 361).
19. *Id.* at 743.
20. *Id.* at 743–45. For an explanation of the third-party doctrine, see, e.g., Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561 (2009). The future of the third-party doctrine is less certain following *Carpenter v. United States*, 138 S. Ct. 2206 (2018), where the Court held that the third-party doctrine at least does not extend to location data given to cell towers through the automatic communication between cell phones and cell towers.
21. 480 U.S. 709, 711–12 (1987).
22. *Id.* at 725–26.
23. *Id.* at 712.
24. *Id.* at 713.
25. *Id.* at 719–20.
26. The Court held that

> Given the societal expectations of privacy in one's place of work . . . , we reject the contention made by the Solicitor General and petitioners that public employees can never have a reasonable expectation of privacy in their place of work. Individuals do not lose Fourth Amendment rights merely because they work for the government instead of a private employer. The operational realities of the workplace, however, may make some employees' expectations of privacy unreasonable when an intrusion is by a supervisor rather than a law enforcement official. Public employees' expectations of privacy in their offices, desks, and file

there was no hospital policy on the subject, Ortega had a reasonable expectation of privacy in the contents of his office.[27] The Court then remanded the case to determine whether the employer's intrusion was reasonable in scope and inception given the expectation of privacy Ortega had.[28]

Private-sector employees, however, are not protected by the Fourth Amendment; naturally, there is no state action involved when a private employer acts. Instead, private-sector employees must rely on either the common law or a patchwork of statutory protections to protect their privacy interests at work.

The tort "intrusion upon the seclusion of another" is the "most commonly used [tort] to protect employee privacy against excessive employer intrusion."[29] Despite *O'Connor*'s nonbinding precedent, the courts import the same basic idea: a determination of reasonable expectation of privacy with the goal "to distinguish personal from work-related matters."[30] However, this tort must also be "highly offensive to a reasonable person,"[31] a higher standard than the public employment cases. Instead of balancing privacy expectations with the reasonableness in the inception and scope of intrusion, private employment cases turn on privacy expectations and whether the intrusion is "highly offensive to a reasonable person."[32]

> cabinets, like similar expectations of employees in the private sector, may be reduced by virtue of actual office practices and procedures, or by legitimate regulation.

Id. at 717 (emphasis omitted).

27. *Id.* at 718–19.

28. *Id.* at 729.

29. Ronald P. Angerer II, *Moving Beyond a Brick and Mortar Understanding of State Action: The Case for a More Majestic State Action Doctrine to Protect Employee Privacy in the Workplace*, 4 CHARLOTTE L. REV. 1, 9 (2013).

30. *See* Pauline T. Kim, *Electronic Privacy and Employee Speech*, 87 CHI.-KENT L. REV. 901, 907–08 (2012).

31. *Id.*

32. *See, e.g.*, K-Mart Corp. Store No. 7441 v. Trotti, 677 S.W.2d 632, 637 (Tex. Ct. App. 1984) (holding that an employee did have a legitimate expectation of privacy in a locker where the employee used his own lock and the search was highly offensive). However, because of the nature of the employment relationship, a reasonable expectation of privacy is often not found. *See, e.g.*, Terrell v. Rowsey, 647 N.E.2d 662, 667 (Ind. Ct. App. 1995) (finding the plaintiff did not have a reasonable expectation of privacy in his vehicle when parked on the employer's property during work hours). Common areas have no expectation of privacy. *See, e.g.*, Craig v. M & O Agencies, Inc., 496 F.3d 1047, 1061–62 (9th Cir. 2007) (holding there is no reasonable expectation of privacy under Arizona law when

A comparison of two GPS-tracking cases illuminates this difference. In *Cunningham v. New York Department of Labor*, a tracking device was placed on a public employee's car prompted by the concern that the employee was submitting false time reports.[33] The court first found that GPS tracking constituted a search for Fourth Amendment purposes.[34] Relying on *Ortega v. O'Connor*, the court also held that the location of a vehicle used in the course of employment is entitled to the same degree of privacy as personal effects on a desk.[35] The court next used the inception-and-scope framework from *O'Connor* and found the search was unreasonable in its scope because "[i]t examined much activity with which the State had no legitimate concern . . . ."[36] Because the car was owned by the employee and tracked twenty-four hours a day, seven days a week, it was impossible "to eliminate all surveillance of private activity" and therefore the surveillance exceeded the necessary scope.[37]

In *Elgin v. St. Louis Coca-Cola Bottling Co*, the private employer, in the course of investigating a cash shortage, attached a GPS tracking device to a company-owned vehicle used by an employee during both work and off-work hours.[38] The company did not tell the employee that a GPS device was placed on the vehicle until the investigation had concluded.[39] The employee brought an invasion-of-privacy claim under Missouri common law.[40] The court granted summary judgment for the employer.[41] The court held that because "an automobile's path of travel is, as a matter of law, not [a] secret and private subject matter as necessary for a viable invasion of privacy claim under Missouri law," the plaintiff did not have a high enough reasonable expectation of privacy to surpass a "highly offensive to a reasonable person" standard.[42] The court determined that the type of

---

a supervisor followed a woman into the bathroom because, although the stall was private, the area immediately outside was a common area).

