Chicago-Kent Law Review

Volume 93
Issue 1 *FinTech's Promises and Perils*

Article 8

3-16-2018

Survey of (Mostly Outdated and Often Ineffective) Laws Affecting Work-Related Monitoring

Robert Sprague
University of Wyoming

SURVEY OF (MOSTLY OUTDATED AND OFTEN INEFFECTIVE) LAWS AFFECTING WORK-RELATED MONITORING

ROBERT SPRAGUE*

> [Smartphones] are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy.[1]

> The scope and variety of the types of surveillance that are possible today are unprecedented in human history. This fact alone should give us pause.[2]

I. INTRODUCTION

We already know, or at least suspect, that the government uses our online and mobile applications to surveil us.[3] As do businesses for their own commercial purposes.[4] To what extent do employers monitor the activities of their workers?

* J.D., M.B.A. Professor of Legal Studies in Business, University of Wyoming College of Business. The author thanks César F. Rosado Marzán and Martin H. Malin for their invitation to present the contents of this article at the 39th Annual Kenneth M. Piper Memorial Lecture in Labor Law hosted by the Institute for Law and the Workplace and the Chicago-Kent College of Law, Chicago, Illinois, April 4, 2017.

1. Riley v. California, 134 S. Ct. 2473, 2484 (2014).

2. Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1936 (2013).

3. *See, e.g.*, Lorenzo Franceschi-Bicchierai, *The 10 Biggest Revelations from Edward Snowden's Leaks*, MASHABLE (June 5, 2014), mashable.com/2014/06/05/edward-snowden-revelations [https://perma.cc/9TDN-6BPG]; Matt Cagle, *Facebook, Instagram, and Twitter Provided Data Access for a Surveillance Product Marketed to Target Activists of Color*, ACLU OF N. CAL.: BLOG (Oct. 11, 2016), https://www.aclunc.org/blog/facebook-instagram-and-twitter-provided-data-access-surveillance-product-marketed-target [http://perma.cc/XHP6-EJ7P] (noting social media monitoring product marketed to law enforcement); *FISC Orders on Illegal Government Surveillance*, ELEC. FRONTIER FOUND., https://www.eff.org/foia/fisc-orders-illegal-government-surveillance [https://perma.cc/P4MU-SN39] (last visited Dec. 13, 2016) (discussing Freedom of Information Act requests for information related to email and telephone call surveillance at the National Security Agency).

4. *See, e.g.*, Steven Englehardt & Arvind Narayanan, *Online Tracking: A 1-Million-Site Measurement and Analysis*, *in* PROCEEDINGS OF THE 2016 ACM SIGSAC CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY 1388, 1397 (2016) (revealing tracking techniques used to "fingerprint" web browsers and devices as users move from site to site, tracking them even when they explicitly demand not to be tracked and take countermeasures to prevent the tracking); Alexander Tsesis, *The Right to Erasure: Privacy, Data Brokers, and the Indefinite Retention of Data*, 49 WAKE FOREST L. REV. 433, 433 (2014) ("Under current U.S. law, online businesses can track private users without their

This article provides an overview of laws associated with work-related monitoring, particularly related to electronic communications and other forms of data monitoring. Part II focuses on workplace privacy and employer monitoring, first briefly exploring why employers monitor employee communications. Part II then reviews common law privacy protections as applied to work-related electronic communications, followed by a review of potential federal and state statutory protections that, on the surface, may provide similar protections. In Part III, this article considers evolving communications and monitoring platforms, namely smartphone GPS applications and privacy implications of wellness programs. This article concludes with an analysis of the state of worker privacy in the modern American workplace, noting that what legal protections are available are mostly outdated and extremely limited in scope.

The erosion of the demarcation between work and personal life was noted by Justice Blackmun thirty years ago—"It is . . . all too true that the workplace has become another home for most working Americans. . . . [T]he 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."[5]—and has more recently been the subject of scholarly comment.[6] Add to this the ubiquity of the smartphone[7] and the emergence

being aware of the extent to which websites monitor conduct, aggregate it with other personal details, create marketing profiles, and sell the cumulative character sketches to third parties."); Jeff Desjardins, *Is Your Favorite Website Spying on You?*, VISUAL CAPITALIST (Mar. 28, 2017, 12:34 PM), http://www.visualcapitalist.com/favorite-website-spying/ [http://perma.cc/KJZ4-EJRU]; *see also* Richards, *supra* note 2, at 1937 ("Surveillance, it seems, is not just good politics, but also good business.").

5. O'Connor v. Ortega, 480 U.S. 709, 739 (1987) (Blackmun, J., dissenting) (citations omitted).

6. *See, e.g.*, Patricia Sánchez Abril et al., *Blurred Boundaries: Social Media Privacy and the Twenty-First-Century Employee*, 49 AM. BUS. L.J. 63, 64 (2012) (arguing that "boundary-crossing" communications systems and devices provided by employers "blur the already elusive line between the private and the public, the home and the workplace" for employees); Ariana R. Levinson, *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." (footnote omitted)); Robert Sprague, *Invasion of the Social Networks: Blurring the Line Between Personal Life and the Employment Relationship*, 50 U. LOUISVILLE L. REV. 1, 1 (2011) (arguing the dual-use nature of communications services and devices for both work and personal uses causes the distinction between work and personal use to become lost or, at a minimum, blurred).

7. Riley v. California, 134 S. Ct. 2473, 2490 (2014) ("Today . . . it is no exaggeration to say that many of the more than 90% of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives—from the mundane to the intimate."); *see also* City of Ontario v. Quon, 560 U.S. 746, 760 (2010) ("Cell phone and text message communications are so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification.").

of wearable technologies in the workplace,[8] and we have the scenario for real-time, continuous collection of personal data by employers.

Consider, for example, Myrna Arias's experience with her employer, Intermex Wire Transfer. Shortly after Arias was hired, Intermex instructed its employees to download the Xora app to their smartphones.[9] After determining that the Xora app contains a GPS function, Arias and other employees asked whether Internex would be monitoring their movements while off duty,[10] particularly since Arias and other employees were required to keep their phones' power on "'24/7' to answer phone calls from clients."[11] Not only did Arias's supervisor state that employees would be monitored while off duty, the supervisor "bragged that he knew how fast [Arias] was driving at specific moments ever since she had installed the app on her phone."[12] Arias sued Intermex for, *inter alia*, invasion of privacy after she was "scolded" by her supervisor for de-installing the Xora app from her smartphone and being fired a few weeks later.[13]

II. WORKPLACE PRIVACY AND EMPLOYER MONITORING

Employers monitor employees' behavior and communications for a number of legitimate business reasons, including productivity, safety and threat prevention, and liability prevention and compliance.[14] After all, a GPS

8. *See, e.g.*, 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 (2016) ("Employers make key decisions based on employees' biometric data, collected from specialized devices like a Fitbit or the health-related apps installed on mobile phones."); *see also* 29 C.F.R. § 1630.14(d)(3) (2017) (allowing employers to use incentives to encourage employees to participate in wellness programs). The EEOC describes wellness programs as including health risk assessments as well as encouraging employees to engage in physical activities such as walking or exercising. *See* 29 C.F.R. pt. 1630 Appendix. *See generally infra* Part III. B.

9. Complaint at 3, Arias v. Intermex Wire Transfer, LLC, No. 1:15-CV-01101 (E.D. Cal. Nov. 23, 2015), 2015 WL 2254833. Xora appears to be part of the StreetSmart workforce management software distributed by ClickSoftware, which, in part, promises to "provide the location of every mobile employee on a Google Map with detailed information such as arrival times, break status, the route driven and more." *See StreetSmart*, CLICKSOFTWARE, https://www.clicksoftware.com/products/streetsmart/ [https://perma.cc/Y369-29R7] (last visited Jan. 16, 2017).

10. Complaint, *supra* note 9.

11. *Id.* at 3–4.

12. *Id.* at 4.

13. *Id.* Arias and Intermex subsequently settled the lawsuit. *See* Elizabeth Austermuehle, *Monitoring Your Employees Through GPS: What Is Legal, and What Are Best Practices?*, GREENSFELDER (Feb. 18, 2016, 2:13 PM), http://www.greensfelder.com/business-risk-management-blog/monitoring-your-employees-through-gps-what-is-legal-and-what-are-best-practices [https://perma.cc/5JKY-6HQW].

14. *See* Corey A. Ciocchetti, *The Eavesdropping Employer: A Twenty-First Century Framework for Employee Monitoring*, 48 AM. BUS. L.J. 285 (2011) (proposing an employee-monitoring framework that balances employer and employee interests with respect to business, liability-avoidance, and

application installed on an employee's smartphone can reveal that the employee is in Las Vegas the day he called in sick (and the employer does not have an office there).[15] More often than not, monitoring employee web activity by the employer will probably reveal that many employees do waste work time visiting web sites unrelated to work.[16]

In certain circumstances, employers may even be legally compelled to monitor workers. Hostile work environment jurisprudence is one such area.[17] *Burlington Industries, Inc. v. Ellerth*,[18] and its companion case *Faragher v. City of Boca Raton*,[19] offer 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.[20] This places greater pressure on employers to monitor employee behavior.[21] And this duty to monitor may extend beyond a hostile work environment. In *Anicich v. Home Depot U.S.A., Inc.*,[22] the Seventh Circuit Court of Appeals applied *Ellerth* in holding that the employer, Home Depot U.S.A., could potentially be civilly liable for a supervisor murdering his subordinate because Home Depot granted the killer the supervisory power, which he then abused.[23]

investigatory purposes); *see also* Jessica K. Fink, *In Defense of Snooping Employers*, 16 U. PA. J. BUS. L. 551 (2014); Lee Michael Katz, *Monitoring Employee Productivity: Proceed with Caution*, SOC'Y HUM. RESOURCE MGMT. (June 1, 2015), https://www.shrm.org/hr-today/news/hr-magazine/pages/0615-employee-monitoring.aspx [https://perma.cc/6J3Z-5SJK].

15. *See* Will Yakowicz, *When Monitoring Your Employees Goes Horribly Wrong*, INC. (July 6, 2015), https://www.inc.com/will-yakowicz/drones-catch-employees-having-sex-and-other-employee-monitoring-gone-wrong.html [http://perma.cc/4JRZ-DZ3Z].

16. *See* Ciocchetti, *supra* note 14, at 336.

17. *See* Fink, *supra* note 14, at 587–89.

18. 524 U.S. 742 (1998).

19. 524 U.S. 775 (1998).

20. Specifically, when no tangible employment action is taken, a defending employer may raise an affirmative defense to liability or damages comprised of two necessary elements: "(a) that the employer exercised reasonable care to prevent and correct promptly any sexually harassing behavior, and (b) that the plaintiff employee unreasonably failed to take advantage of any preventive or corrective opportunities provided by the employer or to avoid harm otherwise." *Burlington*, 524 U.S. at 765; *Faragher*, 524 U.S. at 807.

21. *See, e.g.*, *Burlington*, 524 U.S. at 770 (Thomas, J., dissenting) ("Sexual harassment is simply not something that employers can wholly prevent without taking extraordinary measures—constant video and audio surveillance, for example—that would revolutionize the workplace in a manner incompatible with a free society." (citation omitted)); Ellerth v. Burlington Indus., Inc., 123 F.3d 490, 513 (7th Cir. 1997) (Posner, J., dissenting), *aff'd*, 524 U.S. 742 ("It is facile to suggest that employers are quite capable of monitoring a supervisor's actions affecting the work environment. Large companies have thousands of supervisory employees. Are they all to be put under video surveillance?").

22. 852 F.3d 643 (7th Cir. 2017).

23. *Id.* at 650–51. The supervisor threatened to fire or reduce the subordinate's hours if she did not accompany him on a personal trip; the supervisor murdered the subordinate on that trip. *Id*. at 648. The supervisor had a history of sexually harassing and verbally abusing his young female subordinates, including his victim. And although he was ordered twice to attend anger management classes, he never completed them and the employer never followed up to make sure he did. *Id*. at 647; *see also* Doe v. XYC

But these duties to monitor do not necessarily give employers unfettered rights to monitor employees, and particularly employees' computer activities and electronic communications.