33. 997 N.E.2d 468, 470 (N.Y. 2013).
34. *Id.* at 471.
35. *Id.* at 472.
36. *Id.* at 473.
37. *Id.*
38. No. 4:05CV970-DJS, 2005 WL 3050633, at *1 (E.D. Mo. Nov. 14, 2005).
39. *Id.*
40. *Id.* at *3.
41. *Id.* at *4.
42. *Id.* at *3.

information obtained by the GPS tracker was limited to the whereabouts of the vehicle and was therefore permissible.[43]

The limits of both the Fourth Amendment and common-law privacy protection are seen with mandatory suspicionless drug testing. The Supreme Court recognized in *Skinner v. Railway Labor Executives' Ass'n* the high level of expectation of privacy one has in the sample-collection process:

> There are few activities in our society more personal or private than the passing of urine. Most people describe it by euphemisms if they talk about it at all. It is a function traditionally performed without public observation; indeed, its performance in public is generally prohibited by law as well as social custom.[44]

Nevertheless, the Court held that public employers could still mandate drug testing so long as there was a "compelling Government interest."[45] Following *Skinner*, despite the high level of expectation of privacy, courts of appeals consistently upheld government-mandated drug-testing policies by finding compelling justifications.[46]

Private-sector employees fared no better. Some plaintiffs were successful where the act of observing the urination violated a right to privacy,[47] and the state of California found suspicionless drug testing where there was no legitimate employer interest to be a violation of privacy.[48] These cases are,

---

43. *Id.*; *see also* Tubbs v. Wynne Transp. Servs. Inc., No. H-06-0360, 2007 WL 1189640, at *10–11 (S.D. Tex. Apr. 19, 2007) (granting employer's motion for summary judgment on the tort claim of invasion of privacy finding that Tubbs, who drove employer-owned trucks that were each outfitted with a GPS device that transmitted the truck's location to the company, failed to show the objective standard of a reasonable expectation of privacy).

44. 489 U.S. 602, 617 (1989) (quoting Nat'l Treasury Emps. Union v. Von Raab, 816 F.2d 170, 175 (5th Cir. 1987)).

45. *Id.* at 633. Although the employer in *Skinner* was a privately owned railroad, the Court treated it as a public employer because its actions were mandated by federal law. *Id.* at 614-15.

46. "For example, in all eight reported courts of appeals' decisions in 1989 which followed *Skinner* . . . and involved broad Fourth Amendment challenges to employer drug testing policies, the employer prevailed on appeal." Pauline T. Kim, *Collective and Individual Approaches to Protecting Employee Privacy: The Experience with Workplace Drug Testing*, 66 LA. L. REV. 1009, 1018 n.38 (2006).

47. *See, e.g.*, Kelley v. Schlumberger Tech. Corp., 849 F.2d 41, 43–46 (1st Cir. 1988).

48. Luck v. S. Pac. Transp. Co., 267 Cal. Rptr. 618, 631–32 (Ct. App. 1990).

however, the exception, and the overwhelming majority of private drug-testing cases did not find a privacy violation, even where the employer had no rational business interest or suspicion.[49]

B. Statutory Protection

There are a few federal statutory protections against the more egregious privacy violations, although most commentators believe that these are woefully inadequate.[50] Title I of the Electronic Communications Privacy Act (ECPA), known as the Wiretap Act, governs electronic communications in transit and prohibits interception without consent.[51] The Wiretap Act's main weakness comes from the "in transit" and "interception" requirements.[52] Employers do not need to intercept any communications when they are stored on employer-owned devices because employees have little expectation of privacy.[53]

---

49. *See, e.g.*, Baggs v. Eagle-Picher Indus., Inc., 957 F.2d 268 (6th Cir. 1992); Horne v. J.W. Gibson Well Serv. Co., 894 F.2d 1194 (10th Cir. 1990); Frye v. IBP, Inc., 15 F. Supp. 2d 1032 (D. Kan. 1998); Hart v. Seven Resorts Inc., 947 P.2d 846 (Ariz. 1997); Gilmore v. Enogex, Inc., 878 P.2d 360 (Okla. 1994); Stein v. Davidson Hotel Co., 945 S.W.2d 714 (Tenn. 1997); Jennings v. Minco Tech. Labs, Inc., 765 S.W.2d 497 (Tex. Ct. App. 1989); Roe v. Quality Transp. Servs., 838 P.2d 128 (Wash. Ct. App. 1992).

50. *See, e.g.*, Ifeoma Ajunwa, Kate Crawford & Jason Schultz, *Limitless Worker Surveillance*, 105 CAL. L. REV. 735, 750 (2017); Michael Z. Green, *Against Employer Dumpster-Diving for Email*, 64 S.C. L. REV. 323, 334 (2012); Kara Lyons, *Corporate Reputation Management vs. Employee Privacy*, LAW360 (July 29, 2015, 12:39 PM), http://www.law360.com/articles/684280/corporate-reputation-management-vs-employee-privacy [https://perma.cc/SNR2-ATJL].

51. 18 U.S.C. § 2511 (2012). The Wiretap Act 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 . . .

Id.

52. Ajunwa et al., *supra* note 50, at 749.

53. *See* United States v. Simons, 206 F.3d 392, 398–99 (4th Cir. 2000). Furthermore, consent is considered a viable waiver, and with the employment-at-will doctrine, consent is easily attainable. Pauline T. Kim, *Bargaining with Imperfect Information: A Study of Worker Perceptions of Legal Protection in an At-Will World*, 83 CORNELL L. REV. 105, 106 (1997) (noting the limited negotiation power left to the employee under an at-will employment contract).

Title II of the ECPA, known as the Stored Communications Act (SCA), protects electronic communications held in storage.[54] The phrasing of the act, however, "belies its age."[55] The Act focuses on authorization to access a facility, a concept no longer pertinent with the advent of the internet and other technologies. Moreover, the focus on authorization does little, if anything, to protect the large majority of workers who are employed-at-will.[56] In practice, every employer has de facto authorization.