A. Common Law Right to Privacy in the Workplace

In the private realm, a person's privacy is not invaded unless there has been a highly offensive intrusion upon that person's solitude or private affairs.[24] In general, courts do not consider the workplace a secluded and private area sufficient to provide a "zone of privacy."[25] Even within a privately-owned workplace, courts consider it more akin to a public place[26] than, say, one's home, where privacy is most sacrosanct.[27] While courts have indeed recognized that employees can have some degree of privacy in the

Corp., 887 A.2d 1156, 1158 (N.J. Super. Ct. App. Div. 2005) ("[A]n employer who is on notice that one of its employees is using a workplace computer to access pornography, possibly child pornography, has a duty to investigate the employee's activities and to take prompt and effective action to stop the unauthorized activity, lest it result in harm to innocent third-parties. No privacy interest of the employee stands in the way of this duty on the part of the employer."); *cf.* Muick v. Glenayre Elec., 280 F.3d 741, 743 (7th Cir. 2002) ("[T]he abuse of access to workplace computers is so common (workers being prone to use them as media of gossip, titillation, and other entertainment and distraction) that reserving a right of inspection is so far from being unreasonable that the failure to do so might well be thought irresponsible.").

24. *See* RESTATEMENT (SECOND) OF TORTS § 652B (AM. LAW INST. 1977); *see also* RESTATEMENT (THIRD) OF EMPLOYMENT LAW § 7.06 (AM. LAW INST. 2014) (applying this standard in the employment context); *infra* notes 49–60 and accompanying text. In contrast, the government must obtain a warrant if a search would infringe upon a person's reasonable expectation of privacy. *See* Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring).

25. *See, e.g.*, Benn v. Fla. E. Coast Ry. Co., No. 97-4403-CIV, 1999 WL 816811, at *8 (S.D. Fla. July 21, 1999) (noting unique exceptions such as when an employee looks up a coworker's skirt or when an employee enters the ladies' restroom and commits a battery upon a coworker). For public employers, courts apply the Fourth Amendment-based reasonable expectation of privacy in a workplace setting. *See, e.g.*, O'Connor v. Ortega, 480 U.S. 709, 714 (1987); Nelson v. Salem State Coll., 845 N.E.2d 338, 346 (Mass. 2006). However, Fourth Amendment protections do not directly apply to private-employer monitoring. *See* Skinner v. Ry. Labor Execs.' Ass'n, 489 U.S. 602, 614 (1989) ("[T]he Fourth Amendment does not apply to a search or seizure. . . effected by a private party on his own initiative."); Burdeau v. McDowell, 256 U.S. 465, 475 (1921) (finding that the Fourth Amendment "was not intended to be a limitation upon other than governmental agencies"); Sam Kamin, *The Private Is Public: The Relevance of Private Actors in Defining the Fourth Amendment*, 46 B.C. L. REV. 83, 85 (2004).

26. *See, e.g.*, Kemp v. Block, 607 F. Supp. 1262, 1264 (D. Nev. 1985) (finding employee had no reasonable expectation of privacy in small, open shop room, particularly when employee had a loud voice).

27. Polay v. McMahon, 10 N.E.3d 1122, 1127 (Mass. 2014) ("Nowhere are expectations of privacy greater than in the home . . . ." (internal quotation marks omitted)). The sanctity of the home vis-à-vis privacy has been a long-recognized doctrine in Fourth Amendment jurisprudence. *See, e.g.*, Florida v. Jardines, 133 S. Ct. 1409, 1414 (2013); Kyllo v. United States, 533 U.S. 27, 31 (2001); Boyd v. United States, 116 U.S. 616, 630 (1886) (recognizing "the sanctity of a man's home and the privacies of life" as protected from unwarranted government search and seizure).

workplace,[28] it is also true that notice by the employer of monitoring can often defeat any expectation of privacy by employees.[29]

For example, in *Stengart v. Loving Care Agency, Inc.*,[30] the New Jersey Supreme Court concluded that an employee had a reasonable expectation of privacy in email communications sent to her attorney through a private, password-protected, web-based email account, although the employee accessed the account using her employer-provided laptop.[31] The court concluded the employee had "plainly [taken] steps to protect the privacy of those e-mails and shield them from her employer."[32] Importantly, the court also concluded that the employer's electronic communications policy did not address the use of personal, web-based email accounts accessed through company equipment.[33] *Stengart* involved an employee's communications with her attorney and whether the attorney-client privilege should be maintained.[34] Compare *Stengart* with *Holmes v. Petrovich Development Co.*, which also involved an employee sending her attorney email messages using the employer's computer system.[35] In *Holmes*, however, the employer's policy clearly stated that employees using company computers to create or

28. *See Muick*, 280 F.3d at 743 (listing cases in which courts have held employees had a right to privacy in papers stored in their offices).

29. *See id.* (listing cases in which courts have held that providing notice of monitoring defeated expectations of privacy); *see also* Shefts v. Petrakis, 758 F. Supp. 2d 620, 633 (C.D. Ill. 2010) ("[A] party's expectation of privacy in messages sent and received on company equipment or over a company network hinge on a variety of factors, including whether or not the company has an applicable policy on point."; applying Illinois Eavesdropping Statute, 720 ILL. COMP. STAT. 5/14-1(e) (2014)); Lothar Determann & Robert Sprague, *Intrusive Monitoring: Employee Privacy Expectations Are Reasonable in Europe, Destroyed in the United States*, 26 BERKELEY TECH. L.J. 979 (2011) (arguing that while U.S. employers can destroy actual expectations of privacy through the use of notices and consent forms, the level of detail and specificity of such notices must increase when the intrusiveness of the surveillance increases).

30. 990 A.2d 650 (N.J. 2010).

31. *Id.* at 663.

32. *Id.*

33. *Id.* ("[The policy] does not address personal accounts at all. Nor does it warn employees that the contents of e-mails sent via personal accounts can be forensically retrieved and read by the company. Indeed, in acknowledging that occasional personal use of e-mail is permitted, the Policy created doubt about whether those e-mails are company or private property."). The court also distinguished the content of the emails from the content at issue in *Muick*, 280 F.3d at 742–43, and Doe v. XYC Corp., 887 A.2d 1156, 1158 (N.J. Super. Ct. App. Div. 2005): "the e-mails are not illegal or inappropriate material stored on [the employer's] equipment, which might harm the company in some way." *Stengart*, 990 A.2d at 663–64. In *Muick*, the employer had seized the employee's employer-provided laptop in cooperation with a criminal investigation of child pornography. 280 F.3d at 742. "An employer has a legitimate business interest in prohibiting certain computer uses that are likely to negatively impact the business or workplace." Ariana R. Levinson, *Industrial Justice: Privacy Protection for the Employed*, 18 CORNELL J. L. & PUB. POL'Y 609, 662 (2009) (reviewing labor arbitration decisions governing the right to privacy from employer monitoring).

34. 990 A.2d at 655.

35. 191 Cal. App. 4th 1047, 1051 (2011). The court never explicitly states, but does imply, that the employee was using the employer's email system to communicate with her lawyer.

maintain personal information or messages "have no right of privacy with respect to that information or message."[36] The California Court of Appeals concluded that by using the company's computer to communicate with her lawyer, knowing the communications violated company computer policy and could be discovered by her employer due to company monitoring of email usage, the employee's communications were not privileged.[37]

Courts do appear to respect individual expectations of privacy in personal, password-protected accounts,[38] even when accessed from an employer-provided computer[39] and the employee in question has configured the account to pre-populate the account's user name and password.[40] Restricting access alone is no absolute bar from an employer still viewing personal information with impunity. Although the "third-party doctrine" originates from Fourth Amendment jurisprudence,[41] it applies equally in the

36. *Id.* (internal quotation marks omitted).

37. *Id.* at 1051–52 (analogizing the employee's e-mails "to consulting her lawyer in her employer's conference room, in a loud voice, with the door open, so that any reasonable person would expect that their discussion of her complaints about her employer would be overheard by him").

38. *See, e.g.*, Pietrylo v. Hillstone Rest. Grp., No. 06-5754 (FSH), 2008 WL 6085437, at *7 (D.N.J. July 25, 2008) (concluding employer violated employees' expectation of privacy if it coerced an employee to reveal the password required to access the web site used by employees to discuss working conditions). *But see* Pietrylo v. Hillstone Rest. Grp., No. 06-5754 (FSH), 2009 WL 3128420 (D.N.J. Sept. 25, 2009) (reporting that jury concluded employer did not violate plaintiffs' common law right to privacy).

39. *See, e.g.*, Borchers v. Franciscan Tertiary Province of the Sacred Heart, Inc., 962 N.E.2d 29, 42 (Ill. App. Ct. 2011) (concluding the employer accessing multiple email messages on plaintiff's AOL account, which employee had temporarily accessed through employer's computer system, could be actionable under the Stored Communications Act; see *infra* notes 74–80 and accompanying text).

40. *See, e.g.*, Pure Power Boot Camp v. Warrior Fitness Boot Camp, 587 F. Supp. 2d 548, 552 (S.D.N.Y. 2008) (holding former employee "had a subjective belief that his personal e-mail accounts, stored on third-party computer systems, protected (albeit ineffectively) by passwords, would be private"). The court analogized the situation to one where if the former employee "had left a key to his house on the front desk at [the employer], one could not reasonably argue that he was giving consent to whoever found the key, to use it to enter his house and rummage through his belongings." *Id.* at 561. In addition, the court noted that there was nothing in the employer's email policy to alert employees to the possibility that their private email accounts could also be accessed and viewed by their employer. *Id.*

41. The third party doctrine is a Fourth Amendment doctrine originating with respect to law enforcement's ability to obtain records held by third parties. *See* United States v. Miller, 425 U.S. 435, 443 (1976) ("[T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."), *superseded by statute*, Right to Financial Privacy Act of 1978, Pub. L. No. 95-630, tit. XI, 92 Stat. 3641, 3697 (1978) (codified as amended at 12 U.S.C. §§ 3401–3422 (2012)), *as recognized in* SEC v. Jerry T. O'Brien, Inc., 467 U.S. 735, 745 (1984); Smith v. Maryland, 442 U.S. 735, 743–44 (1979) ("[A] person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."), *superseded by statute*, Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, tit. III, 100 Stat. 1848, 1868–69 (1986) (codified as amended at 18 U.S.C. § 3121 (2012)) (requiring government authorities to obtain a court order or permission of the user prior to recording telephone numbers dialed), *as recognized in* Saldana v. Wyoming, 846 P.2d 604, 628 n.1 (Wyo. 1993). *But see* Klayman v. Obama, 957 F. Supp. 2d 1, 37 (D.D.C. 2013), *vacated and remanded*, 800 F.3d 559 (D.D.C. 2015) (questioning "whether people can have a reasonable expectation of privacy in telephony metadata

common law privacy context. Fundamentally, one generally cannot claim an invasion of privacy against someone who has obtained highly personal or private information from a third party. Deborah Ehling's experience exemplifies application of this doctrine in a private-employment setting. Ehling, a nurse and paramedic, was fired by her employer, Monmouth-Ocean Hospital Service Corporation (MONOC), after its management became aware of certain information Ehling had posted on her personal Facebook page.[42] Although Ehling had restricted access to her account, excluding MONOC management,[43] her invasion of privacy claim was dismissed because management had "passively" received Ehling's Facebook posts from one of Ehling's Facebook friends.[44]

And careless employees should not expect much privacy protection. For example, Santiago Victor linked his personal Apple account to his employer/Sunbelt-provided iPhone.[45] When Victor left Sunbelt he returned the iPhone, and then linked the iPhone provided by his new employer with his personal Apple account.[46] However, Victor did not "unlink" the Sunbelt-provided iPhone from his account; as a result, for several weeks, electronic data and messages, including text messages, sent to Victor's new employer-provided iPhone were also sent to his Sunbelt-provided iPhone.[47] The court concluded:

> Victor personally caused the transmission of his text messages to the Sunbelt iPhone by syncing his new devices to his Apple account without first unlinking his Sunbelt iPhone. As such, even if he subjectively harbored an expectation of privacy in his text messages, such expectation cannot be characterized as objectively reasonable, since it was Victor's

under all circumstances[;]" "I cannot possibly navigate these uncharted Fourth Amendment waters using as my North Star a case [*Smith*] that predates the rise of cell phones."); Rebecca Lipman, Note, *The Third Party Exception: Reshaping an Imperfect Doctrine for the Digital Age*, 8 HARV. L. & POL'Y REV. 471, 479–80 (2014) (noting that *Miller* and *Smith* took note to minimize the significance of the information attained by law enforcement, in contrast to the extent to which non-content data can be analyzed today).

42. Ehling v. Monmouth-Ocean Hosp. Serv. Corp., 961 F. Supp. 2d 659, 661–63 (D.N.J. 2013).

43. *Id.* at 663.