The Computer Fraud and Abuse Act (CFAA)[57] once again fails to adapt to the modern workplace. The CFAA prohibits individuals from accessing a computer without authorization and thereby obtaining information.[58] In workplaces where employers provide a computer and where authorization is easily obtainable, the CFAA is of little help.

Employment discrimination statutes may provide some protections against discrimination from the *misuse* of the data legally collected but does nothing to hamper the collection of data itself. The Americans with Disabilities Amendments Act,[59] Title VII of the Civil Rights Act of 1964,[60] the Age Discrimination in Employment Act,[61] the Employment Non-Discrimination Act,[62] the Pregnancy Discrimination Act,[63] and the Genetic Information Nondiscrimination Act[64] all protect against employment-related discrimination resulting from the data collected. The Health Insurance Portability and Accountability Act (HIPAA) was designed to protect the confidentiality of patients' health information.[65] To the extent that the data being collected is individually identifiable health information,

54. 18 U.S.C. §§ 2701–2712 (2018).
55. Ajunwa et al., *supra* note 50, at 749.
56. *Id.* at 749–50; *see generally* Kim, *supra* note 53.
57. 18 U.S.C. § 1030(a)–(h) (2018).
58. *Id.* § 1030(a).
59. 42 U.S.C. § 12112(a) (2018).
60. *Id.* § 2000e-2 (2018).
61. 29 U.S.C. §§ 621–634 (2018).
62. Employment Non-Discrimination Act of 2013, S. 815, 113th Cong. (2013).
63. Pregnancy Discrimination Act, S. 995, 95th Cong. (1978).
64. Genetic Information Nondiscrimination Act of 2008, Pub. L. No. 110-233, 122 Stat. 881 (2008).
65. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996).

HIPAA may provide some protection against its misuse and dissemination.[66]

State laws are more targeted to specifically address employee privacy rights. State-law protections, however, vary drastically from state to state. Connecticut and California, for example, have very strong protections.[67] Many states, however, provide little or no additional statutory protections for employees. Only two states, Delaware and Connecticut, require employers to inform their employees that their activities are being monitored.[68] In the RFID context, a handful of states prohibit the mandatory implantation of an RFID microchip as a condition of employment.[69] A patchwork of state protections, nonetheless, still leads to patches of unprotected employees.

---

66. The statute defines "individually identifiable health information" as the "subset of health information" that

> (1) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual; and (i) identifies the individual; or (ii) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Id. § 1171(6).

67. In California, employers cannot eavesdrop on employees' private telephone conversations without consent, or conduct video or audio surveillance in specified areas such as bathrooms or locker rooms. CAL. LAB. CODE § 435 (West 2019). California also prohibits the tracking of vehicles without consent. CAL. PENAL CODE § 637.7 (West 2019). California additionally outlaws requiring employees to undergo the subcutaneous implantation of identification devices. CAL. CIV. CODE § 52.7 (West 2019).

68. Kaplan, *supra* note 6.

69. These states include Arkansas, California, Missouri, Montana, Nevada, North Dakota, Oklahoma, and Wisconsin. *Radio Frequency Identification (RFID) Privacy Laws*, NAT'L CONFERENCE OF ST. LEGISLATURES, http://www.ncsl.org/research/telecommunications-and-information-technology/radio-frequency-identification-rfid-privacy-laws.aspx [https://perma.cc/436S-MRD5] (last updated Nov. 6, 2018). Legislation is also currently pending in New York. Glenn Bain, *State Pol Proposes Legislation to Ban Employers from Planting Microchips in Workers*, N.Y. DAILY NEWS (Sept. 21, 2017, 6:14 PM), https://www.nydailynews.com/news/politics/n-y-pol-reveals-bill-ban-employers-microchipping-workers-article-1.3512050 [https://perma.cc/H3TK-7CR5].

C. Worker Surveillance

Given the little expectation of privacy in the workplace,[70] a "highly offensive" standard, and no federal statutory prohibitions, private employers are able to monitor and surveil employees in the workplace with near impunity.[71] For example, an employer can video-record or photograph employees in plain view at the workplace.[72] Hidden cameras, however, may give rise to issues when placed in bathrooms or changing rooms,[73] and surveillance of protected concerted activity is likely a violation of the National Labor Relations Act (NLRA).[74] Even surveillance outside of the workplace may be legal if the actions are not impermissibly intrusive. Surveillance of activities performed in public or plain sight, for example, is almost always permissible.[75] Some courts and commentators have argued that filing a claim such as worker's compensation waives any reasonable

70. Some scholars have criticized relying on a reasonable-expectation-of-privacy test as inherently insufficient because it relies on employer policies and practices, rather than existing social norms to determine reasonableness. Business practices and the existence of any legitimate business concern can be used to undermine an employee's privacy. *See, e.g.*, Matthew W. Finkin, *Employee Privacy, American Values, and the Law*, 72 CHI.-KENT L. REV. 221, 226 (1996); Don Mayer, *Workplace Privacy and the Fourth Amendment: An End to Reasonable Expectations?*, 29 AM. BUS. L.J. 625 (1992).

71. *See, e.g.*, SIMONE BROWNE, DARK MATTERS: ON THE SURVEILLANCE OF BLACKNESS 12–17 (2015) ("This history can be traced through many pivotal points including massive efforts through warfare, slavery, globalization, and other forms of colonialism used to control and exploit workers.").

72. Smith v. Colo. Interstate Gas Co., 777 F. Supp. 854, 857 (D. Colo. 1991) (placing employee under "close observation" at desk was not an invasion of privacy); Thomas v. General Elec. Co., 207 F. Supp. 792 (W.D. Ky. 1962).