44. *Id.* at 674 ("The evidence does not show that Defendants [MONOC management] obtained access to Plaintiff's Facebook page by, say, logging into her account, logging into another employee's account, or asking another employee to log into Facebook. Instead, the evidence shows that Defendants were the passive recipients of information that they did not seek out or ask for. Plaintiff voluntarily gave information to her Facebook friend, and her Facebook friend voluntarily gave that information to someone else. This may have been a violation of trust, but it was not a violation of privacy." (citations omitted)). Contrast with Pietrylo v. Hillstone Rest. Grp., No. 06-5754 (FSH), 2008 WL 6085437 (D.N.J. July 25, 2008) (allowing an invasion of privacy claim to go to the jury where one employee with access to a limited-access MySpace group was allegedly coerced into providing managers access to the site; though the jury ultimately denied the invasion of privacy claim, No. 06-5754 (FSH), 2009 WL 3128420 (D.N.J. Sept. 25, 2009)).

45. Sunbelt Rentals, Inc. v. Victor, 43 F. Supp. 3d 1026, 1028 (N.D. Cal. 2014).

46. *Id.* at 1028–29.

47. *Id.*

> conduct that directly caused the transmission of his text messages to Sunbelt in the first instance.[48]

Chapter 7 of the *Restatement (Third) of Employment Law*[49] addresses employee privacy and personal autonomy. As reported by the *Restatement*, employees have a right not to be subjected to wrongful employer intrusions upon their protected privacy interests.[50] Fundamentally, Chapter 7 applies the intrusion-upon-seclusion tort developed in the *Restatement (Second) of Torts* § 652B, to the employment relationship.[51] Chapter 7 attempts to strike a balance between the employer's responsibility for conduct within the workplace and employees' privacy rights.[52]

With respect to monitoring electronic communications and data, section 7.03 reports that "[a]n employee has a protected privacy interest against employer intrusion into physical and electronic locations, including employer-provided locations, *as to which the employee has a reasonable expectation of privacy*."[53] The focus of section 7.03 is on the employee's interest in keeping his or her physical person, certain physical functions, personal possessions, and activities in certain physical and electronic locations private from employer intrusion.[54] The privacy interests in locations reported in section 7.03(a)(2) include non-workplace physical or electronic locations in which the employee has a reasonable expectation of privacy, such as the employee's home, property, and personal possessions.[55]

The approach expressed by section 7.03 is that when it comes to personal property or locations that the employee owns or has access to outside of the workplace, employees will generally enjoy the same expectations of privacy against employer intrusions as they do with respect to other third-party intrusions.[56] Importantly, even though the employee might not expect an employer to intrude into non-workplace locations, the employee cannot expect a greater level of freedom from intrusion by the employer than by the general public.[57] By the same token, the employer is not privileged to intrude upon an employee's privacy outside the workplace

48. *Id.* at 1035 (footnote omitted).

49. RESTATEMENT (THIRD) OF EMPLOYMENT LAW ch. 7 (AM. LAW INST. 2014).

50. *Id.* § 7.01.

51. *Id.* § 7.01 cmt. b.

52. *Id.*

53. *Id.* § 7.03(a)(2) (emphasis added).

54. *Id.* § 7.03 cmt. a.

55. *Id.* § 7.03 cmt. d.

56. *Id.* § 7.03 cmt. g.

57. *Id.* Courts have generally found no invasion of privacy when employers have observed employees in public places where the employees' expectations of privacy are diminished. *See, e.g.*, York v. Gen. Elec. Co., 759 N.E.2d 865, 868 (Ohio Ct. App. 2001); I.C.U. Investigations, Inc. v. Jones, 780 So. 2d 685 (Ala. 2000).

simply because the employer is otherwise pursuing a legitimate business interest.[58]

In congruence with *Restatement (Second) of Torts* § 652B, Chapter 7 of the *Restatement (Third) of Employment Law* recognizes that, in order to be actionable, an intrusion upon seclusion must be highly offensive to a reasonable person under the circumstances.[59] In the employment context, the *Restatement* reports that an intrusion is highly offensive if the nature, manner, and scope of the intrusion are clearly unreasonable when judged against the employer's legitimate business interests or the public's interests in intruding.[60] Owing, then, to the "public" nature of the workplace, finding an intrusion to be highly offensive creates a high bar for workplace privacy.

B. Federal Statutes that May Protect Employee Work-Related Communications

Although, on their face, a variety of federal laws appear promising in providing workplace privacy protections, in reality they provide very little protection. And when they do provide protections, it is usually in very constrained circumstances, such as when a worker's private, third-party online account is involved. The statutes do not provide any overarching workplace privacy protection.[61] Federal labor law, on the other hand, provides some of the strongest restrictions on employer monitoring, but, as explained in this part, the foundation for those restrictions may be subject to a changing composition of the National Labor Relations Board. And when it comes to workers recording workplace conversations, labor law is in complete opposition to common law. Finally, the one area providing anything close to an overarching right of privacy in employee electronic communications and data appears to come from the Federal Rules of Civil Procedure.

58. RESTATEMENT (THIRD) OF EMPLOYMENT LAW § 7.03 cmt. g.; *see, e.g.*, Burns v. Masterbrand Cabinets, Inc., 874 N.E.2d 72 (Ill. App. Ct. 2007) (remanding intrusion claim for trial based on surveillance of employee's home for workers' compensation case, including entry into the home on false pretenses); Wal-Mart Stores, Inc. v. Lee, 74 S.W.3d 634 (Ark. 2002) (ruling that search of employee's home for stolen merchandise was intrusion); Ass'n Servs., Inc. v. Smith, 549 S.E.2d 454, 461 (Ga. Ct. App. 2001). *But see* Saldana v. Kelsey-Hayes Co., 443 N.W.2d 382, 384 (Mich. Ct. App. 1989) (holding employee had no privacy right against employer, despite investigator posing as a process server in order to gain entrance to and taking photographs inside of the employee's home, because he had filed a workers' compensation claim).

59. RESTATEMENT (THIRD) OF EMPLOYMENT LAW § 7.06(a).

60. *Id.* § 7.06(b).

61. *Cf.* Richards, *supra* note 2, at 1942 ("[T]he general principle under which American law operates is that surveillance is legal unless forbidden.").

1. The Electronic Communications Privacy Act

By its name, the Electronic Communications Privacy Act of 1986 (ECPA) may appear to be an avenue of privacy protection for employee electronic communications. Fundamentally, Title I of the ECPA[62] (also commonly referred to as the Wiretap Act) prohibits the interception of any "wire, oral, or electronic communication."[63] And, "any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of [the ECPA]" may bring a civil action for relief.[64] But as one court noted over one dozen years ago, "the ECPA was written prior to the advent of the Internet and the World Wide Web. As a result, the existing statutory framework is ill-suited to address modern forms of communication like . . . secure website[s]."[65]

Courts have recognized limited circumstances in which an employer may violate the ECPA in accessing employee communications. For example, in *Brahmana v. Lembo*,[66] the District Court for the Northern District of California refused to dismiss an employee's ECPA claim that his employer had used key loggers to ascertain the password to his private email account and access that account.[67] The fundamental requirement for an ECPA violation is an intentional interception of electronic communications during transmission from inception to end-point.[68] In addition, exceptions within the Wiretap Act also render much of the Act inapplicable to ordinary uses of computer and communications systems within the workplace. Service providers are exempt from liability for intercepting, disclosing, or using communications transmitted over the service in the ordinary course of

62. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, tit. I, 100 Stat. 1848, 1848–59 (codified as amended at 18 U.S.C. §§ 2510–2522 (2012)).

63. 18 U.S.C. § 2511.

64. *Id.* § 2520(a)–(b).

65. Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 874 (9th Cir. 2002).

66. No. C-09-00106 RMW, 2009 WL 1424438 (N.D. Cal. May 20, 2009).

67. *Id.* at *3.

68. *See* Sunbelt Rentals, Inc. v. Victor, 43 F. Supp. 3d 1026, 1030 (N.D. Cal. 2014) ("Here, Victor has failed to allege facts sufficient to establish that Sunbelt 'intentionally intercepted' any of his text messages."; *supra* notes 45–48 and accompanying text); Shubert v. Metrophone, Inc., 898 F.2d 401, 405 (3d Cir. 1990) (noting that Congress specifically intended that "inadvertent interceptions are not crimes under the [ECPA]"); Byrd v. Aaron's, Inc., No. 11-101Erie, 2012 WL 12887775, at *7 (W.D. Pa. Feb. 17, 2012) ("[A] qualifying 'intercept' under the ECPA can only occur where a communication is accessed at some point between the time the communication is sent and the time it is received by the destination server, at which point it becomes a 'stored communication' within the meaning of the Stored Communications Act."); Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 113 (3d Cir. 2003) (holding employer did not "intercept" employee's email within the meaning of Title I of the ECPA because an "intercept" can only occur contemporaneously with transmission and it did not access employee's email at the initial time of transmission).

business.[69] The Wiretap Act also exempts from liability anyone who intercepts a communication who is a party to the communication, or where one of the parties has consented to interception.[70] As a result, employers who own and provide their own email and communications systems are exempt from Title I of the ECPA.[71] And employers who outsource their email and communications systems to service providers can also rely on Title I exceptions when they work with their service provider to intercept employee communications.[72] One scholar has concluded the Wiretap Act is already tilted toward employers' interests; it provides no protection for employees from several types of monitoring, including GPS and silent video; and provides no baseline of privacy, such as prohibiting monitoring of communications made between employees and family members in their homes regardless of whether an employee consents.[73]

Title II of the ECPA, the Stored Communications Act[74] (SCA), makes it unlawful to access stored communications. The SCA was enacted to address "the growing problem of unauthorized persons deliberately gaining access to, and sometimes tampering with, electronic or wire communications that are not intended to be available to the public."[75] The SCA is violated when a person "(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system . . . ."[76] The ECPA defines "electronic storage" as "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an

69. 18 U.S.C. § 2511(2)(a)(i).

70. *Id.* § 2511(2)(d); *see also* Sporer v. UAL Corp., No. C 08-02835 JSW, 2009 WL 2761329, at *5–6 (N.D. Cal. Aug. 27, 2009) (holding the employer's monitoring of employees' email messages did not violate § 2511 because employees impliedly consented to monitoring by consenting to the employer's monitoring policy).

71. *See* Lisa Smith-Butler, *Workplace Privacy: We'll Be Watching You*, 35 OHIO N.U. L. REV. 53, 67 (2009).

72. *See* Leonard Court & Courtney Warmington, *The Workplace Privacy Myth: Why Electronic Monitoring Is Here to Stay*, 29 OKLA. CITY U. L. REV. 15, 28–30 (2004).

73. Levinson, *supra* note 6, at 475. Despite these shortcomings, Professor Levinson argues "the ECPA can and should be interpreted to provide employees some significant level of protection for their electronic communications." *See generally id.*

74. Pub. L. No. 99-508, tit. II, 100 Stat. 1848, 1860–68 (codified at 18 U.S.C. §§ 2701–2711 (2012)).

75. S. REP. NO. 99-541, at 35 (1986).

76. 18 U.S.C. § 2701(1).

electronic communication service for purposes of backup protection of such communication[.]"[77]

This definition of electronic storage has caused some confusion with respect to messages stored on a third-party web-based email system. It is accepted that unread email messages can be considered temporarily stored incidental to transmission. But are read messages being stored for backup purposes?[78] The complexities, confusion, and conflicting opinions with respect to applying the SCA to electronic communications are beyond the scope of this article. Suffice it to say the "SCA is not a catch-all statute designed to protect the privacy of stored Internet communications[.]"[79] At least one court has held that employers are exempt from liability under the SCA for accessing employee email messages stored on their computer systems.[80] The District Court for the District of Maryland has ruled, however, that an employer may be liable under the SCA for accessing a former employee's personal Gmail messages stored on Google's servers that were once stored on the former employee's employer-provided cell phone.[81]

2. The Computer Fraud and Abuse Act

The Computer Fraud and Abuse Act[82] (CFAA) provides civil and criminal penalties for anyone who "intentionally accesses a computer

77. *Id.* § 2510(17).

78. *See, e.g.*, Theofel v. Farey-Jones, 359 F.3d 1066, 1070 (9th Cir. 2004) ("A remote computing service might be the only place a user stores his messages; in that case, the messages are not stored for backup purposes."); United States v. Weaver, 636 F. Supp. 2d 769, 772 (C.D. Ill. 2009); *see also* Garcia v. City of Laredo, Tex., 702 F.3d 788, 793 (5th Cir. 2012) (concluding text messages and photos stored on a cell phone are not in "electronic storage" as defined by the SCA). *But see* Pietrylo v. Hillstone Rest. Grp., No. 06-5754 (FSH), 2009 WL 3128420, at *3 (D.N.J. Sept. 25, 2009) (refusing to overturn jury verdict that defendant had violated SCA by coercing employee to provide password to restricted-access web site); Borchers v. Franciscan Tertiary Province of the Sacred Heart, Inc., 962 N.E.2d 29, 32 (Ill. App. Ct. 2011) (concluding the employer accessing multiple email messages on plaintiff's AOL account, which employee had temporarily accessed through employer's computer system, could be actionable under the SCA).

79. Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1214 (2004). *See also generally* Melissa Medina, Note, *The Stored Communications Act: An Old Statute for Modern Times*, 63 AM. U. L. REV. 267 (2013) (critiquing the SCA).

80. *See, e.g.*, Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 114–15 (3d Cir. 2003).

81. Levin v. ImpactOffice LLC, No. TDC-16-2790, 2017 WL 2937938, at * 5 (D. Md. July 10, 2017) ("Where [Plaintiff's] assertions . . . suggest that [she] stored copies of the emails from her personal Gmail account on her cell phone while also maintaining copies on Google's servers, she has adequately alleged that the emails were in 'electronic storage' because they were stored for backup purposes, regardless of whether they were unopened. . . . [Plaintiff] will be required to prove that the allegedly accessed emails were either unopened and in temporary storage under [18 U.S.C.] § 2510(17)(A) or were stored for the purposes of backup protection under [18 U.S.C.] § 2510(17)(B).").

82. Pub. L. No. 98-473, tit. II, § 2102(a), 98 Stat. 2190 (1984) (codified as amended at 18 U.S.C. § 1030 (2012)).

without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer[.]"[83] The issue raised is whether an employer who allegedly gains unauthorized access to employees' email messages may also be in violation of the CFAA. *Theofel v. Farey-Jones*[84] involved a commercial dispute between Farey-Jones and International Capital Associates, Inc. (ICA) in which Farey-Jones issued an overly-broad subpoena for ICA email messages stored with a third-party provider.[85] Theofel, an ICA employee whose email messages were read by Farey-Jones pursuant to the subpoena, sued Farey-Jones for, *inter alia*, violation of the CFAA. The Ninth Circuit Court of Appeals reversed the district court holding that the CFAA did not apply to unauthorized access of a third party's computer.[86] According to the Ninth Circuit, "Individuals other than the computer's owner may be proximately harmed by unauthorized access, particularly if they have rights to data stored on it."[87] Based on *Theofel*, an employer that improperly accesses an employee's private third-party web-based email system would also violate the CFAA[88] (provided the employee could show that the value of the information obtained was at least $5,000).[89]

3. Section 7 of the National Labor Relations Act

Employers who fire or otherwise discipline employees based on work-related electronic communications may run afoul of the National Labor Relations Act[90] (NLRA). Section 7 of the NLRA expresses the right of employees to "engage in concerted activities, for the purpose of . . . mutual aid or protection."[91] Section 8(a)(1) of the NLRA makes it an unfair labor practice for an employer "to interfere with, restrain, or coerce employees in the exercise of the rights guaranteed in [Section 7]."[92] While the NLRA does not define "concerted activities," it has been interpreted to arise whenever

83. 18 U.S.C. § 1030(a)(2)(C). A protected computer includes a computer "which is used in or affecting interstate or foreign commerce or communication." *Id.* § 1030(e)(2)(B).

84. 359 F.3d 1066 (9th Cir. 2004).

85. *Id.* at 1071.

86. *Id.* at 1078.

87. *Id.*

88. *But see* Owen v. Cigna, 188 F. Supp. 3d 790, 793 (N.D. Ill. 2016) (holding that former employer did not violate CFAA when accessing former employee's private email account using computer owned by former employer; "Neither party has identified—and the Court has not found—any CFAA case involving an employee's claim that her former employer exceeded its authority to access its own computer.").

89. 18 U.S.C. § 1030(c)(2)(B)(iii) (2012).

90. National Labor Relations Act, ch. 372, 49 Stat. 449 (1935) (codified as amended at 29 U.S.C. §§ 151–169 (2012)).

91. *Id.* § 7 (codified as amended at 29 U.S.C. § 157).

92. *Id.* § 8(1) (codified as amended at 29 U.S.C. § 158(a)(1)).

employees collectively seek to improve their lot as employees.[93] For example, the National Labor Relations Board (NLRB), which enforces the NLRA, has found that employees discussing on Facebook improper state tax withholding by their employer were engaged in protected concerted activity, precisely because the participants were seeking to initiate, induce, or prepare for group action related to a workplace issue (the calculation of the employees' tax withholding).[94]

As noted above, an employer's policy can have a significant impact on whether an employee may have an objective expectation of privacy in work-related electronic communications.[95] Employers do not, however, have unlimited freedom to restrict employees' electronic communications through their policies. Where a workplace rule is likely to have a chilling effect on Section 7 rights, its maintenance may be considered an unfair labor practice, even absent evidence of enforcement.[96] A rule that explicitly restricts activities protected by Section 7 is unlawful.[97] Even if a rule does not explicitly restrict activity protected by Section 7, it can still be unlawful if: "(1) employees would reasonably construe the language to prohibit Section 7 activity; (2) the rule was promulgated in response to union activity; or (3) the rule has been applied to restrict the exercise of Section 7 rights."[98]

Applying *Lutheran Heritage Village-Livonia*, the NLRB has deemed many employer email and social media policies to be unlawful under the NLRA.[99] For example, in *Triple Play Sports Bar and Grille*, the NLRB

93. *See* St. Margaret Mercy Healthcare Ctrs., 350 N.L.R.B. 203, 211 (2007), *enforced*, 519 F.3d 373 (7th Cir. 2008); *see also* NLRB v. Wash. Aluminum Co., 370 U.S. 9, 14 (1962) (referring to workers who had walked off the job because complaints of an unacceptably cold work shop had been ignored as "workers [acting] together to better their working conditions"). Section 7 rights are available to all employees, not just unionized workers; indeed, Section 7 rights are especially important for unorganized employees for they have no representative to take their grievances to their employer. *See id.* at 14-15.

94. Three D, LLC d/b/a Triple Play Sports Bar and Grille v. NLRB, 629 Fed. App'x 33, 35–36 (2d Cir. 2015). Indeed, one employee was considered to have engaged in protected concerted activity by merely "liking" part of the Facebook conversation. *Id.* at 37; *see also* Mexican Radio Corp., 02-CA-168989, 2017 WL 1507464 (N.L.R.B. Div. of Judges Apr. 26, 2017) (finding by Administrative Law Judge (ALJ) that employees engaged in protected concerted activities by positively responding via email, as a group, to a former employee's email complaints about restaurant's treatment of employees). *See generally* Christine Neylon O'Brien, *The First Facebook Firing Case Under Section 7 of the National Labor Relations Act: Exploring the Limits of Labor Law Protection for Concerted Communication on Social Media*, 45 SUFFOLK U. L. REV. 29 (2011) (analyzing NLRB's approach to protected concerted activity through social media posts); Robert Sprague, *Facebook Meets the NLRB: Employee Online Communications and Unfair Labor Practices*, 14 U. PA. J. BUS. L. 957 (2012) (reviewing NLRB considerations of employee conduct constituting protected concerted activity).

95. *Supra* note 33 and accompanying text and note 40.

96. Lafayette Park Hotel, 326 N.L.R.B. 824, 825 (1998), *enforced*, 203 F.3d 52 (D.C. Cir. 1999).

97. Lutheran Heritage Vill.-Livonia, 343 N.L.R.B. 646, 646 (2004).

98. *Id.* at 647.

99. *See generally* Christine Neylon O'Brien, *The Top Ten NLRB Cases on Facebook Firings and Employer Social Media Policies*, 92 OR. L. REV. 337 (2014) (reviewing social media policies); Robert

concluded that the employer's social media policy that prohibited "[inappropriate] discussions" could be interpreted by employees as prohibiting discussions about the employees' terms and conditions of employment.[100] Recently, an NLRB ALJ concluded the following employer policy was unlawful: "Any inappropriate or prohibited Internet, voice mail or e-mail access or use may result in discipline up to and including termination from employment."[101] As the ALJ explained:

> The rule prohibits "inappropriate or prohibited" use of the internet and email, as well as transmitting information to anyone that is "defamatory" and "otherwise offensive[']. These terms are not defined by [the employer], and the policy fails to provide any examples to clarify for employees what is to be considered inappropriate, defamatory or otherwise offensive. As such, employees would reasonably consider their Section 7 protected activity to be prohibited acts. For example, employees would reasonably fear that criticizing their employer to a third party or to one another would lead to discipline as the criticism may be viewed by the employer as inappropriate, defamatory or offensive.[102]

In *Purple Communications, Inc.*,[103] the NLRB ruled that an employer's policy prohibiting personal use of the employer's email system violated employees' Section 7 rights: "employees who have rightful access to their employer's email system in the course of their work have a right to use the email system to engage in Section 7-protected communications on nonworking time."[104] The NLRB expressly pointed out, however, that "an employer [is not] ordinarily prevented from notifying its employees . . . that it monitors (or reserves the right to monitor) computer and email use for legitimate management reasons and that employees may have no expectation of privacy in their use of the employer's email system."[105]

Sprague & Abigail E. Fournier, *Online Social Media and the End of the Employment-at-Will Doctrine*, 52 WASHBURN L.J. 557, 563–69 (2013) (reviewing NLRB opinions and decisions regarding lawfulness of employee social media policies).

100. 361 N.L.R.B. No. 31, 2014 WL 4182705, at *8–9 (Aug. 22, 2014), *enforced sub nom.* Three D, LLC d/b/a Triple Play Sports Bar and Grille v. NLRB, 629 Fed. App'x 33, 38 (2d Cir. 2015).

101. Thrifty Dollar Auto. Grp., 27-CA-173054, slip op. at 6 (N.L.R.B. Div. of Judges Jan. 27, 2017), http://apps.nlrb.gov/link/document.aspx/09031d458234634f [https://perma.cc/Z86E-79B2].

102. *Id.* at 7.

103. 361 N.L.R.B. No. 126, 2014 WL 6989135 (Dec. 11, 2014), *adopted by* 365 N.L.R.B. No. 50, 2017 WL 1132013 (Mar. 24, 2017).

104. 2014 WL 6989135, at *14.

105. *Id.* at *15. However, "[a]n employer that changes its monitoring practices in response to union or other protected, concerted activity, however, will violate the Act." *Id.* at *15 n.75. *But see* Quicken Loans, Inc., 07-CA-145794, slip op. at 29 (N.L.R.B. Div. of Judges Apr. 7, 2016), http://apps.nlrb.gov/link/document.aspx/09031d4582085e90 [https://perma.cc/CT5U-YTMY] (declining to extend *Purple Communications*' rationale to company policy prohibiting employees from downloading non-business related information or participating in web-based surveys without authorization; "I do not read *Purple Communications* to grant unrestricted right to download materials

4. Turning the Tables—Employees Monitoring Employers

It is becoming more and more common for employees, often using their smartphones, to record workplace conversations and incidents.[106] Twelve states have statutes that prohibit recording communications without the consent of all parties to the conversation.[107] Most of the statutes emulate Title I of the ECPA,[108] prohibiting the interception or attempt to intercept any wire, oral or electronic communication (without the consent of all parties to the conversation). But some of the statutes have their own nuances. For example, California's statute applies only to confidential communications, but defines confidential communications as "any communication carried on in circumstances as may reasonably indicate that any party to the communication desires it to be confined to the parties thereto."[109] This definition excludes, however, "a communication made in . . . any . . . circumstance in which the parties to the communication may reasonably

from the internet onto the Employer's email system. . . [or] a presumptive right to freely download materials from the internet onto the employer's server.").

106. *See, e.g.*, James R. Beyer, *Employers: Assume Your Employees Are Taping You . . . There's An App for That!*, SEYFARTH SHAW: WORKPLACE WHISTLEBLOWER (June 11, 2013), http://www.seyfarth.com/dir_docs/publications/WorkplaceWhistleblowerBeyer061113.pdf [https://perma.cc/V8KU-VUT5] (noting lawyers representing employees say more than fifty percent of their clients bring in digital evidence, saying they are more surprised when someone comes into their office *without* digital evidence); L.M. Sixel, *One-Third of Workers with Beefs Tape Their Bosses*, HOUS. CHRON. (Feb. 3, 2011, 6:30 AM), http://www.chron.com/business/sixel/article/One-third-of-workers-with-beefs-tape-their-bosses-1684505.php [https://perma.cc/G872-XML8] (reporting Houston EEOC office estimates that one-third of employees who visit it to file discrimination complaints bring secretly made recordings of sensitive conversations with their bosses or with human resources); *see also* Gabriel Sherman, *The Revenge of Roger's Angels: How Fox News Women Took Down the Most Powerful, and Predatory, Man in Media*, N.Y. MAG. (Sept. 2, 2016, 7:30 AM), http://nymag.com/daily/intelligencer/2016/09/how-fox-news-women-took-down-roger-ailes.html [https://perma.cc/WG9Y-DNT9] (reporting that Gretchen Carlson secretly recorded conversations with Fox News then-Chairman and CEO Roger Ailes to bolster her sexual harassment lawsuit against him).

107. California (CAL. PENAL CODE § 632 (2017)), Connecticut (CONN. GEN. STAT. § 52-570d (1990)), Delaware (DEL. CODE ANN. tit. 11, § 2402 (2014), Florida (FLA. STAT. ANN. § 934.03 (2015), Illinois (720 ILL. COMP. STAT. 5/14-2 (2016)), Maryland (MD. CODE ANN., CTS. & JUD. PROC. § 10-402 (2015)), Massachusetts (MASS. GEN. LAWS ch. 272, § 99 (1998)), Montana (MONT. CODE ANN. § 45-8-213 (2007)), New Hampshire (N.H. REV. STAT. ANN. § 570-A:2 (2017)), Oregon (OR. REV. STAT. § 165.540 (2016)), Pennsylvania (18 PA. CONS. STAT. § 5704(4) (2016)), Washington (WASH. REV. CODE § 9.73.030 (1986)). Nevada's statute could be construed to prohibit one person from recording a conversation involving multiple parties unless one of those parties consented. NEV. REV. STAT. ANN. § 200.650 (1989) (prohibiting a person from intruding "upon the privacy of other persons by surreptitiously listening to, monitoring or recording, or attempting to listen to, monitor or record, by means of any mechanical, electronic or other listening device, any private conversation engaged in by the other persons . . . unless authorized to do so by one of the persons engaging in the conversation"); *see Laws on Recording Conversations in All 50 States*, MATTHIESEN, WICKERT & LEHRER, S.C., https://www.mwl-law.com/wp-content/uploads/2013/03/LAWS-ON-RECORDING-CONVERSATIONS-CHART.pdf [https://perma.cc/Z9X3-5CBJ] (last updated Mar. 10, 2017).

108. *See supra* notes 62–73 and accompanying text.

109. CAL. PENAL CODE § 632(c).

expect that the communication may be overheard or recorded."[110] Connecticut's statute only applies to "oral private telephonic communication."[111] Illinois's statute applies to using an eavesdropping device in a surreptitious manner.[112] Massachusetts defines "interception" to mean "to secretly hear, secretly record, or aid another to secretly hear or secretly record the contents of any wire or oral communication through the use of any intercepting device by any person other than a person given prior authority by all parties to such communication[.]"[113] And that portion of Montana's statute that prohibits using electronic communications "to terrify, intimidate, threaten, harass, annoy, or offend . . . [by using] obscene, lewd, or profane language, suggest[ing] a lewd or lascivious act, or threaten[ing] to inflict injury or physical harm to the person or property of the person"[114] has been held unconstitutionally overbroad.[115]

Texas does not have a statute banning secret recordings. The Dallas County Community College District does, however, have a policy prohibiting employees from making secret recordings, the violation of which could lead to termination.[116] Not only is there no known common law right for employees to secretly record conversations with their supervisors,[117] "numerous courts have upheld the termination of employees for making or attempting to make secret recordings in violation of a company policy."[118]

As discussed above, company policies may run afoul of the NLRA if they are deemed to chill or potentially chill employees' exercise of their

110. *Id.*

111. CONN. GEN. STAT. § 52-570d(a).

112. 720 ILL. COMP. STAT. 5/14-2(a)(1). The Illinois Supreme Court ruled the original version of the statute, that did not specify surreptitious eavesdropping, deemed "all conversations to be private and, thus, not subject to recording absent consent, even if the participants have no expectation of privacy." People v. Melongo, 6 N.E.3d 120, 126–27 (Ill. 2014); *see* Michael J. Gibson, Comment, *Just Because It's Legal Doesn't Mean You Can Do It: The Legality of Employee Eavesdropping and Illinois Workplace Recording Policies*, 46 LOY. U. CHI. L.J. 913 (2015) (addressing workplace recording policies in light of the statute's amendment).

113. MASS. GEN. LAWS ch. 272, § 99(B)(4) (1998).

114. MONT. CODE ANN. § 45-8-213(1)(a) (2007).

115. State v. Dugan, 303 P.3d 755, 769 (Mont. 2013).

116. Mohamad v. Dallas Cty. Cmty. Coll. Dist., No. 3:10-CV-1189-L-BF, 2012 WL 4512488, at *7–8 (N.D. Tex. Sept. 28, 2012).

117. *Id.* at *9.

118. *Id.* (citing numerous cases in support); *see also* Argyropoulos v. City of Alton, 539 F.3d 724 (7th Cir. 2008) (holding evidence supported employer's legitimate reason for terminating plaintiff—she had secretly tape-recorded a conversation with employer's representatives—rather than Title VII retaliation); McBeth v. Shearer's Foods, Inc., No. 1:12CV00086, 2014 WL 4385764, at *8 (W.D. Va. Sept. 4, 2014) (granting employer's motion for summary judgment in discrimination claim where employee was fired for secretly making recording at work in violation of company policy).

Section 7 rights.[119] In a series of decisions, the NLRB has severely curtailed the right of employers to ban workplace recordings.[120] For the most part, these decisions rest upon application of *Lutheran Heritage Village-Livonia*.[121] In *Rio All-Suites Hotel & Casino*, the NLRB concluded that two employer rules—"Camera phones may not be used to take photos on property without permission from a Director or above" and "Cameras, any type of audio visual recording equipment and/or recording devices may not be used unless specifically authorized for business purposes (e.g. events)"—were unlawfully overbroad.[122] The Board stated, "Employee photographing and videotaping is protected by Section 7 when employees are acting in concert for their mutual aid and protection and no overriding employer interest is present."[123] In addition, neither of these prohibitions was tied to any particularized employer interest, such as the privacy of its patrons.[124]

Whole Foods Market banned any recordings without prior approval, with the purpose of eliminating "a chilling effect on the expression of views that may exist when one person is concerned that his or her conversation with

119. *See supra* notes 96–104 and accompanying text; *see also* Whole Foods Mkt. Grp., Inc., 363 N.L.R.B. No. 87, 2015 WL 9460031, at *4 n.11 (Dec. 24, 2015), *enforced sub nom.* Whole Foods Mkt. Grp., Inc. v. NLRB, Nos. 16-0002-ag, 16-0346, 2017 WL 2374843 (2d Cir. June 1, 2017) ("Where reasonable employees are uncertain as to whether a rule restricts activity protected under the Act, that rule can have a chilling effect on employees' willingness to engage in protected activity. Employees, who are dependent on the employer for their livelihood, would reasonably take a cautious approach and refrain from engaging in Sec. 7 activity for fear of running afoul of a rule whose coverage is unclear.").

120. *See* Stephens Media, LLC, d/b/a Hawaii Tribune-Herald v. NLRB, 677 F.3d 1241, 1257 (D.C. Cir. 2012) (upholding Board ruling that employee was entitled to reinstatement because he was engaged in protected concerted activity, despite having secretly tape-recorded conversations at work); T-Mobile USA, Inc., 363 N.L.R.B. No. 171, 2016 WL 1743244 (Apr. 29, 2016) (Board concluding employer's overly-broad rule restricting employees from using cameras and audio and recording devices in the workplace could reasonably be read by employees to prohibit recording that would be protected by Section 7); Whole Foods Mkt. Grp., Inc., 2015 WL 9460031 (Board concluding that rules prohibiting the recording of conversations, phone calls, images, or company meetings with a camera or recording device without prior approval by management would reasonably be construed by employees to prohibit Section 7 activity); Caesars Entm't d/b/a Rio All-Suites Hotel & Casino, 362 N.L.R.B. No. 190, 2015 WL 5113232 (Aug. 27, 2015) (Board concluding that rule banning use of cameras, camera phones, audiovisual, and other recording equipment unlawfully overbroad); Opryland Hotel, 323 N.L.R.B. 723 (1997) (Board ruling that in the absence of a rule, prohibition, or practice against employees using or possessing tape recorders at work, such possession or use does not constitute misconduct that would defeat reinstatement); AT&T Mobility, LLC, 05-CA-178637, 2017 WL 1488998 (N.L.R.B. Div. of Judges Apr. 25, 2017) (finding by ALJ that company's no-recording policy was illegal, following *T-Mobile USA*, *Whole Foods Mkt. Grp.*, and *Rio All-Suites Hotel & Casino*, despite company's concerns for customer privacy).

121. *See supra* text accompanying notes 97–98.

122. 2015 WL 5113232, at *4.

123. *Id.* ("Such protected conduct may include, for example, employees recording images of employee picketing, documenting unsafe workplace equipment or hazardous working conditions, documenting and publicizing discussions about terms and conditions of employment, or documenting inconsistent application of employer rules." (footnote omitted)).

124. *Id.*

another is being secretly recorded."[125] The Board concluded this ban "unqualifiedly prohibit[s] all workplace recording" and it does not "differentiate between recordings protected by Section 7 and those that are unprotected."[126] In *T-Mobile USA, Inc.*, the employer maintained the following policy:

> To prevent harassment, maintain individual privacy, encourage open communication, and protect confidential information employees are prohibited from recording people or confidential information using cameras, camera phones/devices, or recording devices (audio or video) in the workplace. Apart from customer calls that are recorded for quality purposes, employees may not tape or otherwise make sound recordings of work-related or workplace discussions.[127]

As with *Whole Foods Market Group, Inc.*, the Board concluded T-Mobile's "rule [did] not differentiate between recordings that are protected by Section 7 and those that are not, and[, additionally, included] in its prohibition recordings made during nonwork time and in nonwork areas."[128] T-Mobile argued its recording restriction was "justified by its general interest in maintaining employee privacy, protecting confidential information, and promoting open communication."[129] The Board rejected T-Mobile's "proffered rationales" because they "cannot justify the rule's broad restriction that employees would reasonably read as prohibiting activity protected by Section 7."[130]

The NLRB has found a workplace recording prohibition lawful. In *Flagstaff Medical Center, Inc.*,[131] the hospital had promulgated a rule prohibiting "[t]he use of cameras for recording images of patients and/or hospital equipment, property, or facilities . . . ."[132] Here, the Board did not consider the prohibition unlawfully overbroad because the "privacy interests of hospital patients are weighty, and [the hospital] has a significant interest in preventing the wrongful disclosure of individually identifiable health information, including by unauthorized photography."[133]

125. Whole Foods Mkt. Grp., Inc., 2015 WL 9460031, at *1.

126. *Id.* at *4 ("That the rule contains language setting forth an intention to promote open communication and dialogue does not cure the rule of its overbreadth.").

127. T-Mobile USA, Inc., 363 N.L.R.B. No. 171, 2016 WL 1743244, at *4 (Apr. 29, 2016).

128. *Id.* at *5.

129. *Id.*

130. *Id.*

131. 357 N.L.R.B. 659 (2011), *enforced in relevant part*, 715 F.3d 928 (D.C. Cir. 2013).

132. *Id.* at 662.

133. *Id.* at 663 ("Employees would reasonably interpret [the hospital's] rule as a legitimate means of protecting the privacy of patients and their hospital surroundings, not as a prohibition of protected activity.").

Board Member—now Chairman—Philip Miscimarra dissented in *Whole Foods Market Group, Inc.* with respect to the majority-Board's application of *Lutheran Heritage Village-Livonia*. Chairman Miscimarra took issue with the majority's conclusion that "employees would reasonably read the rules as prohibiting recording activity that would be protected by Section 7."[134] Noting that the rules themselves state that their purpose is to "encourage open communication, free exchange of ideas, spontaneous and honest dialogue and an atmosphere of trust" and "to eliminate a chilling effect on the expression of views . . . especially when sensitive or confidential matters are being discussed[,]"[135] he believes "[t]he rules are no less solicitous of open, free, spontaneous and honest conversations about union representation or group action for the purpose of mutual aid or protection than of other subjects of conversation."[136] Chairman Miscimarra has expressed his displeasure in other cases with the way in which the Board has applied *Lutheran Heritage Village-Livonia*. He has stated, for example, that he believes the time has come to abandon the analysis.[137] He believes the Board must, instead:

> [E]valuate at least two things: (i) the potential adverse impact of the rule on NLRA-protected activity, *and* (ii) the legitimate justifications an employer may have for maintaining the rule. The Board must engage in a meaningful balancing of these competing interests, and a facially neutral rule should be declared unlawful only if the justifications are outweighed by the adverse impact on Section 7 activity.[138]

As noted above, Philip Miscimarra is now Chairman of the NLRB. In addition, two open Board positions have been filled by the Trump administration and confirmed by the current Senate. If the two new Board members share Chairman Miscimarra's concerns with the manner in which *Lutheran Heritage Village-Livonia* has been applied, we may see a fundamental shift in determinations of whether employer policies—no-recording as well as social media in general—are unlawfully overbroad.[139]

134. Whole Foods Mkt. Grp., Inc., 363 N.L.R.B. No. 87, 2015 WL 9460031, at *4 (Dec. 24, 2015), *enforced sub nom.* Whole Foods Mkt. Grp., Inc. v. NLRB, Nos. 16-0002-ag, 16-0346, 2017 WL 2374843 (2d Cir. June 1, 2017).