73. *Compare* Brazinski v. Amoco Petroleum Additives Co., 6 F.3d 1176, 1184 (7th Cir. 1993) (finding that employee must prove that she had actually been observed in a state of undress), *with* Hernandez v. Hillsides, Inc., 211 P.3d 1063, 1066 (Cal. 2009) (holding that placement of cameras can be an invasion of privacy).

74. *See, e.g.*, Danzansky-Goldberg Mem'l Chapels, Inc., 264 N.L.R.B. 840, 843 (1982).

75. *See, e.g.*, Munson v. Milwaukee Bd. of Sch. Dirs., 969 F.2d 266, 270–71 (7th Cir. 1992) (watching a public school principal to ascertain whether his residence conformed to school board policy was not a violation of privacy where he was observed on public streets or highways); Brady v. Wal-Mart Stores, Inc., 43 F. Supp. 2d 652, 657 (S.D. Miss. 1998) (holding surveillance acceptable as to a medical leave claim); York v. Gen. Elec. Co., 759 N.E.2d 865, 868 (Ohio Ct. App. 2001) (investigating worker's compensation claim when employee was in an area observable by the public is acceptable).

expectation of privacy.[76] Regardless, trespassing on a person's home, is likely a step too far.[77]

The modern workplace, however, uses more advanced forms of surveillance than video cameras and photographs in order to monitor productivity. 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."[78] One survey "found that more than 50% of 239 large corporations surveyed are using 'nontraditional' monitoring techniques."[79] Employers have long tracked the time the employee is engaged with the machine, the error rate, or the time per stroke to compare against the employee's prior performance or against average performances.[80] Now, employers are able to put RFID chips and microphones in employee ID badges or hide them in lights.[81] Companies collect data on employees' whereabouts and "latency"—length of time in between tasks, length and

76. *See* McLain v. Boise Cascade Corp., 533 P.2d 343, 346 (Or. 1975) ("[O]ne who seeks to recover damages for alleged injuries must expect that his claim will be investigated and he waives his right of privacy to the extent of a reasonable investigation."); Daniel P. O'Gorman, *Looking Out for Your Employees: Employers' Surreptitious Physical Surveillance of Employees and the Tort of Invasion of Privacy*, 85 NEB. L. REV. 212 (2006). This is however not the dominant view. See *Beaumont v. Basham*, 205 S.W.3d 608 (Tex. Ct. App. 2006), for an example of the dominant view that the filing of such a claim does not waive an employee's reasonable expectation of privacy.

77. *See, e.g.*, Ass'n Servs. v. Smith, 549 S.E.2d 454 (Ga. Ct. App. 2001). Interestingly, gaining access to a person's home through deceit was ruled not to be "highly offensive to a reasonable person." Turner v. Gen. Adjustment Bureau, Inc., 832 P.2d 62, 67 (Utah Ct. App. 1992).

78. *The Rise of Workplace Spying*, THE WEEK (July 5, 2015), http://theweek.com/articles/564263/rise-workplace-spying [https://perma.cc/232Q-XXQT].

79. Rick Wartzman, *Workplace Tracking is Growing Fast. Most Workers Don't Seem Very Concerned*, FAST COMPANY (Mar. 20, 2019), https://www.fastcompany.com/90318167/workplace-tracking-is-growing-fast-most-workers-dont-seem-very-concerned [https://perma.cc/RM4E-47CN].

80. This was topic was addressed as early as 1989. SHOSHANA ZUBOFF, IN THE AGE OF THE SMART MACHINE: THE FUTURE OF WORK AND POWER (1989) (explaining the history of employers' tracking an employee's performance as the employee engages with a machine).

81. The company Enlightened is the biggest seller of this technology. It currently collects data from over 350 companies including fifteen percent of Fortune 500 companies. Rebecca Greenfield, *New Office Sensors Know When You Leave Your Desk*, BLOOMBERG (February 14, 2017, 6:30 AM), https://www.bloomberg.com/news/articles/2017-02-14/new-office-sensors-know-when-you-leave-your-desk [https://perma.cc/5Q7V-N7XY]; *see also There Will Be Little Privacy in the Workplace of the Future*, THE ECONOMIST (Mar. 28, 2018), https://www.economist.com/special-report/2018/03/28/there-will-be-little-privacy-in-the-workplace-of-the-future [https://perma.cc/NQ5U-D83S].

tone of conversations, and frequency of bathroom breaks.[82] The data is then used as "people analytics" to increase productivity and make personnel decisions.[83] At its best, the technology is used to ensure hospital caregivers wash their hands[84] or to prevent insider trading.[85] At its worst, over-surveillance breeds inhumane proposals such as electrocuting truck drivers whose eyes fall off the road for a few seconds[86] and creates a workplace Panopticon. Ifeoma Ajunwa argues, "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."[87]

D. Bring Your Own Devices and Wearable Technologies

Increasingly, people use their personal mobile phones and laptops for work.[88] A recent survey found that seventy-two percent of companies in the United States already had or planned to have bring-your-own-device (BYOD) policies by late 2018.[89] The use of a device for both personal and

---

82. *See, e.g.*, Josh Bersin, *The Geeks Arrive in HR: People Analytics Is Here*, FORBES (Feb. 1, 2015, 6:12 PM), https://www.forbes.com/sites/joshbersin/2015/02/01/geeks-arrive-in-hr-people-analytics-is-here/2/#5c752e0c2902 [https://perma.cc/5KXZ-4RHR]; Ryan Derousseau, *The Tech that Tracks Your Movements at Work*, BBC (June 14, 2017), http://www.bbc.com/capital/story/20170613-the-tech-that-tracks-your-movements-at-work [https://perma.cc/HVR6-3CE8].