135. *Id.* at *6 (Miscimarra, Member, dissenting).

136. *Id.* (Miscimarra, Member, dissenting) ("I believe it strains credulity to find that an employee could reasonably interpret the no-recording rules to prohibit Section 7 activity.").

137. William Beaumont Hosp., 363 N.L.R.B. No. 162, 2016 WL 1461576, at *8 (Apr. 13, 2016) (Miscimarra, Member, dissenting).

138. *Id.* (Miscimarra, Member, dissenting) (emphasis in original).

139. At publication, the NLRB revised its analysis of the *Lutheran Heritage Village-Livonia* standard to reflect Chairman Miscimarra's earlier dissents, as reflected *William Beaumont Hospital* (see

5. Federal Rules of Civil Procedure

In a few cases, federal magistrates have protected employee privacy by rejecting what they considered to be overly broad discovery requests. In *Bakhit v. Safety Marking, Inc.*,[140] the plaintiff sought access to text messages of his former fellow employees in his racial discrimination lawsuit against his former employer.[141] Noting that the right to information through discovery "is counterbalanced by a responding party's confidentiality or privacy interests[,]"[142] the magistrate was concerned with the implication of the individual defendants' privacy interests in the data stored on their cell phones.[143] In *Crabtree v. Angie's List, Inc.*,[144] the plaintiffs finalized sales with service providers for advertising on the Angie's List website and spent a significant portion of their workday using their personal computers and cell phones.[145] When the plaintiffs initiated a Fair Labor Standards Act lawsuit against Angie's List claiming unpaid overtime compensation, the defendant sought to obtain GPS and location services data from the plaintiffs' personal cell phones to "construct a detailed and accurate timeline of when Plaintiffs were or were not working."[146] The magistrate denied the request because it would reveal "all GPS/location data for 24-hours a day for a one year period from a personal device that would be tracking Plaintiffs' movements well outside of their working time."[147]

C. State Statutes that May Protect Employee Work-Related Communications

As noted above, twelve states outlaw surreptitious—i.e., without the consent of all parties—recording of conversations.[148] These twelve states[149] appear to support the position reported in the *Restatement (Third) of*

supra text accompanying note 138). *See* Boeing Co., 365 N.L.R.B. No. 154, 2017 WL 6403495 (Dec. 14, 2017).

140. No. 3:13CV1049 (JCH), 2014 WL 2916490 (D. Conn. June 26, 2014).

141. *Id.* at *1–2.

142. *Id.* at *2 (quoting Genworth Fin. Wealth Mgmt., Inc. v. McMullan, 267 F.R.D. 443, 446 (D. Conn. 2010)).

143. *Id.* at *3 (citing Riley v. California, 134 S. Ct. 2473 (2014)). *But see* Freres v. Xyngular Corp., No. 2:13–cv–400–DAK–PMW, 2014 WL 1320273 (D. Utah Mar. 31, 2014) (permitting discovery of information stored on plaintiff's cell phone).

144. No. 1:16-cv-00877-SEB-MJD, 2017 WL 413242 (S.D. Ind. Jan. 31, 2017).

145. *Id.* at *1.

146. *Id.*

147. *Id.* at *2. *See generally* Agnieszka A. McPeak, *Social Media, Smartphones, and Proportional Privacy in Civil Discovery*, 64 U. KAN. L. REV. 235 (2015) (analyzing privacy protection with respect to discovery requests).

148. *See supra* notes 107–115 and accompanying text.

149. Along with Nevada as well. *See supra* note 107.

Employment Law: "Eavesdropping via wiretapping has been conspicuously singled out on several occasions as precisely the kind of conduct that gives rise to an intrusion-on-seclusion claim."[150]

In addition, two states, Connecticut[151] and Delaware,[152] require employers to provide notice to employees of electronic monitoring. However, Connecticut's statute does not appear to provide much relief for employees who believe they have been monitored without notice, as the Connecticut Supreme Court has ruled the statute does not provide a private right of action to aggrieved employees.[153]

Twenty-five states have enacted what may generally be referred to as social media privacy statutes.[154] Fundamentally, these statutes prohibit employers (and prospective employers) from requiring or requesting employees and job applicants[155] to disclose their usernames and passwords to personal online accounts, often including personal email accounts. Many of the statutes also prohibit employers from requesting employees and applicants to access their accounts in the presence of the employer,[156] and

150. RESTATEMENT (THIRD) OF EMPLOYMENT LAW § 7.06 cmt. g (AM. LAW. INST. 2014) (citing Narducci v. Vill. of Bellwood, 444 F. Supp. 2d 924, 938 (N.D. Ill. 2006)). For additional cases involving employers surreptitiously recording employee conversations, see Hernandez v. Hillsides, Inc., 211 P.3d 1063 (Cal. 2009) (holding employees had a reasonable expectation of privacy in their office protecting against the employer's installation of a secret video camera, but remanded to jury question of whether intrusion was highly offensive); and Dorris v. Absher, 179 F.3d 420, 423–25 (6th Cir. 1999). *But see* Acosta v. Scott Labor LLC, 377 F. Supp. 2d 647, 651 (N.D. Ill. 2005) (holding "[t]he use of hidden cameras in an open office setting does not automatically transform a non-private area into a private one"); Nelson v. Salem State Coll., 845 N.E.2d 338 (Mass. 2006) (holding no expectation of privacy in office to which other employees had a key).

151. CONN. GEN. STAT. ANN. § 31-48d (West 1998).

152. DEL. CODE ANN. tit. 19, § 705 (West 2002).

153. Gerardi v. City of Bridgeport, 985 A.2d 328, 335 (Conn. 2010).

154. Arkansas: ARK. CODE ANN. § 11-2-124 (West 2014); California: CAL. LAB. CODE § 980 (Deering 2014); Colorado: COLO. REV. STAT. § 8-2-127 (2014); Connecticut: CONN. GEN. STAT. ANN. § 31-40x (West 2016); Delaware: 19 DEL. CODE ANN. § 709A (West 2015); Illinois: 820 ILL. COMP. STAT. 55/10 (2014); Louisiana: LA. REV. STAT. ANN. 51:1951–1955 (2014); Maine: ME. REV. STAT. ANN. tit. 26, §§ 616–619 (2015); Maryland: MD. CODE ANN., LAB. & EMPL. § 3-712 (West 2014); Michigan: MICH. COMP. LAWS §§ 37.272–278 (2014); Montana: MONT. CODE ANN. § 39-2-307 (West 2015); Nebraska: NEB. REV. STAT. ANN. §§ 48-3501–3511 (West 2016); Nevada: NEV. REV. STAT. ANN. § 613.135 (West 2014); New Hampshire: N.H. REV. STAT. § 275:74 (2014); New Jersey: N.J. STAT. ANN. §§ 34:6B-5–10 (West 2014); New Mexico: N.M. STAT. ANN. § 50-4-34 (West 2014); Oklahoma: OKLA. STAT. ANN. tit. 40, §§ 173.2, 173.3 (West 2014); Oregon: OR. REV. STAT. § 659A.330 (2013); Rhode Island: R.I. GEN. LAWS ANN. §§ 28-56-1 – -6 (West 2014); Tennessee: TENN. CODE ANN. §§ 50-1-1001–1004 (West 2015); Utah: UTAH CODE ANN. §§ 34-48-101–201 (West 2014); Virginia: VA. CODE ANN. § 40.1-28.7:5 (West 2015); Washington: WASH. REV. CODE §§ 49.44.200, 205 (2014); West Virginia: W. VA. CODE ANN. § 21-5H-1 (West 2016); Wisconsin: WIS. STAT. ANN. § 995.55 (West 2014).

155. New Mexico's statute applies only to job applicants. N.M. STAT. ANN. § 50-4-34(A).

156. *See, e.g.*, CAL. LAB. CODE § 980(b)(2).

some prohibit employers from requiring employees to add them to the list of contacts associated with the employees' accounts.[157]

Restatement (Third) of Employment Law § 7.04 reflects the privacy concerns at the core of these state social media privacy statutes:

> (a) An employee has a protected privacy interest in information relating to the employee that is of a personal nature and that the employee has made reasonable efforts to keep private.
>
> (b) An employer intrudes upon this protected privacy interest by requiring that the employee provide information described in subsection (a) or by obtaining the information through deceit.[158]

As this brief review of state statutes reveals, outside of employers surreptitiously recording their employees' conversations, these statutes provide little meaningful workplace privacy protections. While the social media privacy statutes appear the strongest, in reality the situation they address has occurred rarely, and usually in relation to sensitive employment positions, such as teachers, sheriff's deputies, and corrections officials.[159]

III. SMARTPHONES AND FITBITS

As the opening quote in this article from *Riley v. California*[160] implies, courts are beginning to realize the capacity of devices such as smartphones to store tremendous amounts of personal data. Those data can now include a person's locations twenty-four hours a day, seven days a week. In addition, wearable devices, such as the Fitbit, can track personal health information including continuous heart rate, steps taken, stairs climbed, active minutes, amount of sleep, and even GPS location.[161] What remains unanswered is what privacy rights workers have when employers require or encourage the use of these applications and devices, which can easily track movements and activities during non-work time.

157. *See, e.g.*, COLO. REV. STAT. § 8-2-127(2)(a). For further analysis of these statutes, see Jordan M. Blanke, *The Legislative Response to Employers' Requests for Password Disclosure*, 14 J. HIGH TECH. L. 42 (2014); Susan Park, *Employee Internet Privacy: A Proposed Act That Balances Legitimate Employer Rights and Employee Privacy*, 51 AM. BUS. L.J. 779 (2014); and Robert Sprague, *No Surfing Allowed: A Review & Analysis of Legislation Prohibiting Employers from Demanding Access to Employees' & Job Applicants' Social Media Accounts*, 24 ALB. L.J. SCI. & TECH. 481 (2014).

158. RESTATEMENT (THIRD) OF EMPLOYMENT LAW § 7.04(a) & (b) (AM. LAW INST. 2014); *see also id*. § 7.04 cmt. d.

159. *See, e.g.*, Park, *supra* note 157, at 779–80; Sprague, *supra* note 157, at 142.

160. *Supra* note 1 and accompanying text.

161. Brown, *supra* note 8, at 7–8.

A. GPS Tracking with Smartphones

As *Arias v. Intermex Wire Transfer* demonstrates, employers may be inclined to track employees' locations using the GPS feature in their smartphones.[162] Because the case settled, we have no way of knowing the strength of Arias's invasion of privacy claim. Courts generally find no privacy violation when the tracking device is installed on a company-owned vehicle.[163] At least eleven states outlaw private citizens from installing or using tracking devices,[164] though they regularly do not apply when the owner or lessor of the vehicle consents to the placement of the tracking device. As such, they provide no protection for private-sector employees when they are driving a company car. For example, California broadly prohibits the use of an "electronic tracking device to determine the location or movement of a person."[165] However, the California statute does not apply "when the registered owner, lessor, or lessee of a vehicle has consented to the use of the electronic tracking device with respect to that vehicle."[166] Similarly, Tennessee's statute, like most of the other state statutes, prohibits the installation of an electronic tracking device on or in a motor vehicle without the consent of all the owners or lessees of the vehicle.[167] Texas makes it a Class A misdemeanor to "knowingly install[] an electronic or mechanical tracking device on a motor vehicle owned or leased by another person,"[168] but provides an affirmative defense if the accused "obtained the effective

162. *See supra* notes 9–13 and accompanying text. *See generally* Haggins v. Verizon New England, Inc., 648 F.3d 50 (1st Cir. 2011) (affirming Labor Management Relations Act preempted state-law privacy claims where collective bargaining agreement required union employees to carry company-issued cell phones containing GPS capabilities while on the job).

163. *See, e.g.*, Elgin v. St. Louis Coca-Cola Bottling Co., No. 4:05CV970-DJS, 2005 WL 3050633, at *3–4 (E.D. Mo. Nov. 14, 2005) (citing United States v. Knotts, 460 U.S. 281 (1983)) (holding use of a tracking device on defendant's company car, even though it was assigned to plaintiff, does not constitute a substantial intrusion upon plaintiff's seclusion, as it revealed no more than highly public information as to the van's location; holding further that especially because the van was the property of defendant, defendant's use of the tracking device on its own vehicle does not rise to the level of being highly offensive to a reasonable person); RESTATEMENT (SECOND) OF TORTS § 652B cmt. c (AM. LAW INST. 1977)).

164. California: CAL. PENAL CODE § 637.7 (1998); Delaware: DEL. CODE ANN. tit. 11, § 1335(a)(8) (West 2014); Florida: FLA. STAT. § 934.425 (2015); Illinois: 720 ILL. COMP. STAT. 5/21-2.5 (2014); Louisiana: LA. STAT. ANN. § 14:323 (2015); Michigan: MICH. COMP. LAWS § 750.539l (West 2010); North Carolina: N.C. GEN. STAT. ANN. § 14-196.3 (West 2015); Rhode Island: 11 R.I. GEN. LAWS ANN. § 11-69-1 (West 2016); Tennessee: TENN. CODE ANN. § 39-13-606 (2016); Texas: TEX. PENAL CODE ANN. § 16.06 (West 2009); Virginia: VA. CODE ANN. § 18.2-60.5 (West 2013).

165. CAL. PENAL CODE § 637.7(a). The statute defines an "electronic tracking device" as "any device attached to a vehicle or other movable thing that reveals its location or movement by the transmission of electronic signals." *Id.* § 637.7(d).

166. *Id.* § 637.7(b).

167. TENN. CODE ANN. § 39-13-606(a)(1)(B).

168. TEX. PENAL CODE ANN. § 16.06(b).

consent of the owner or lessee of the motor vehicle before the electronic or mechanical tracking device was installed."[169] While Illinois's statute also prohibits the use of an "electronic tracking device to determine the location or movement of a person[,]"[170] it does not apply if the tracking device is used by a business for the purpose of tracking vehicles driven by employees of that business.[171]

Note that, with the exception of Florida, the state statutes refer to installing or attaching physical devices to vehicles, so they may not be applicable to smartphone tracking applications (such as the type involved in *Arias*). Florida is the only state that expressly mentions tracking *applications*.[172] "Tracking application" is defined as "any software program whose primary purpose is to track or identify the location or movement of an individual."[173] However, Florida's statute does not apply to a "person acting in good faith on behalf of a business entity for a legitimate business purpose."[174] It is uncertain which statute, if applicable, would have assisted more, Arias or Intermex Wire Transfer.

As noted earlier, courts have generally found no invasion of privacy when employers have observed employees in public places where the employees' expectations of privacy are diminished.[175] The same concept applies to GPS tracking—individuals driving cars are out in public, generally observable.[176]

Public-sector employees' privacy may, however, be afforded greater protection. Under evolving Fourth Amendment jurisprudence, courts are beginning to acknowledge that prolonged GPS tracking can reveal a detailed, intimate portrait of an individual's actions, and that this prolonged tracking

169. *Id.* § 16.06(d)(1).

170. 720 ILL. COMP. STAT. 5/21-2.5(b) (2014).

171. *Id*. § 21-2.5(c)(3).

172. FLA. STAT. § 934.425(2) (2016).

173. *Id.* § 934.425(1)(b).

174. *Id.* § 934.425(4)(d).

175. *See supra* note 57.

176. *See, e.g.*, Troeckler v. Zeiser, No. 14-cv-40-SMY-PMF, 2015 WL 1042187, at *3 (S.D. Ill. Mar. 5, 2015) (holding plaintiffs failed to plead that the placement of a GPS led to the disclosure of private facts; specifically, that plaintiffs failed to plead that the GPS conveyed information that the vehicle was driven into a private secluded location in which plaintiffs would have a reasonable expectation of privacy; in other words, plaintiffs failed to plead how a passerby on the street or an individual in another vehicle could not capture the same information that the tracking device captured and thus failed to plead the disclosure of a private fact) (applying Illinois common law to facts related to interfamily dispute); Villanova v. Innovative Investigations, Inc., 21 A.3d 650, 654–55 (N.J. Super. Ct. App. Div. 2011) (finding no invasion of privacy from private investigator tracking vehicle movement with GPS for forty days because the device never captured the movement of plaintiff into a secluded location that was not in public view); HSG, LLC v. Edge-Works Mfg. Co., No. 15 CVS 309, 2015 WL 5824453 (N.C. Sup. Ct. Oct. 5, 2015).

can defeat an "expectation of privacy that our society recognizes as reasonable."[177] This approach has been applied to public-sector employees.[178] As reported by the *Restatement (Third) of Employment Law*, "the reasonable expectations of privacy of citizens and residents against intrusion by government law-enforcement agents are likely to be significantly different from the privacy expectations of employees against employer intrusion."[179]

B. Employee Monitoring Through Wellness Programs

The Patient Protection and Affordable Care Act[180] provides a mechanism for employers, through their health insurance plans, to offer their employees programs of health promotion or disease prevention—otherwise known as wellness programs.[181] According to a 2016 Kaiser Family Foundation employer health benefits survey, eighty-three percent of surveyed large firms (200 or more employees) and forty-six percent of small firms offer some sort of wellness program, while sixteen percent of large firms and three percent of small firms collect health information from employees through wearable devices such as a Fitbit or Apple Watch.[182] In particular, employees may be rewarded for participating in a wellness program by receiving up to thirty percent of the cost of coverage under the employer's health plan.[183] Forty-two percent of large firms with a wellness program offer employees a financial incentive to participate in or complete

177. United States v. Maynard, 615 F.3d 544, 564 (D.C. Cir. 2010), *aff'd on other grounds sub nom*. United States v. Jones, 565 U.S. 400 (2012).

178. *See* Cunningham v. N.Y. State Dep't of Labor, 997 N.E.2d 468 (N.Y. 2013) (holding government agency placing GPS on personal vehicle of employee (without warrant) constituted an unreasonable search because it was excessively intrusive, as the GPS device tracked appellant on evenings, on weekends, and on vacation).

179. RESTATEMENT (THIRD) OF EMPLOYMENT LAW § 7.03 cmt. f (AM. LAW INST. 2014).

180. Pub. L. No. 111-148, 124 Stat. 119 (2010) (codified in scattered sections of 21, 25, 26, 29, and 42 U.S.C.); also known as the Affordable Care Act and ACA; colloquially known as Obamacare.

181. 42 U.S.C. § 300gg-4(j) (2012). *See generally* Kristin Madison et al., *Smoking, Obesity, Health Insurance, and Health Incentives in the Affordable Care Act*, 310 JAMA 143 (2013) (reviewing the ACA's health incentive initiatives). While the 115th Congress has attempted to repeal and replace the Affordable Care Act, to date its revisions have not addressed wellness programs.

182. *2016 Employer Health Benefits Survey, Summary of Findings*, KAISER FAMILY FOUND. (Sept. 14, 2016), http://kff.org/report-section/ehbs-2016-summary-of-findings/ [https://perma.cc/9BQT-AQUZ]; *see also* Elizabeth A. Brown, *Workplace Wellness: Social Injustice*, 20 N.Y.U. J. LEGIS. & PUB. POL'Y 191, 196–205 (2017) (examining the growth of workplace wellness programs, the incentives offered, and elements of various programs).

183. 42 U.S.C. § 300gg-4(j)(3)(A).

the program;[184] employees, on average, could potentially save between approximately $1,900 to $5,400 per year.[185]

While the Americans with Disabilities Act[186] (ADA) limits medical examinations and disability-related inquiries, it also provides safe harbor exceptions from its restrictions on medical testing for employer-mandated, as well as voluntary, medical examinations tied to employers' insurance[187] and wellness plans,[188] respectively. On May 17, 2016, the EEOC issued a final rule with respect to the interplay between the ADA and wellness programs.[189] Its amended regulation sets the criteria under which medical

184. *2016 Employer Health Benefits Survey, Summary of Findings*, *supra* note 182 (not reporting number of small firms offering incentives).

185. *Id.* (reporting average annual costs for all types of single health plans at $6,435 and average annual costs for all types of family health plans at $18,142).

186. Pub. L. No. 101-336, 104 Stat. 327 (1990) (codified as amended at 42 U.S.C. §§ 12101-12203 (2012)).

187. 42 U.S.C. § 12201(c)(2) provides a safe harbor exception for medical examinations that are tied to employers' insurance plans. *See* EEOC v. Flambeau, Inc., 131 F. Supp. 3d 849, 854 (W.D. Wis. 2015) (holding ADA § 12201(c)(2) safe harbor provision extends to wellness programs that are part of an insurance benefit plan):

> The wellness program requirement was clearly intended to assist defendant with underwriting, classifying or administering risks associated with the insurance plan. The undisputed evidence establishes that defendant's consultants used the data gathered through the wellness program to classify plan participants' health risks and calculate defendant's projected insurance costs for the benefit year. They then provided recommendations regarding what defendant should charge the plan participants for maintenance medications and preventive care. They also made recommendations regarding plan premiums, which included a recommendation that defendant charge cigarette smokers higher premiums.

Id. at 856.

The Seventh Circuit Court of Appeals affirmed *Flambeau*, 846 F.3d 941 (7th Cir. 2017), but declined to rule on the merits of the case due to mootness. *See also* Seff v. Broward Cty., 778 F. Supp. 2d 1370 (S.D. Fla. 2011), *aff'd*, 691 F.3d 1221 (11th Cir. 2012) (holding employer did not violate ADA by requiring employees to undergo medical examinations and making medical inquiries of employees as part of wellness program that was term of employer's group health plan designed to develop and administer current and future benefits plans using accepted principles of risk assessment). *But see* EEOC v. Orion Energy Systems, Inc., No. 14–CV–1019, 2016 WL 5107019 (E.D. Wis. Sept. 19, 2016) (concluding employer's wellness program was not used to underwrite, classify, or administer risk, and therefore not subject to the safe harbor exemption). The EEOC disagrees with the decisions in *Flambeau* and *Seff*, believing they "have applied the safe harbor provision far more expansively to support employers' imposition of penalties on employees who do not answer disability-related questions or undergo medical examinations in connection with wellness programs[.]" Regulations Under the Americans With Disabilities Act, 81 Fed. Reg. 31,125, 31,131 (May 17, 2016) (codified at 29 C.F.R. pt. 1630 (2017)).

188. 42 U.S.C. § 12112(d)(4)(B) provides an exception for medical examinations that are part of "employee health programs" regardless of whether the employer sponsors any sort of employee benefit plan at all. *See Flambeau*, 131 F. Supp. 3d at 854. "A covered entity may conduct *voluntary* medical examinations, *including voluntary medical histories*, which are part of an employee health program available to employees at that work site. A covered entity may make inquiries into the ability of an employee to perform job-related functions." 42 U.S.C. § 12112(d)(4)(B) (emphasis added).

189. Regulations Under the Americans With Disabilities Act, 81 Fed. Reg. 31,125; *see also EEOC's Final Rule on Employer Wellness Programs and Title I of the Americans with Disabilities Act*, EEOC, https://www.eeoc.gov/laws/regulations/qanda-ada-wellness-final-rule.cfm [https://perma.cc/H4K6-XNSW] (last visited May 15, 2017) (providing overview of new rules).

examinations are permitted.[190] In particular, the program must be voluntary—it cannot deny coverage or benefits for non-participation, nor can there be any retaliation for non-participation.[191] And providing an incentive of up to thirty percent of health coverage cost will not render a program involuntary.[192]

Title II of the Genetic Information Nondiscrimination Act[193] (GINA) prohibits employers from discriminating against employees based on genetic information,[194] and prohibits employers, with certain exceptions, from acquiring genetic information about an employee.[195] Under the Affordable Care Act, "[a] group health plan, and a health insurance issuer offering health insurance coverage in connection with a group health plan, shall not request or require an individual or a family member of such individual to undergo a genetic test."[196] However, under a voluntary wellness program, an employer may provide a limited incentive[197] for an employee's spouse to provide information about the spouse's current or past health status.[198] Finally, legislation introduced in the House of Representatives, the Preserving

190. Regulations Under the Americans With Disabilities Act, 81 Fed. Reg. at 31,139 (codified at 29 C.F.R. § 1630.14).

191. *See id.* (codified at § 1630.12).

192. *See id.* at 31,140 (codified at § 1630.14(d)(3)). The EEOC calculates the thirty percent incentive as thirty percent of self-only coverage, including both the employee's and employer's contribution. *Id*. (codified at § 1630.14(d)(3)(i)). The incentive applies to an employee's participation in a "health-contingent" wellness program, which focuses "on an insured individual's satisfaction of a particular health-related factor." AARP v. EEOC, No. 16-2113 (JDB), 2017 WL 3614430, at *1 (D.D.C. Aug. 22, 2017) (citing Incentives for Nondiscriminatory Wellness Programs in Group Health Plans, 78 Fed. Reg. 33, 157, 33,180 (June 3, 2013) (codified at 26 C.F.R. pt. 54 (2017)). There are no incentive caps on "participatory" wellness programs—i.e., "programs that do not condition receipt of the incentive on satisfaction of a health factor." *Id.* (citing Incentives for Nondiscriminatory Wellness Programs in Group Health Plans, 78 Fed. Reg. at 33,167).