83. Derousseau, *supra* note 82.

84. *Id.*

85. Olivia Solon, *Big Brother Isn't Just Watching: Workplace Surveillance Can Track Your Every Move*, THE GUARDIAN (Nov. 6, 2017, 3:00 PM), https://www.theguardian.com/world/2017/nov/06/workplace-surveillance-big-brother-technology [https://perma.cc/3CJ4-GQGB].

86. This idea was proposed by the Roads Minister of Australia and never gained traction as the Transportation Workers Union quickly quashed it. Benedict Brook, *Proposal to 'Electric Shock' Drowsy Truck Drivers in Wake of Fatal Crashes Slammed*, NEWS.COM.AU (Jan. 17, 2018, 6:31 PM), http://www.news.com.au/technology/innovation/motoring/proposal-to-electrocute-drowsy-truck-drivers-in-wake-of-fatal-crashes-slammed/news-story/d69c25f8fe814993848509b6dad40731 [https://perma.cc/X6GX-XWHP].

87. Ajunwa et al., *supra* note 50, at 743.

88. For an overview of the rapid rise of bring-your-own-device policies, see Melinda L. McLellan, James A. Sherer & Emily R. Fedeles, *Wherever You Go, There You Are (With Your Mobile Device): Privacy Risks and Legal Complexities Associated with International "Bring Your Own Device" Programs*, 21 RICH. J.L. & TECH. 11, 12–23 (2015).

89. Michael Lazar, *BYOD Statistics Provide Snapshot of Future*, INSIGHT (Nov. 16, 2017), https://www.insight.com/en_US/content-and-resources/2017/01182017-byod-statistics-provide-snapshot-of-future.html [https://perma.cc/5VRK-EC59].

professional purposes blurs the reasonable-expectation-of-privacy analysis.[90] Typically, employees have no reasonable expectation of privacy while using employer-owned work devices.[91] One likely has a reasonable expectation of privacy in their own home,[92] and a lowered one at their office desk.[93] But as the workplace changes, this distinction is not so sharp. Workers telecommute from a home office,[94] and one-third of employees are required to check work emails outside of work.[95] From 2005 to 2012, remote working increased seventy-nine percent "and now makes up 2.6 percent of the American workforce, or 3.2 million workers."[96] Moreover, a large portion of the workforce is now expected to be on call, all but eliminating the line between personal time and work time.[97]

BYOD policies show how the distinction between work and personal devices can lead to difficult questions of privacy rights. For example, *Arias*

---

90. Emily J. Tewes, Comment, *#Privatesphere: Can Privacy Laws Adequately Protect Employees Amidst the Complexities of the Modern Employment Relationship?*, 57 SANTA CLARA L. REV. 287, 306–07 (2017).

91. *See, e.g.*, Garrity v. John Hancock Mut. Life Ins. Co., No. CIV.A. 00-12143-RWZ, 2002 WL 974676, at *2 (D. Mass. May 7, 2002) (finding that an employee had no reasonable expectation of privacy in work emails on a work computer); Smyth v. Pillsbury Co., 914 F. Supp. 97, 100–01 (E.D. Pa. 1996) (finding similarly that an employee had no reasonable expectation of privacy in work email on work computer). *But see* Stengart v. Loving Care Agency, Inc., 990 A.2d 650, 663–34 (N.J. 2010) (holding that emails from a password protected personal account used on a company computer between plaintiff and attorney were protected by a reasonable expectation of privacy).

92. Telecommuting has already blurred the distinction between home and work. Some software used to monitor freelance workers at home is extremely intrusive. For example, Upwork monitors freelance employees by taking random screenshots of their desktop to send to the person hiring to ensure they are not wasting time. Sue Shellenbarger, *Work at Home? Your Employer May Be Watching*, WALL ST. J., (July 30, 2008, 11:59 PM), http://www.wsj.com/articles/SB121737022605394845 [https://perma.cc/G57T-KA3W].

93. *See* O'Connor v. Ortega, 480 U.S. 709 (1987).

94. Kaplan, *supra* note 6.

95. Jim Harter et al., *Most U.S. Workers See Upside to Staying Connected to Work*, GALLUP (Apr. 30, 2014), http://news.gallup.com/poll/168794/workers-upside-staying-connected-work.aspx?g_source=work%20email&g_medium=search&g_campaign=tiles [https://perma.cc/SAJ5-ZQNM].

96. Alina Tugend, *It's Unclearly Defined, but Telecommuting Is Fast on the Rise*, N.Y. TIMES (Mar. 7, 2014), http://www.nytimes.com/2014/03/08/your-money/when-working-in-your-pajamas-is-more-productive.html [https://perma.cc/BRD4-ZTMK].

97. Kaplan, *supra* note 6; *see also* Ilya Marritz, *In New Economy, Minimum-Wage Workers Are Always on Call*, WNYC (Nov. 21, 2013), http://www.wnyc.org/story/new-economy-many-employers-expect-open-availability [https://perma.cc/8HND-MMW3].

v. Intermex Wire Transfer[98] is one of the first challenges to GPS tracking of an employee's smartphone:

> Intermex required all employees to install an app, Xora, which contained a GPS function that allowed the company to track the employee's whereabouts through the employee's phone. The plaintiff asked her supervisor whether [] actions off the job would also be tracked. The supervisor told her off duty whereabouts would be tracked, and confirmed that the plaintiff was expected to keep her phone on 24/7 to answer any calls from clients. The plaintiff told her supervisor she was fine with the tracking while she was on duty, but expressed discomfort with being tracked when she was off duty and during the weekends. . . . Ultimately, the plaintiff decided to uninstall the app, [] was reprimanded for doing so[,] . . . [and] was fired [a few weeks later]. Arias sued Intermex for invasion of privacy, violations of the California Constitution and California Labor Code, wrongful violation, and unfair business practices, among other things. The case ultimately settled out of court.[99]

Even in a state with stronger employee protections such as California, the inherent weakness embedded in an employment-at-will regime easily undermines employee rights; because an employee can be fired for any reason so long as it is not illegal, the employee must overcome the difficult burden of proving retaliation.