193. Pub. L. No. 110-223, tit. II, 122 Stat. 881, 905 (2008) (codified at 42 U.S.C. §§ 2000ff–2000ff-11 (2012)).

194. 42 U.S.C. § 2000ff-1(a).

195. *Id.* § 2000ff-1(b).

196. 42 U.S.C. § 300gg-4(c)(1) (2012).

197. Essentially, thirty percent of self-only coverage, including both the employee's and employer's contribution. Genetic Information Nondiscrimination Act, 81 Fed. Reg. 31,143 (May 17, 2016) (codified at 29 C.F.R. § 1635.8(b)(2)(iii)(A)).

198. *Id*. (codified at 29 C.F.R. § 1635.8(b)(2)); *see also EEOC's Final Rule on Employer Wellness Programs and the Genetic Information Nondiscrimination Act*, EEOC, https://www.eeoc.gov/laws/regulations/qanda-gina-wellness-final-rule.cfm [https://perma.cc/D4KL-Y3JQ] (last visited May 15, 2017). While the Health Insurance Portability and Accountability Act (HIPAA), Pub. L. No. 104-191, tit. I, § 702, 110 Stat. 1936, 1945 (1996) (codified as amended at 29 U.S.C. § 1182 (2015)), prohibits group health insurance plans from excluding employees based on, inter alia, health status, medical history, genetic information, and disability (29 U.S.C. § 1182(a)(1)), it does allow group health plans to offer premium discounts or rebates for participation in wellness programs (*id.* § 1182(b)(2)(B)). The IRS has similar prohibitions and wellness program exceptions at 26 U.S.C. § 9802 (2012).

Employee Wellness Programs Act,[199] allows collection of genetic information of family members as part of a wellness program.[200]

On a practical basis, just how voluntary are wellness programs when individual employees may save up to $1,900 per year by participating? In effect, is this not really a penalty for not participating? The AARP believes so. It filed a complaint against the EEOC seeking a preliminary injunction to stop implementation of the EEOC's wellness program ADA and GINA rules, claiming the definition of "voluntary" adopted by the EEOC is inconsistent with both the ADA and GINA because permitting incentives at up to thirty percent of the cost of coverage renders the incentives coercive.[201] Although the U.S. District Court for the District of Columbia initially denied AARP's motion for a preliminary injunction,[202] it subsequently ruled that the EEOC failed to provide a reasoned explanation for its decision to adopt the thirty percent incentive levels in both the ADA and GINA rules.[203] It did not vacate the rules, but remanded them to the EEOC for reconsideration.[204]

Put another way, is foregoing the premium discount a "privacy tax?"[205] Fitbit data can reveal a lot of information to an employer:

> 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

199. H.R. 1313, 115th Cong. (2017).

200. *Id.* § 3(b).

201. Complaint, AARP v. EEOC, 226 F. Supp. 3d 7 (D.D.C. 2016) (No. 16-cv-2113), 2016 WL 6211326.

202. *AARP*, 226 F. Supp. 3d 7.

203. AARP v. EEOC, No. 16-2113 (JDB), 2017 WL 3614430, at *16 (D.D.C. Aug. 22, 2017) ("Neither the final rules nor the administrative record contain any concrete data, studies, or analysis that would support any particular incentive level as the threshold past which an incentive becomes involuntary in violation of the ADA and GINA.").

204. *Id.* at *17 ("[W]hile the Court has serious concerns about the agency's reasoning regarding the GINA and ADA rules, these concerns are currently outweighed by the 'disruptive consequences' that are likely to result from vacatur. Assuming that the agency can address the rules' failings in a timely manner, vacatur 'is not the required remedy,' and would indeed be inappropriate at this time." (quoting AFL-CIO v. Chao, 496 F. Supp. 2d 76, 91 (D.D.C. 2007)). AARP has filed a motion with the court requesting that the rules either be vacated effective January 1, 2018, or their enforcement enjoined, again effective January 1, 2018, pending the EEOC's reconsideration of the rules. AARP's Memorandum of Law in Support of Rule 59(e) Motion to Alter or Amend the Court's Aug. 22, 2017 Order, *AARP*, 2017 WL 3614430 (No. 16-cv-2113 (JDB)), https://benefitslink.com/src/ctop/AARP_motion-to-amend_DDC_08302017.pdf [https://perma.cc/5V9T-5XSQ].

205. *See* Mark A. Rothstein & Heather L. Harrell, *Health Risk Reduction Programs in Employer-Sponsored Health Plans: Part I—Efficacy*, 51 J. OCCUPATIONAL & ENVTL. MED. 943, 944 (2009) (suggesting that higher-paid employees can more easily afford to pay a "privacy tax" and not have to share health information in a wellness program, whereas lower-paid employees may be more economically vulnerable, and, thus, more likely to feel coerced into signing up to participate; completing analysis prior to the EEOC's May 17, 2016 final rules).

> cognitive performance, and negative emotions such as anger, depression, sadness, and fear.[206]

One scholar has questioned whether companies selling Fitbits and similar wearable technology are in the business of selling devices or in the business of selling the data those devices generate.[207]

> [T]he data coming off of sensors are incredibly high quality. I can paint an incredibly detailed and rich picture of who you are based on your Fitbit data or any of this other fitness and health data. And that data is so high quality that I can do things like price insurance premiums or I could probably evaluate your credit score incredibly accurately.[208]

One could easily conclude that the thirty-percent incentives to participate in "voluntary" wellness programs coerces employees to forego medical privacy otherwise provided by the ADA and GINA.

IV. CONCLUDING ANALYSIS

As noted at the beginning of Part II above, employers have a number of legitimate business reasons—and, in some cases, legal obligations—to monitor their workers. Except in extreme cases (or except under Section 7 of the NLRA as currently applied), employers should have no problems justifying workplace monitoring, particularly during working hours. But technology that almost all workers use allows monitoring twenty-four hours a day, seven days a week. All that data may sometime prove too tempting to employers, causing them to cross the boundary from monitoring—to watch or keep track of, usually for a special purpose[209]—to snooping—to make a presumptuous inquiry, especially in a sneaking or meddlesome manner.[210]

206. Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 TEX. L. REV. 85, 119 (2014) (footnotes omitted) [hereinafter Peppet, *Internet of Things*].

207. *See* Scott Peppet, Professor of Law, Univ. of Colo. Law Sch., Address at the Federal Trade Commission Internet of Things Workshop 168 (Nov. 19, 2013), http://www.ftc.gov/sites/default/files/documents/public_events/internet-things-privacy-security-connected-world/final_transcript.pdf [https://perma.cc/LCT2-CYDP].

208. *Id.* at 169. "Ira Hunt, who is the CIO of the CIA said you can be 100 percent identified, as an individual, by your Fitbit data. Why? Because no two persons' gaits or ways of moving are the same. We can almost always figure out who you are based on that kind of incredibly rich detail." *Id*. at 170-71; *see also* Brown, *supra* note 8, at 13 ("The explosive growth of wearable device ownership makes it easier than ever for employers to collect health and fitness data about their employees."); Cathy O'Neil, *That Health Tracker Could Cost You*, BLOOMBERG VIEW (Feb. 23, 2017, 6:30 AM; updated Mar. 8, 2017, 9:08 AM), https://www.bloomberg.com/view/articles/2017-02-23/that-free-health-tracker-could-cost-you [https://perma.cc/6FUH-6XYE] ("In the short term, there's more money in profiling people as high-risk or low-risk than there is in solving their actual health problems. Granted, the information people provide to insurance companies might never be used against them personally. But it could ultimately be used against people like them.").

209. MERRIAM-WEBSTER'S COLLEGIATE DICTIONARY 801 (11th ed. 2011).

210. *Id.* at 1181. Recall RESTATEMENT (THIRD) OF EMPLOYMENT LAW § 7.06(b) (AM. LAW INST. 2014): "An intrusion is highly offensive . . . if the nature, manner, and scope of the intrusion are clearly

While this article has reviewed laws affecting "traditional" work-related privacy protections for electronic data and communications, the growing trend is ever-more powerful devices that can collect and store ever-more personal information, twenty-four hours a day, seven days a week, usually intermingled with work-related data and communications. Courts still apply common law GPS privacy standards under the notion that an individual driving a car around the streets of a city that has a tracking device installed in or on the car is not necessarily driving in secluded areas.[211] In the meantime, individuals can be now identified with high degrees of accuracy based upon "anonymous" mobility data sets.[212]

Massive amounts of data are being collected, juxtaposed with large, diverse data sets, and processed with mathematical algorithms—all to determine, say, whether an employee is more likely to be productive or even remain on the job for a given length of time.[213] Add to this the GPS data accumulated when employees are required to install a GPS app on their smartphone—and keep their smartphone turned on 24/7—and the biometric data accumulated when employees are given a Fitbit along with a substantial financial incentive to allow their group health insurance provider to track

unreasonable when judged against the employer's legitimate business interests or the public's interests in intruding."

211. *See supra* note 176 and accompanying text.

212. *See* Yves-Alexandre de Montjoye et al., *Unique in the Crowd: The Privacy Bounds of Human Mobility*, 3 SCI. REP. 1, 1 (2013) (concluding that their formula for the uniqueness of human mobility traces represents fundamental constraints to an individual's privacy); *see also* Ira S. Rubinstein & Woodrow Hartzog, *Anonymization and Risk*, 91 WASH. L. REV. 703, 704-05 (2016) (discussing the risk to privacy by the failed assumption that data sets are truly anonymized).

213. *See* Robert Sprague, *Welcome to the Machine: Privacy and Workplace Implications of Predictive Analytics*, 21 RICH. J.L. & TECH. 12 (2015), http://jolt.richmond.edu/v21i4/article12.pdf [https://perma.cc/66ES-PXRV]; PRESIDENT'S COUNCIL OF ADVISORS ON SCI. & TECH., EXEC. OFFICE OF THE PRESIDENT, BIG DATA AND PRIVACY: A TECHNOLOGICAL PERSPECTIVE 21 (2014), https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/ pcast_big_data_and_privacy_-_may_2014.pdf [https://perma.cc/L3CU-RCD8]; CATHY O'NEIL, WEAPONS OF MATH DESTRUCTION: HOW BIG DATA INCREASES INEQUALITY AND THREATENS DEMOCRACY (2016) (revealing that algorithmic models that determine, say, whether someone gets a car loan or how much they pay for health insurance, are opaque, unregulated, and uncontestable, even when they're wrong); Rachel Emma Silverman, *Tracking Sensors Invade the Workplace: Devices on Workers, Furniture Offer Clues for Boosting Productivity*, WALL ST. J. (Mar. 7, 2013, 11:42 AM), https://www.wsj.com/articles/SB10001424127887324034804578344303429080678 [https://perma.cc/67F2-8RTX] ("As Big Data becomes a fixture of office life, companies are turning to tracking devices to gather real-time information on how teams of employees work and interact. Sensors, worn on lanyards or placed on office furniture, record how often staffers get up from their desks, consult other teams and hold meetings."); *see also* Timothy L. Fort et al., *The Angel on Your Shoulder: Prompting Employees to Do the Right Thing Through the Use of Wearables*, 14 NW. J. TECH. & INTELL. PROP. 139 (2016) (positing that wearable technologies, such as a Fitbit, could be used by employers to "nudge" employees toward more ethical behaviors); Richards, *supra* note 2, at 1934 ("The digital technologies that have revolutionized our daily lives have also created minutely detailed records of those lives.").

their vital signs—again, 24/7.[214] Because so many different devices are now collecting data and are interconnected through the Internet, employers have access to an abundance of data beyond just Fitbits at work or social media posts. For example, driving data from a smartphone GPS might provide inferences about personality and habits; electricity usage may reveal lifestyle traits, such as how late an employee stays up at night; and smartphone data may even reveal insights from conversational patterns.[215]

All of those data may just prove too tempting for snooping employers. Meanwhile, most of our privacy laws were adopted well before smartphones and the Internet became ubiquitous; they still hunt for physical secluded locations; and, because they are based on reasonable expectations of privacy, they can easily be circumvented by employer policies that eliminate that expectation by informing workers they have no right to privacy in the workplace.

The future—indeed the present—does not bode well for worker privacy.

214. *See, e.g.*, Brown, *supra* note 182, at 246 (detailing some of the data risks associated with the use of Fitbits in wellness programs, including re-identification of anonymous data, inaccurate data due to employee misuse or device inaccuracy, and interception of sensitive data by hackers).

215. *See* Peppet, *Internet of Things*, *supra* note 206, at 120.