In 2010, the Supreme Court passed on an opportunity to fit the *O'Connor* framework into the modern workplace. In *City of Ontario v. Quon*, a public employee claimed he had a reasonable expectation of privacy while using an employer-owned cell phone that he was permitted to use for personal purposes.[100] The Court did not determine whether the employee had a

98. No. 1:15-cv-01101-JLT, at *1 (E.D. Cal. Nov. 23, 2015) (dismissing case because of an out-of-court settlement).

99. Shaw, *supra* note 13.

100. City of Ontario v. Quon, 560 U.S. 746, 764 (2010).

reasonable expectation of privacy and instead assumed *arguendo* that he did.[101] The Court then held that because "the search was motivated by a legitimate work-related purpose, and because it was not excessive in scope," the search was still reasonable.[102] Although the Court assumed the employee had a privacy interest—an interest strengthened by the Fourth Amendment's protection against warrantless searches—it has already signaled that so long as the search is rationally related to work and not excessive in scope, a search will still be held to be reasonable.[103]

A close analog to BYODs and RFID microchips is the rise of employment-related wearable wellness devices such as Fitbits.[104] The past few years have seen an explosion of this technology in the workplace.[105] Employers are strongly incentivized to lower health insurance costs, and wearable technologies are the perfect tool.[106] Fitbit offers the ability for employers to see how active employees are. Fitbit's website promises that employers in the program can "monitor individual, team and company-wide progress."[107] The benefits of adopting a Fitbit Wellness program, according to the site, include the ability to "create a culture of well-being," "increase

101. *Id.* The Court declined to answer this question because, "A broad holding concerning employees' privacy expectations vis-à-vis employer-provided technological equipment might have implications for future cases that cannot be predicted." *Id.*

102. *Id.*

103. *Id*.

104. Brown, *supra* note 12.

105. Jane Wild, *Wearables in the Workplace and the Dangers of Staff Surveillance*, FIN. TIMES (Feb. 27, 2017), https://www.ft.com/content/089c0d00-d739-11e6-944b-e7eb37a6aa8e [https://perma.cc/9VGC-UC2M]; *see also* Brown, *supra* note 12, at 14–17 (discussing the rise of the wearable technology industry generally and in the workplace specifically).

106. For example, Appirio, a Bay Area startup, negotiated a $300,000 discount on its $5 million insurance costs by agreeing to share employee health data with its insurer and showing that the staff's health was improving, and BP offers their employees a cut of $1200 for using a Fitbit and logging sufficient activity. Adam Satariano, *Wear This Device So the Boss Knows You're Losing Weight*, BLOOMBERG (Aug. 21, 2014, 12:26 PM), http://www.bloomberg.com/news/articles/2014-08-21/wear-this-device-so-the-boss-knows-you-re-losing-weight [https://perma.cc/FB6L-PA2F]. Due to the proliferation of these programs, John Hancock Insurance offered customers up to a fifteen percent discount on their insurance rates in exchange for healthful activity as measured by the Fitbits the customers agreed to wear. Tara Siegel Bernard, *Giving Out Private Data for Discount in Insurance*, N.Y. TIMES (Apr. 8, 2015), http://www.nytimes.com/2015/04/08/your-money/giving-out-private-data-for-discount-in-insurance.html [https://perma.cc/5SW6-SMCP].

107. *Fitbit Group Health*, IAML SERVICES, http://iamlservices.com/partner/fitbit/ [https://perma.cc/UW3J-73ZQ] (last visited Oct. 8, 2019).

employee productivity," "improve employee health status," and "boost acquisition and retention."[108]

The collected health data, however, can also be used to track employees.[109] In deciding which of two candidates to promote, an employer could review each candidate's sleep pattern,[110] physical activity, or calorie intake, and decide based at least in part on this data.[111] IBM recently filed a patent for "a system wedding currently ubiquitous drones with cameras and biometric sensors that could dispatch caffeine to flagging employees," with nothing prohibiting the collection of the data used for employee analytics.[112] Elizabeth Brown concludes that the collection of health data can easily be used to discriminate and affect employment decisions with little legal recourse; employees likely do not have a reasonable expectation of privacy in this data, and federal statutes offer no additional protection.[113]

---

108. *Id*.

109. For example, a company was able to track the intimate details of employees' pregnancies by encouraging them to use a phone app to monitor their health and then paying the app developers to access all of the details. Drew Harwell, *Is Your Pregnancy App Sharing Your Intimate Data with Your Boss?*, WASH. POST (April 10, 2019), https://www.washingtonpost.com/technology/2019/04/10/tracking-your-pregnancy-an-app-may-be-more-public-than-you-think/?utm_term=.b4bbc077d205 [https://perma.cc/JGU6-G2CR].

110. Already a health insurance company monitors the use of equipment by sleep apnea patients. Marshall Allen, *You Snooze, You Lose: Insurers Make the Old Adage Literally True*, PROPUBLICA (Nov. 21, 2018, 5:00 AM), https://www.propublica.org/article/you-snooze-you-lose-insurers-make-the-old-adage-literally-true [https://perma.cc/X5FS-ELGZ].

111. Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 TEX. L. REV. 85, 118-19 (2014) ("Impulsivity and the inability to delay gratification—both of which might be inferred from one's exercise habits—correlate with alcohol and drug abuse, disordered eating behavior, cigarette smoking, higher credit-card debt, and lower credit scores. Lack of sleep—which a Fitbit tracks—has been linked to poor psychological well-being, health problems, poor cognitive performance, and negative emotions such as anger, depression, sadness, and fear. Such information could tip the scales for or against" a job candidate) (citations omitted); *see also* Dennis D. Hirsch, *That's Unfair! Or Is It? Big Data, Discrimination and the FTC's Unfairness Authority*, 103 KY. L.J. 345, 350–52 (2014) (describing potential discrimination resulting from use of health-related Big Data); Jessica L. Roberts, *Protecting Privacy to Prevent Discrimination*, 56 WM. & MARY L. REV. 2097, 2122 (2015) (noting potential for discrimination when access opens to private information).

112. Camilla Hodgson, *IBM Looks for Caffeine Buzz with Coffee Delivery Drones*, FIN. TIMES (Aug. 22, 2018), https://www.ft.com/content/51a801b2-a464-11e8-8ecf-a7ae1beff35b [https://perma.cc/ZFK3-WC4Z].

113. Brown, *supra* note 12, at 48.

II. ANALYSIS AND PROPOSAL

Put in this context, Three Square Market's use of implanted RFID microchips is not shocking. An implanted microchip is the natural combination of three major workforce trends: increased monitoring and surveillance; decreased expectation of privacy in devices used for work; and wearable technology that tracks health information.

Similar to the drug-testing cases, employee privacy claims against microchip implants have an uphill battle. First, there is generally little expectation of privacy in employer-owned sensor-generated data.[114] And similar to BYOD policies, the line between use for work and personal is not bright. Because a microchip implant can collect data at all hours and cannot readily be turned off or removed, where one's expectation of privacy should begin and end is difficult to ascertain for workers perpetually on call or expected to always check emails.[115]

The Court's reasonable-expectation-of-privacy analysis is outdated. It relies on a spatial distinction between work life and private life that no longer exists.[116] In *O'Connor*, the Supreme Court stated that the "essential" first step is to "delineate the boundaries of the workplace context."[117] This perpetuates the fallacy that work life can be successfully segregated from private life. The autonomy of a "private sphere" no longer exists.[118]

Nonetheless, some courts may find a reasonable expectation of privacy in microchip-generated data during off-work hours. As the Supreme Court pointed out in *Skinner*, there are things with which an employer has no legitimate interest.[119] While employees can take off a Fitbit, an implanted RFID microchip is much harder to remove. An employer having access to employee heart rates at 2:00 a.m. on a Friday night should be found to exceed the legitimate interest delineated by *Skinner*.

---

114. *See* City of Ontario v. Quon, 560 U.S. 746, 747 (2010).
115. *See* Tewes, *supra* note 90, at 298–99.
116. *See* O'Connor v. Ortega, 480 U.S. 709, 715 (1987) (presuming that it is possible to "delineate the boundaries of the workplace context" and suggesting that the boundaries be a threshold determination).
117. *Id.*
118. *See* Tewes, *supra* note 90, at 305–08.
119. Skinner v. Ry. Labor Execs. Ass'n, 489 U.S. 602, 619 (1989).

Finding a reasonable expectation of privacy, however, may still not protect employee privacy interests. Following *Skinner*, courts still upheld nearly all mandatory government drug-testing programs, and the private sector fared no better.[120] Legitimate business reasons will likely always trump any expectation of privacy. Moreover, a finding that some data collected by a microchip is granted a reasonable expectation of privacy would do little to slow down the erosion of privacy rights in other areas such as wearable technologies or BYODs.[121]

Additionally, the reasonable expectation of privacy is relative to the office place. Employer policies and practices can adjust the reasonable expectation of privacy. If the use of microchips to make employment decisions is regular and known, then an employee will likely be unable to assert a violation of their reasonable expectation of privacy.[122]

Furthermore, a reasonable expectation of privacy only helps *ex post* and is severely limited by the employment-at-will regime. An individual employee can receive damages based on a dignitary harm but has little power to bargain over or prevent the injury from occurring. This is partially due to employer privacy policies being a "local public good"—where the policies affect the entire office workplace.[123] One individual likely cannot bargain over these privacy concerns, as seen with Arias' termination.[124] Employees currently only have a few options, all unsatisfactory. If employees acquiesce, they have consented and lose a privacy claim; only where the monitoring exceeds their consent could they have any reasonable claim of a privacy violation. And because of the employment-at-will regime, employees are often left with the choice of consent or be terminated. An employee who refuses and is terminated suffered no privacy violation and any claim rests in a statutory retaliation claim—only where it exists—rather than in common law dignitary harm.

Other workplace privacy commentators have proposed some solutions. One approach to protect employees' health data is omnibus federal

120. *See supra* notes 44–49 and accompanying text.
121. *See supra* Part I.D.
122. "Employers can easily defeat the threshold element of reasonable expectation to privacy through proper planning with prior notice, written consent and practices and procedures." Tewes, *supra* note 90, at 308–09.
123. Kim, *supra* note 46, at 1027.
124. *See supra* text accompanying notes 98–99.

information privacy laws.[125] The European Union's Data Directive has long served as a model for this approach; it empowers the European Data Protection Supervisor, individual National Data Protection Authorities (NDPAs), and various citizens and civil society groups to enforce violations of personal data protection.[126] This scheme then limits the data collected to work-related activities. Having the public and government enforce privacy rights allows employees to avoid adverse employment consequences because the enforcement actions can occur before the harm is suffered.

As Professor Ajunwa points out, however, this type of scheme does not necessarily address the difficulty in mandating consent as a condition of employment:

> In the United States, such an omnibus protection would represent a pyrrhic victory. In the context of at-will employment—where there is asymmetrical bargaining power between the worker and the employer—standard notice and consent mechanisms would merely serve as a sanitizing seal of approval for employer surveillance; there would be no real chance for dispute by the employee.[127]

Additionally, limiting collection to work-related activities will not mitigate collection of data but rather lead to a broader definition of work-related activities. As the definition of work continues to expand so too will the scope of data likely to be collected. Professor Ajunwa's idea therefore still relies on terms of discernable spatial and temporal workplace boundaries.

Professor Brown persuasively argues that the FTC should require sufficient labeling on wearable technologies to inform consumers that their health data is being collected.[128] Brown notes that required and specific labeling on products will make enforcement against wearable-technology companies that collect data easier for employees.[129] This solution is

125. Ajunwa et al., *supra* note 50, at 743.

126. *See*, *e.g.*, *Protection of Personal Data*, EUR. COMM'N, https://ec.europa.eu/info/aid-development-cooperation-fundamental-rights/your-rights-eu/know-your-rights/freedoms/protection-personal-data_en [https://perma.cc/9TDM-CCGV].

127. Ajunwa et al., *supra* note 50, at 774.

128. Brown, *supra* note 12, at 43–45.

129. *Id.* at 44.

transferable to employer-implanted RFID microchips where employees may often not realize the far-reaching data-collection capabilities and the expanding reliance on data analytics in employment decisions. Sufficient notice would allow employees to make an informed decision and, if the employer breaks its own policy, would allow for easier recourse in contract law rather than tort. The largest drawback, similar to most protections, is that the protections are largely illusory in an employment-at-will system. The technical ability to reject a microchip implant can easily be overshadowed by the workplace necessity of having a chip; if firms structure their workplaces around RFID microchips, the only way to function will be with receiving one. And where employees refuse to consent, they will simply be terminated or not hired.

Professor Kim, with drug-testing cases, offers a collectivist, rather than individual, approach to address privacy concerns.[130] A collectivist approach allows employees to address privacy concerns before they suffer a dignitary harm, by bargaining over the implantation of new technology.[131] Such an approach solves the problem presented above where when employees are terminated they fail to suffer a cognizable privacy violation—consent or be terminated.

In the sense that privacy is a "local public good" a collectivist approach may be the only way to successfully negotiate over its implementation.[132] An individual employee, as shown in *Arias*, cannot meaningfully bargain over a local public good. The employer will simply terminate them. Conversely, collective action allows for the cost of bargaining to be evenly distributed across the workforce rather than suffered by the brave employee who objected. For example, unions shot down the idea of electrocuting truck drivers in Australia,[133] and a union in Britain forced the *Daily Telegraph* to remove its spying system, OccupEye.[134] Stopping short of outright bans on

130. Kim, *supra* note 46.

131. *Id.* at 1021. If there is a union with a collective bargaining agreement in place, implantation of microchips would likely be a mandatory subject of bargaining, just as mandatory drug testing was. *See* Johnson-Bateman Co., 295 N.L.R.B. 180 (1989).

132. Kim, *supra* note 46, at 1027.

133. Brook, *supra* note 86.

134. Ben Quinn & Jasper Jackson, *Daily Telegraph to Withdraw Devices Monitoring Time at Desk After Criticism*, THE GUARDIAN (Jan. 11, 2016, 4:13 PM), https://www.theguardian.com/media/2016/jan/11/daily-telegraph-to-withdraw-devices-monitoring-time-at-desk-after-criticism [https://perma.cc/3SFM-M83L].

the implantation of microchips or overturning the employment-at-will system, a collectivist approach that engages in collective bargaining over the implantation of microchips may be the only way for employees to truly assert their privacy rights.

In an employment-at-will regime, employees must assert their privacy rights collectively before the implementation of increased workplace surveillance. Such an approach is the only way to address the "damned if you do, damned if you don't" conundrum offered by employers: consent or be terminated; it is a structure where an employee cannot resist the erosion of their fundamental privacy rights until they have already been harmed.

CONCLUSION

As the workplace rapidly evolves, employers will have more access to employee data than ever before. With wearable technologies, BYODs, and now implanted microchips, employers can access nearly all gatherable information. Employers can make employment decisions based on average heart rate or hours of sleep. Employers may be hesitant to provide health insurance for employees who regularly visit the doctor or promote those who engage in off-duty alcohol consumption.

Under the current regime, there is very little an employee can do to prevent their employer from accessing such personal information. The lowered level of reasonable expectation of privacy for all work-related activities creates a giant hole in privacy torts, and even finding a reasonable expectation of privacy will only prevent the most egregious violations. Similarly, the patchwork of federal statutory protections provides little aid.[135]

In order to protect employee privacy rights, employees should seek a collectivist approach. A collectivist approach will not be limited to employee privacy protection for the mandatory implantation of microchips but will allow employees to assert their rights to privacy in other areas as well. A collectivist approach additionally allows employees to bargain over its implementation before any adverse employment consequences are suffered. Individual resistance over a local public good such as privacy will

135. *See supra* Section I.B.

often simply lead to termination, as Intermex terminated Arias.[136] Instead, a collectivist approach allows employees to negotiate over privacy rights.[137]

136. *See supra* text accompanying notes 98–99.
137. Kim, *supra* note 46.